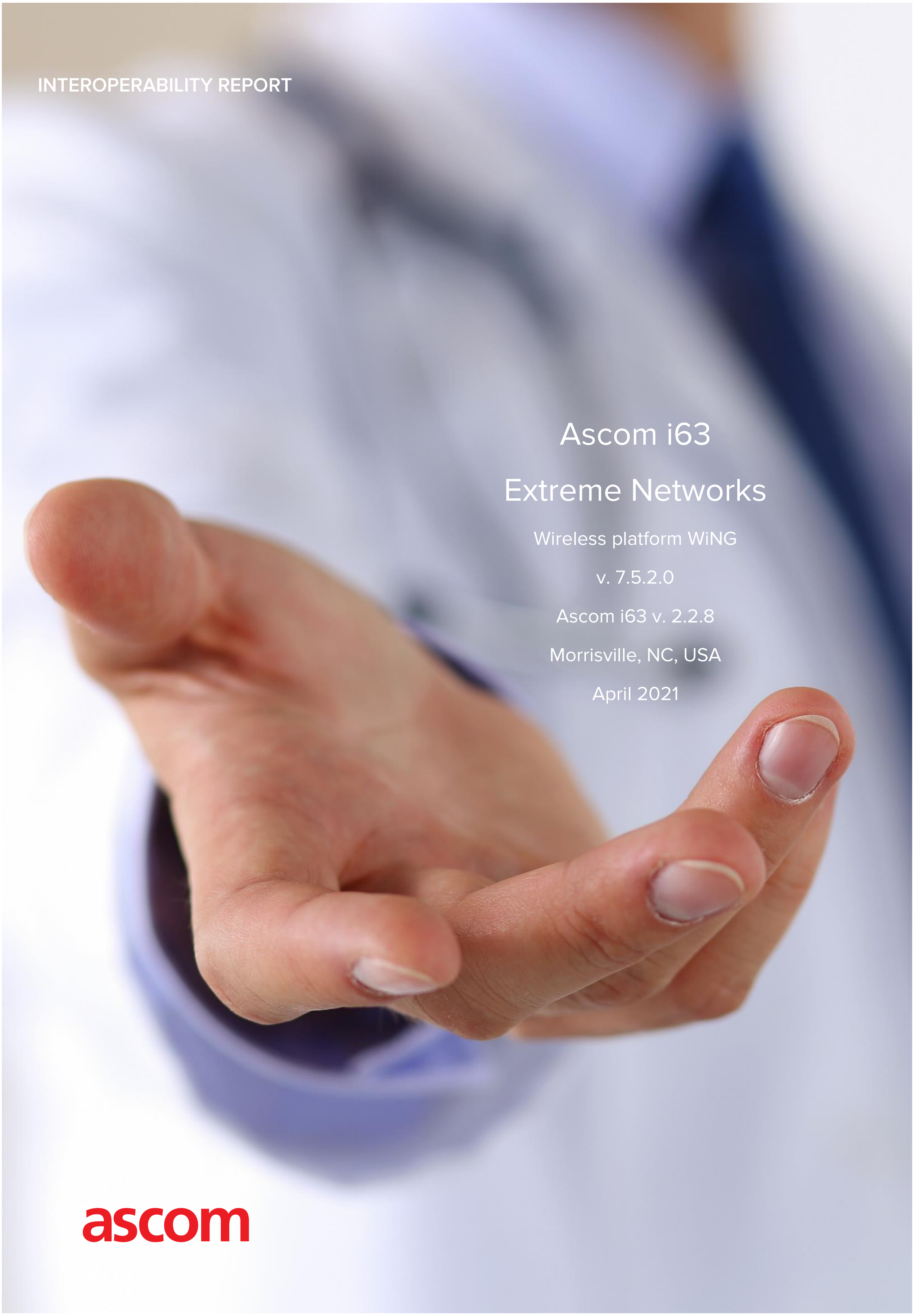


INTEROPERABILITY REPORT

Ascom i63

Extreme Networks

Wireless platform WiNG

v. 7.5.2.0

Ascom i63 v. 2.2.8

Morrisville, NC, USA

April 2021

Contents

Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Extreme Networks platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Extreme Networks and Ascom's platform configuration guides.

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 operating businesses in 18 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

About Extreme Networks

Extreme Networks, Inc. (EXTR) is the industry's first cloud-driven, end-to-end enterprise networking company. Our best-of-breed technology solutions, from the wireless and IoT edge to the data center, are flexible, agile, and secure to accelerate the digital transformation of our customers and provide them with the fastest path to the autonomous enterprise. Our 100% in-sourced services and support are number one in the industry. Even with 50,000 customers globally, including half of the Fortune 50 and some of the world's leading names in business, hospitality, retail, transportation and logistics, education, government, healthcare, and manufacturing, we remain nimble and responsive to ensure customer and partner success. We call this Customer-Driven Networking™. Founded in 1996, Extreme is headquartered in San Jose, California. For more information, visit Extreme's website or call 1-888-257-3000.

=

Site Information

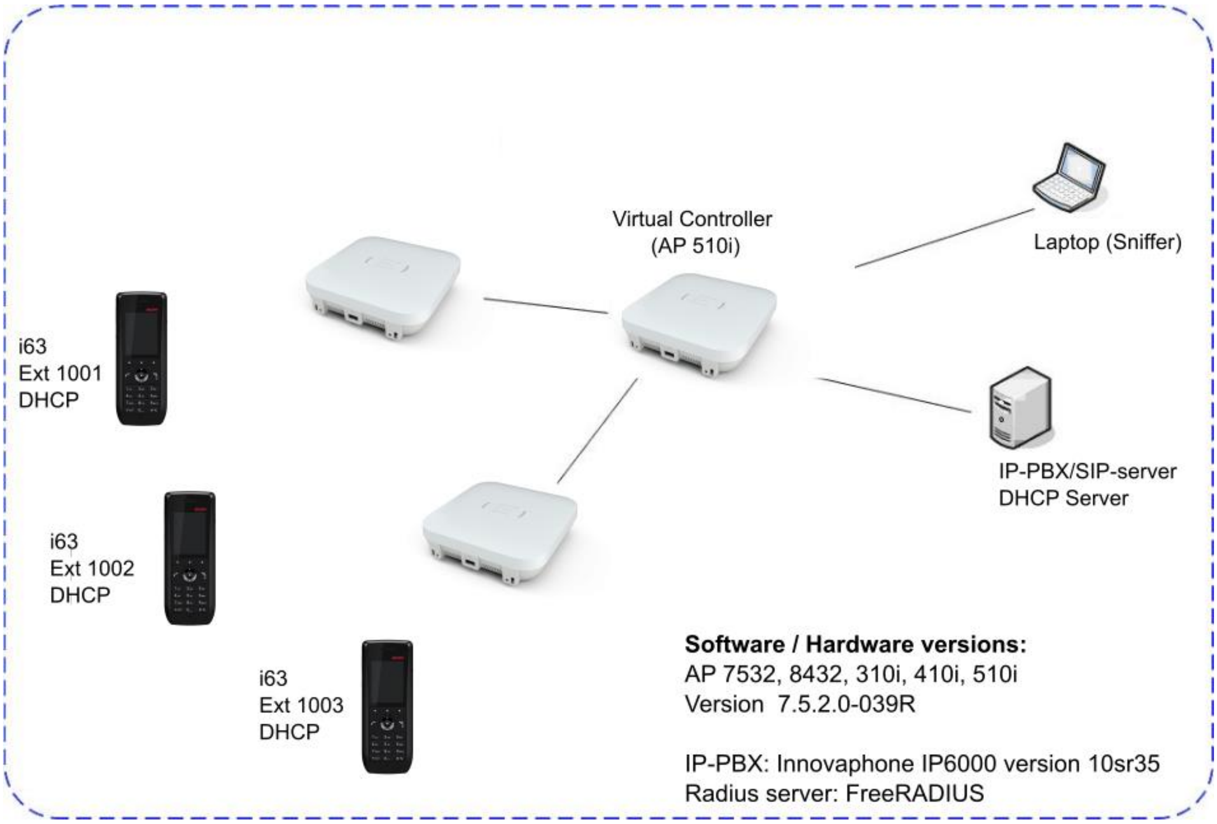
Verification site

Ascom US
300 Perimeter park drive
Morrisville, NC, US-27560
USA

Participants

Karl-Magnus Olsson, Ascom, Morrisville

Verification topology



Summary

General conclusions

The verification, including association, authentication and call stability tests generated in general very good results.

Roaming times were measured in the 30-40ms ranges when using both WPA2-PSK PSK, 802.1X (OKC) and Fast Roaming (802.11r).

It was noted that the 802.11k and 802.11v Neighbour report contained no information. Its recommended to not rely on 802.11k for roaming decision. See Known Issues section for details.

Compatibility information

Based on the test of 310i, 410i, 510i 7532 and 8432 we consider following list of access point models to be covered.

Supported Partner Access Points with Extreme Networks WiNG version 7.5.2.0:

AP7522, 7532, 8132, 8432

AP310i/e

AP410i/e

AP505 and 510 i/e

AP 360i/e, 460i/e and 560i (outdoor)

Supported controller platforms with Extreme Networks WiNG 7.5.2.0:

NX 5500, 75xx, 9500, 9510, 9600, 9610

VX9000

Verification overview

WLAN Compatibility and Performance

High Level Functionality	Result	Comments
Association, Open with No Encryption	OK	
Association, WPA2-PSK / AES Encryption	OK	
Association, PEAP-MSCHAPv2 Auth, AES Encryption	OK	
Association with EAP-TLS authentication	OK	
Association, Multiple ESSIDs	OK	
Beacon Interval and DTIM Period	OK	
PMKSA Caching	OK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	OK	
802.11e U-APSD (load test)	OK	
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 30 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK *	Typical roaming time 33ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 23ms
Channel usage controlled by 802.11k	NOK	See known issues
Network features controlled by 802.11v	N/A	Not supported by i63

Average roaming times are measured using 802.11a/n/ac. Refer to Appendix B for detailed test results

*) Measured times is with opportunistic/proactive Key Caching enabled (default enabled)

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
802.11k/v Neighbor report contains no data rendering the added benefit of the feature not useful. Under investigation	Avoid setting **5GHz Channel** to **802.11k** (See configuration note on page 18)	Contact Ascom or Extreme Wireless support

For additional information regarding the known limitations please contact **interop@ascom.com** or **support@ascom.com**.

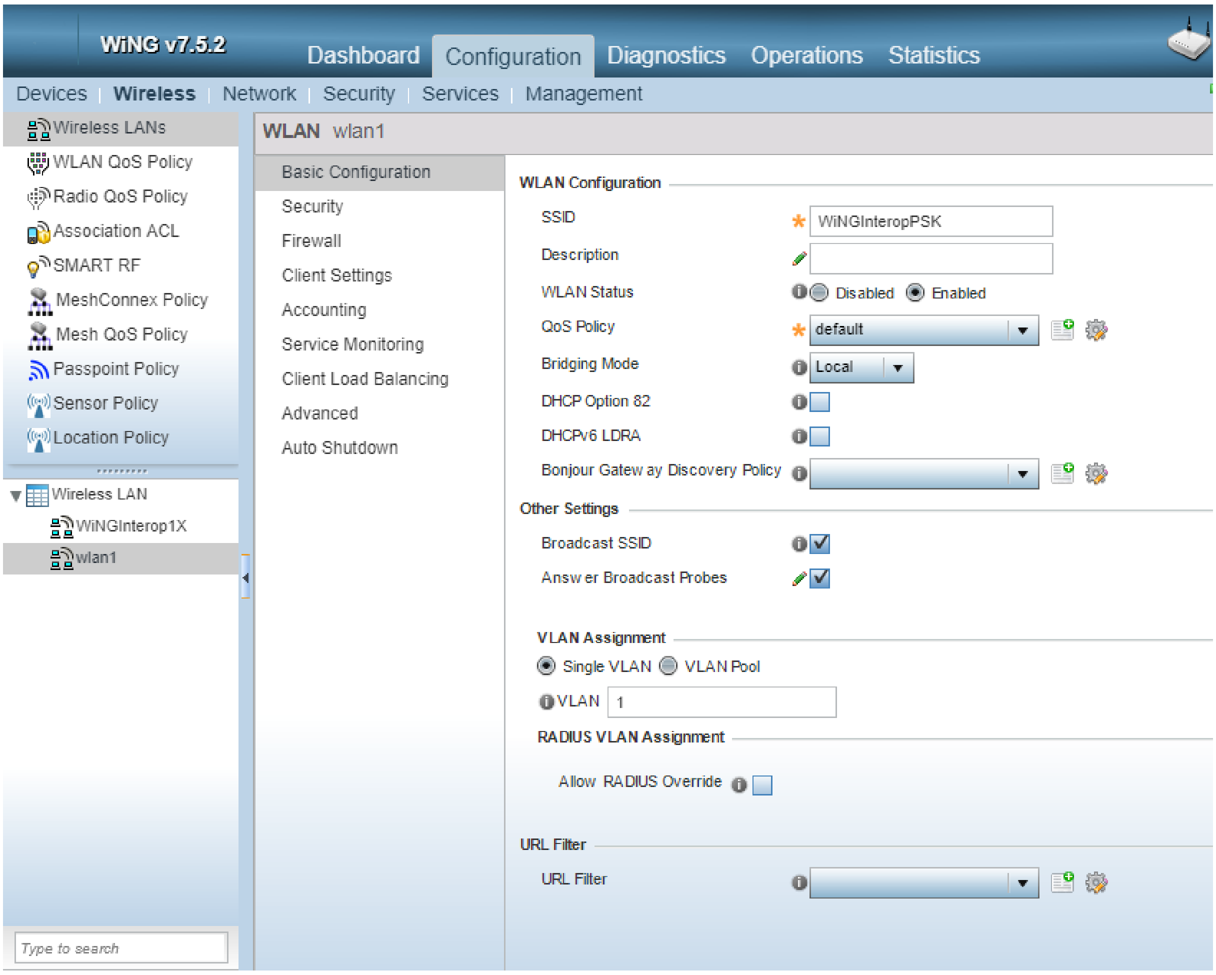
For detailed verification results, refer to Appendix B: Interoperability Verification Records.

Appendix A: Verification Configurations

Extreme Networks WiNG 7.5.2.0

In the following chapter you will find screenshots and explanations of basic settings in order to get an Extreme Networks wireless system to operate with an Ascom i63. Please note that security settings were modified according to requirements in individual test cases.

SSID/WLAN and Security settings PSK



WLAN wlan1

WLAN Configuration

SSID * WiNGInteropPSK

Description

WLAN Status ○ Disabled ● Enabled

QoS Policy * default

Bridging Mode Local

DHCP Option 82 □

DHCPv6 LDRA □

Bonjour Gatew ay Discovery Policy

Other Settings

Broadcast SSID ☑

Answ er Broadcast Probes ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN 1

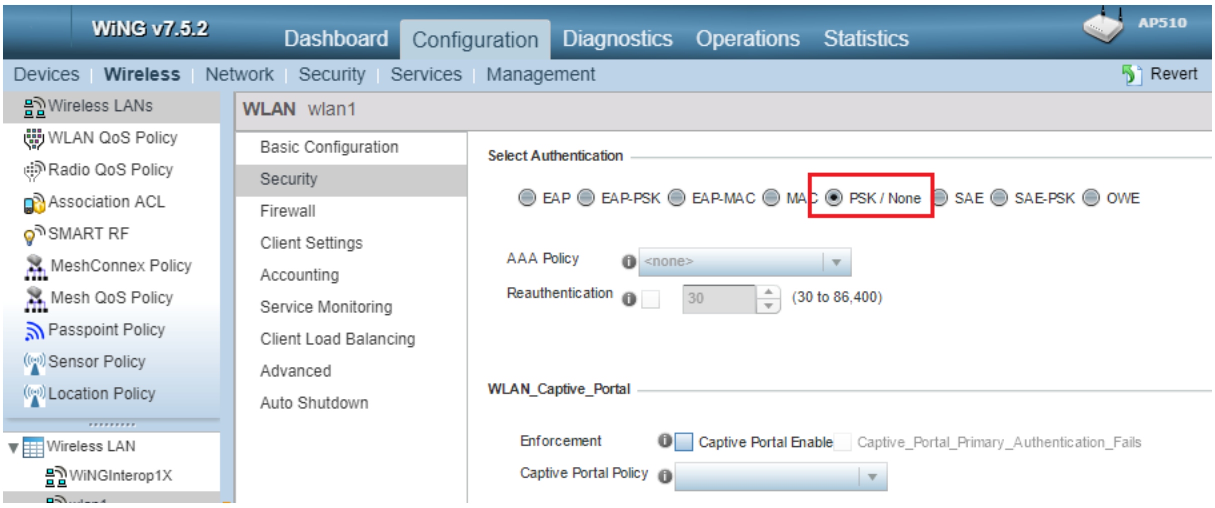
RADIUS VLAN Assignment

Allow RADIUS Override □

URL Filter

URL Filter

WLAN Basic settings



WLAN wlan1

Select Authentication

○ EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ● PSK / None ○ SAE ○ SAE-PSK ○ OWE

AAA Policy <none>

Reauthentication □ 30 (30 to 86,400)

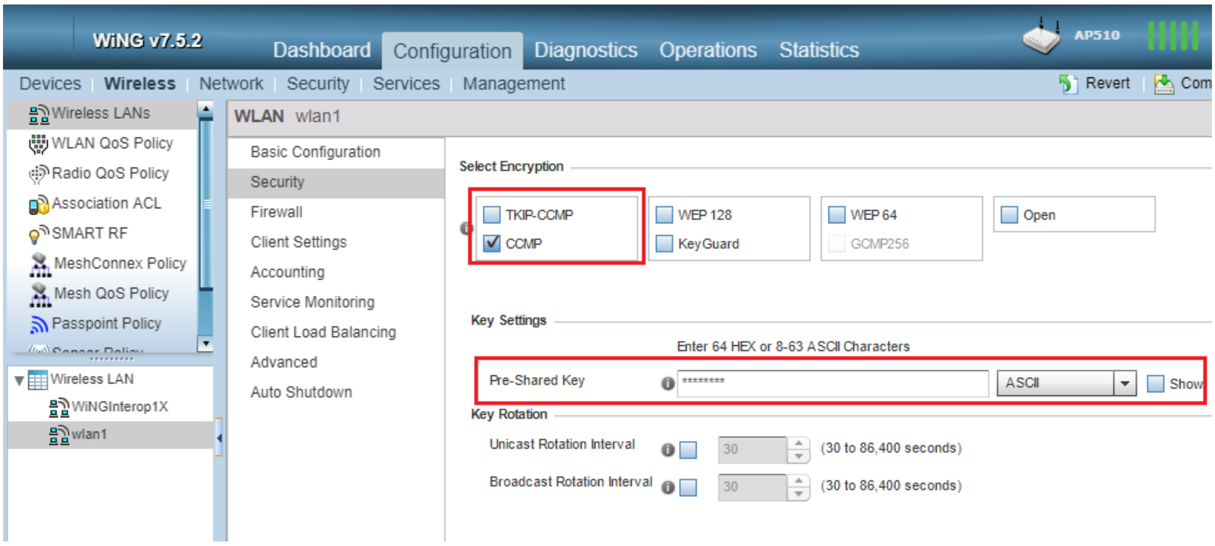
WLAN_Captive_Portal

Enforcement □ Captive Portal Enable □ Captive_Portal_Primary_Authentication_Fails

Captive Portal Policy

Security profile WPA2-PSK, AES-CCMP encryption.

- Select Authentication method: PSK/None



WLAN wlan1

Select Encryption

□ TKIP-CCMP
☑ CCMP
□ WEP 128
□ KeyGuard
□ WEP 64
□ GCMP256
□ Open

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key ******** ASCII □ Show

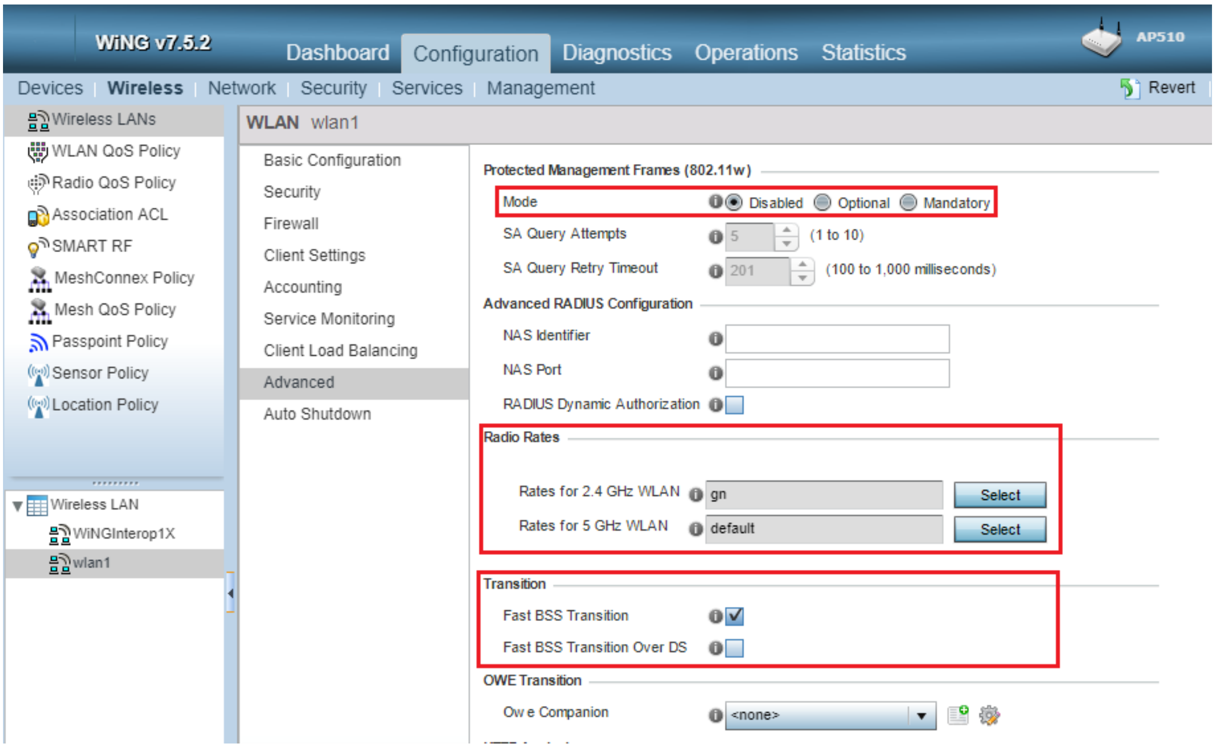
Key Rotation

Unicast Rotation Interval □ 30 (30 to 86,400 seconds)

Broadcast Rotation Interval □ 30 (30 to 86,400 seconds)

Security profile WPA2-PSK, AES-CCMP encryption. Continued.

- Select Encryption: CCPM
- Configure Pre Shared Key



WLAN wlan1

Protected Management Frames (802.11w)

Mode ● Disabled ○ Optional ○ Mandatory

SA Query Attempts 5 (1 to 10)

SA Query Retry Timeout 201 (100 to 1,000 milliseconds)

Advanced RADIUS Configuration

NAS Identifier

NAS Port

RADIUS Dynamic Authorization □

Radio Rates

Rates for 2.4 GHz WLAN gn Select

Rates for 5 GHz WLAN default Select

Transition

Fast BSS Transition ☑

Fast BSS Transition Over DS □

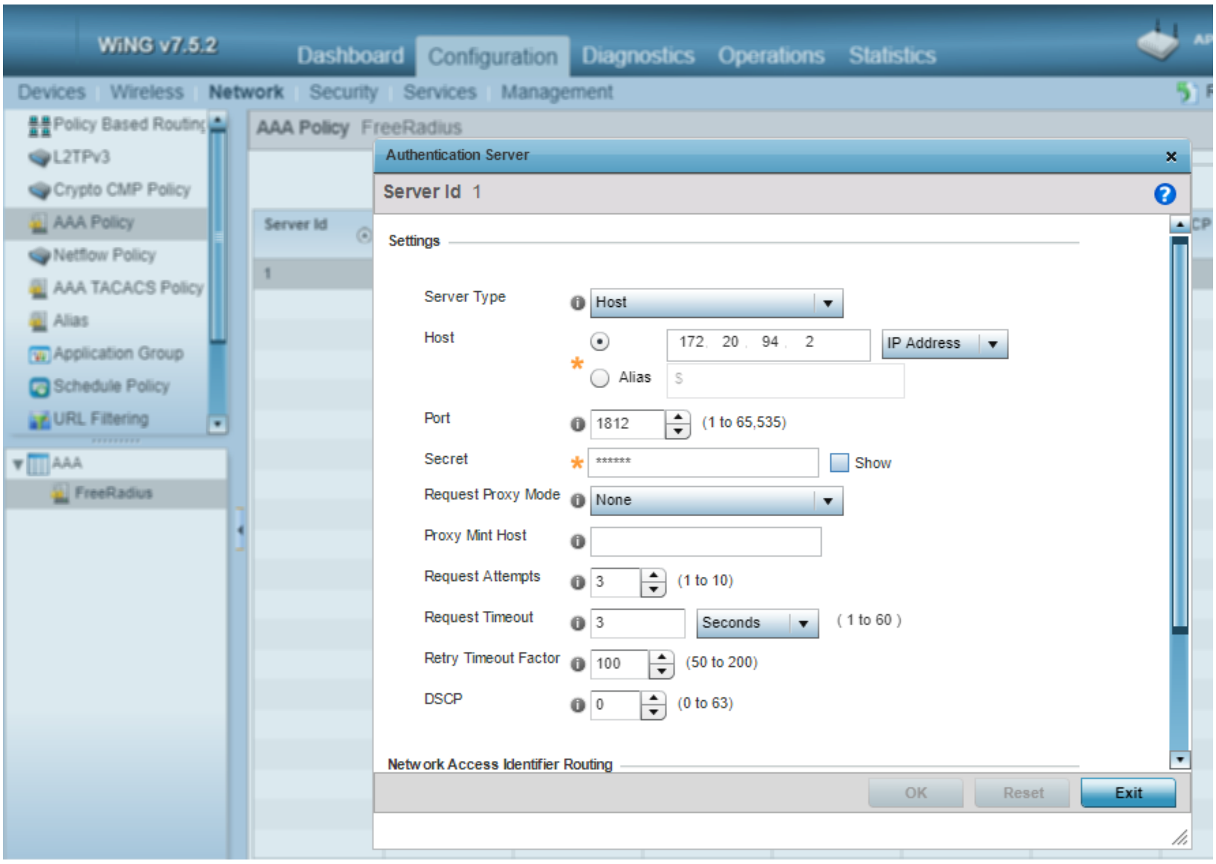
OWE Transition

Owe Companion <none>

WLAN Adbanced settings.

- Make sure Protected management frames is disabled.
- Set 2.4GHz data rates to pre configured set **gn**
  Set 5GHz data rates to **default**
- Its optional but recommended to use Fast BSS transition (802.11r)

SSID/WLAN and Security settings PSK



Authentication Server

Server Id 1

Settings

Server Type: Host

Host: ● 172 . 20 . 94 . 2 IP Address

○ Alias $

Port: 1812 (1 to 65,535)

Secret: ****** □ Show

Request Proxy Mode: None

Proxy Mint Host:

Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

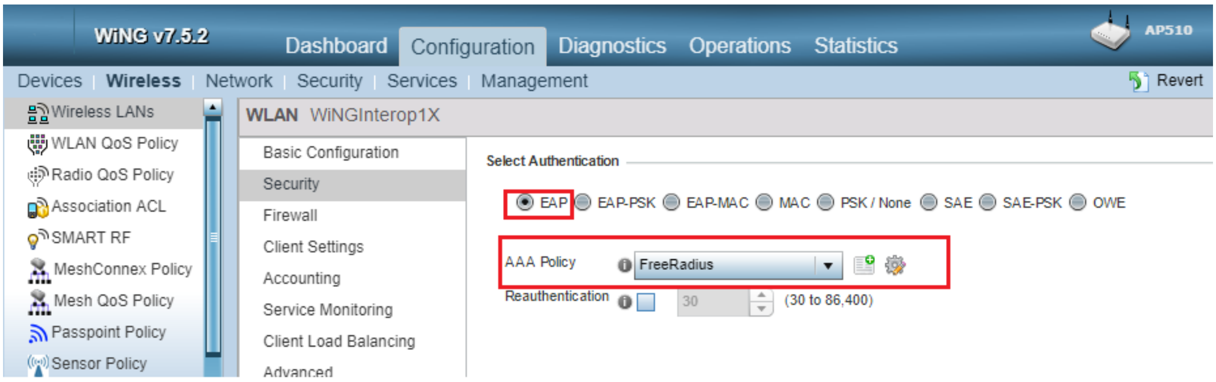
Retry Timeout Factor: 100 (50 to 200)

DSCP: 0 (0 to 63)

Network Access Identifier Routing

Authentication type EAP step 1. Create a Radius policy (**Network /AAA Policy**).

- Configure the IP Address to the Radius server
- Type in the “secret” that corresponds to the secret configured in the Radius server.



WLAN WiNGInterop1X

Select Authentication

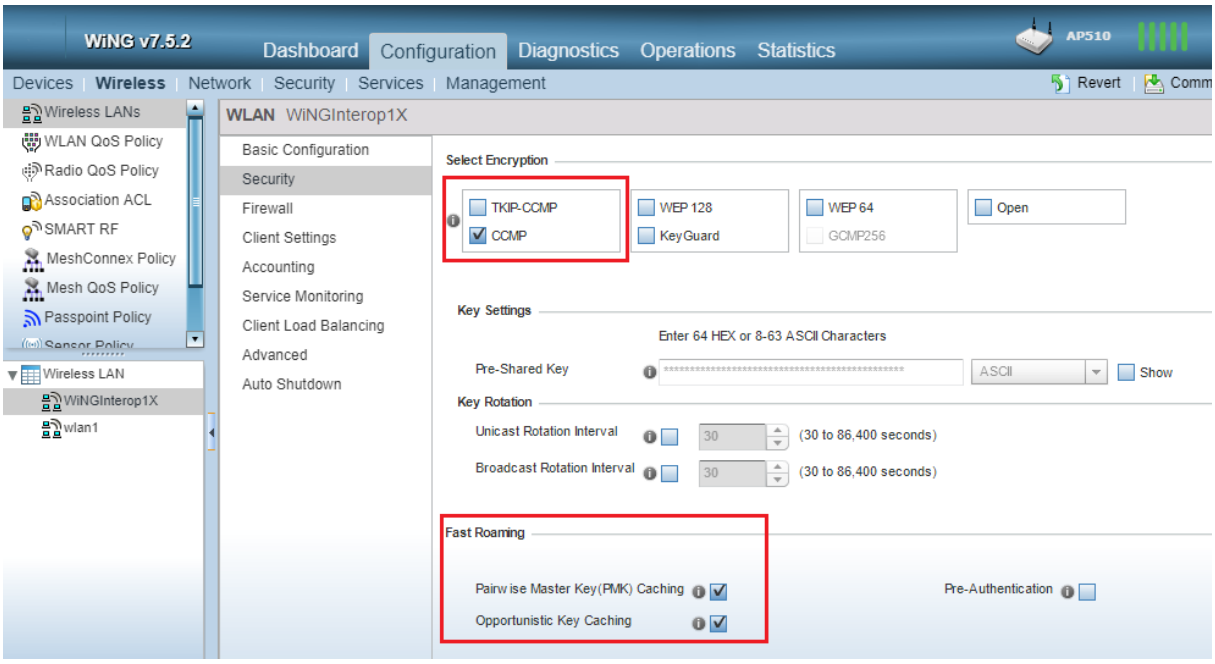
● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ PSK / None ○ SAE ○ SAE-PSK ○ OWE

AAA Policy: FreeRadius

Reauthentication □ 30 (30 to 86,400)

EAP type Authentication. Configure WLAN

- Select Authentication type “EAP”
- Select the previously created AAA Policy (**FreeRadius**).



WLAN WiNGInterop1X

Select Encryption

□ TKIP-CCMP ☑ CCMP □ WEP 128 □ KeyGuard □ WEP 64 □ GCMP256 □ Open

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key ** ASCII □ Show

Key Rotation

Unicast Rotation Interval □ 30 (30 to 86,400 seconds)

Broadcast Rotation Interval □ 30 (30 to 86,400 seconds)

Fast Roaming

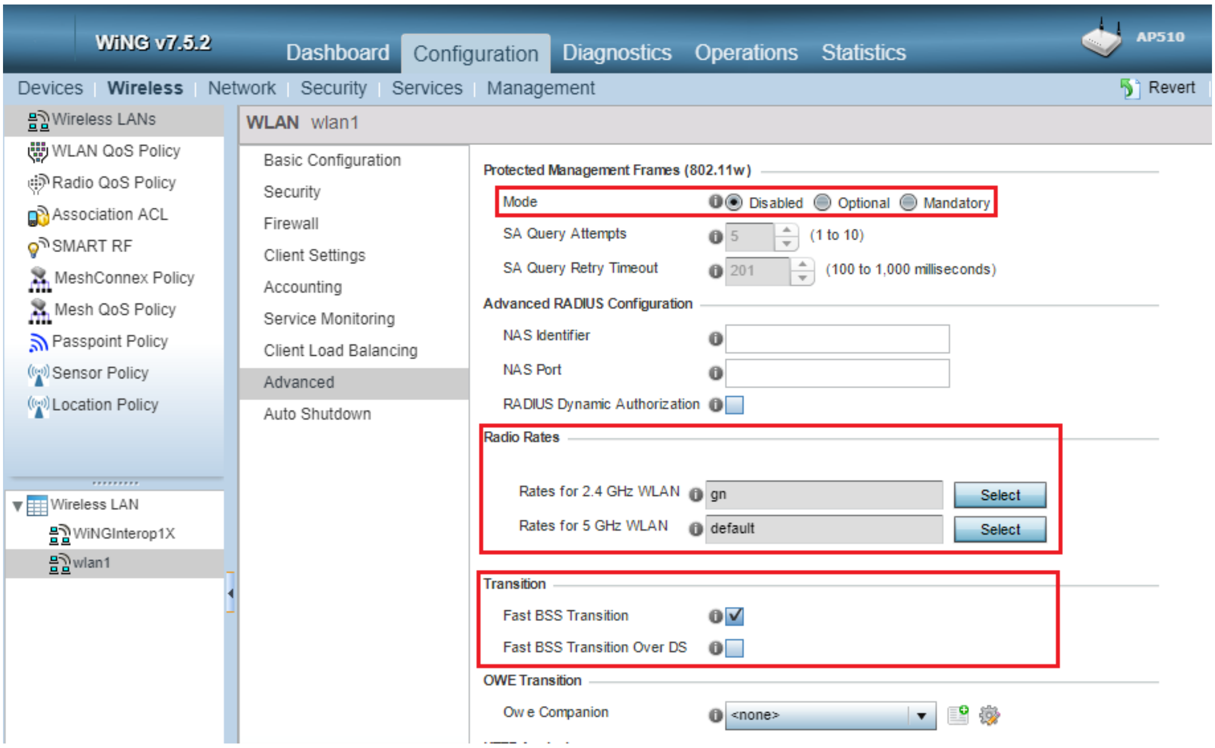
Pairwise Master Key(PMK) Caching ☑

Opportunistic Key Caching ☑

Pre-Authentication □

EAP type Authentication. Configure WLAN continued.

- Select Encrytpion **CCMP**
- Enable PMK caching and Opportunistic Key caching is enabled. (Even if Fast BSS transition (802.11r) described in next step takes precedence its still recommended enable PMK and OKC caching)



WLAN wlan1

Protected Management Frames (802.11w)

Mode ● Disabled ○ Optional ○ Mandatory

SA Query Attempts 5 (1 to 10)

SA Query Retry Timeout 201 (100 to 1,000 milliseconds)

Advanced RADIUS Configuration

NAS Identifier

NAS Port

RADIUS Dynamic Authorization □

Radio Rates

Rates for 2.4 GHz WLAN gn

Rates for 5 GHz WLAN default

Transition

Fast BSS Transition ☑

Fast BSS Transition Over DS □

OWE Transition

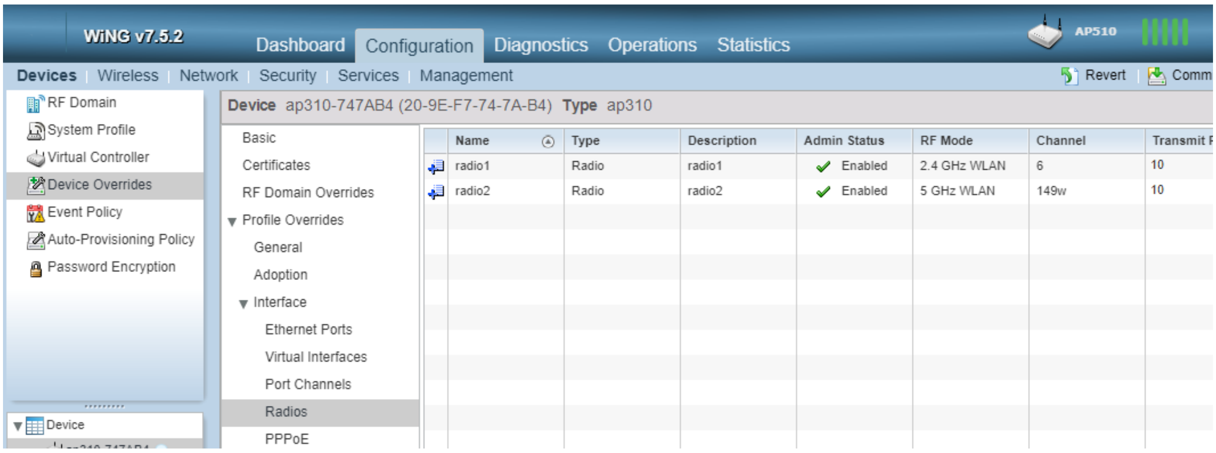
Owe Companion <none>

WLAN Adbanced settings.

- Make sure Protected management frames is disabled.
- Set 2.4GHz data rates to pre configured set **gn**
  Set 5GHz data rates to **default**
- Its optional but highly recommended to use Fast BSS transition (802.11r) especially with EAP authntication.

Data rate configuration (5 Ghz). Wireless-Wireless LANs-Advanced- rates for 5 Ghz WLANs

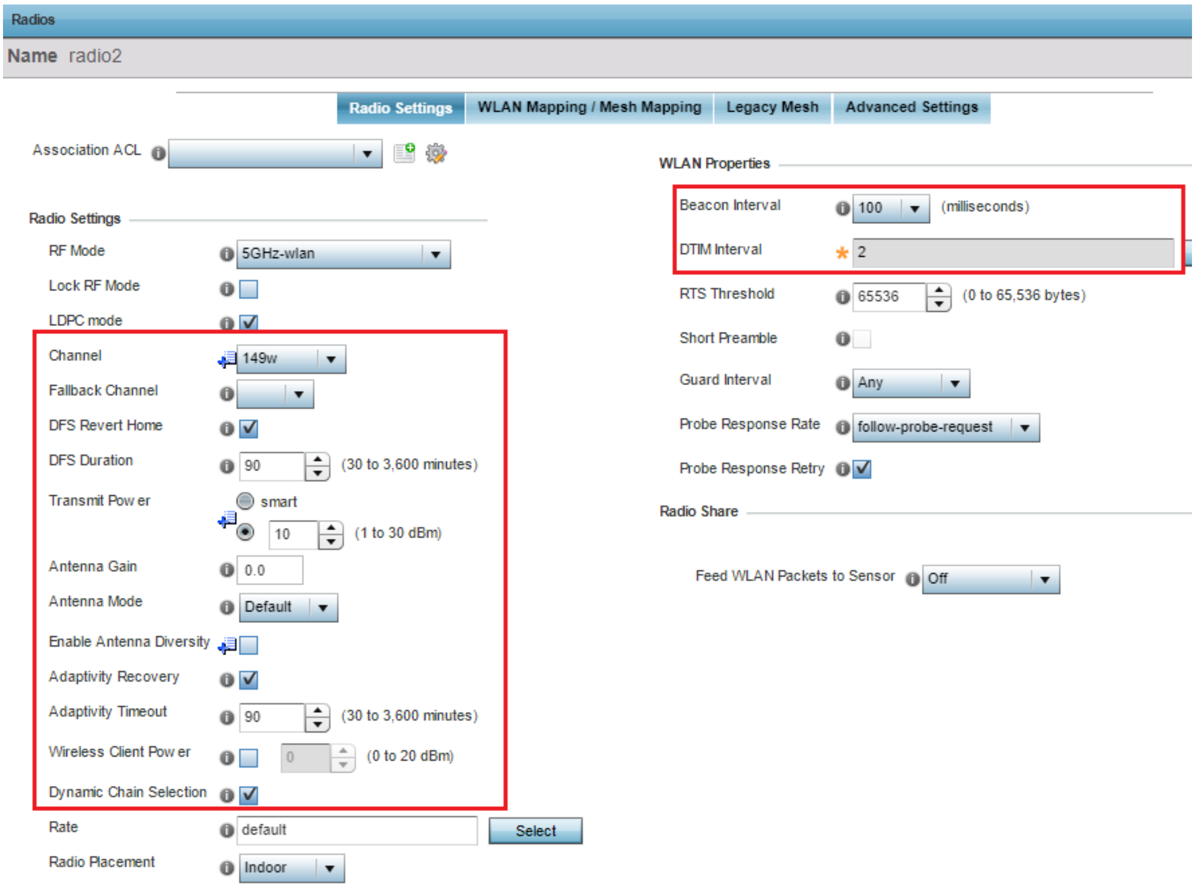
Radio Configuration



Device ap310-747AB4 (20-9E-F7-74-7A-B4) **Type** ap310

Name	Type	Description	Admin Status	RF Mode	Channel	Transmit F
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	6	10
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	149w	10

Radio configuration.



Name radio2

Association ACL

Radio Settings

- RF Mode: 5GHz-wlan
- Lock RF Mode: □
- LDPC mode: ☑
- Channel: 149w
- Fallback Channel:
- DFS Revert Home: ☑
- DFS Duration: 90 (30 to 3,600 minutes)
- Transmit Pow er: ○ smart / ● 10 (1 to 30 dBm)
- Antenna Gain: 0.0
- Antenna Mode: Default
- Enable Antenna Diversity: □
- Adaptivity Recovery: ☑
- Adaptivity Timeout: 90 (30 to 3,600 minutes)
- Wireless Client Pow er: □ 0 (0 to 20 dBm)
- Dynamic Chain Selection: ☑
- Rate: default
- Radio Placement: Indoor

WLAN Properties

- Beacon Interval: 100 (milliseconds)
- DTIM Interval: * 2
- RTS Threshold: 65536 (0 to 65,536 bytes)
- Short Preamble: □
- Guard Interval: Any
- Probe Response Rate: follow-probe-request
- Probe Response Retry: ☑

Radio Share

- Feed WLAN Packets to Sensor: Off

Radio configuration.

- Ascom recommends a Beacon Interval of 100ms and a DTIM period of at least 2 but no higher than 5.
- Make sure Dynamic Chain Selection is enabled. This feature will compensate the power level between single stream client and multi stream clients.

Note that both channel and Tx power was set manually for purpose. Typical deployment use the “Smart” option.

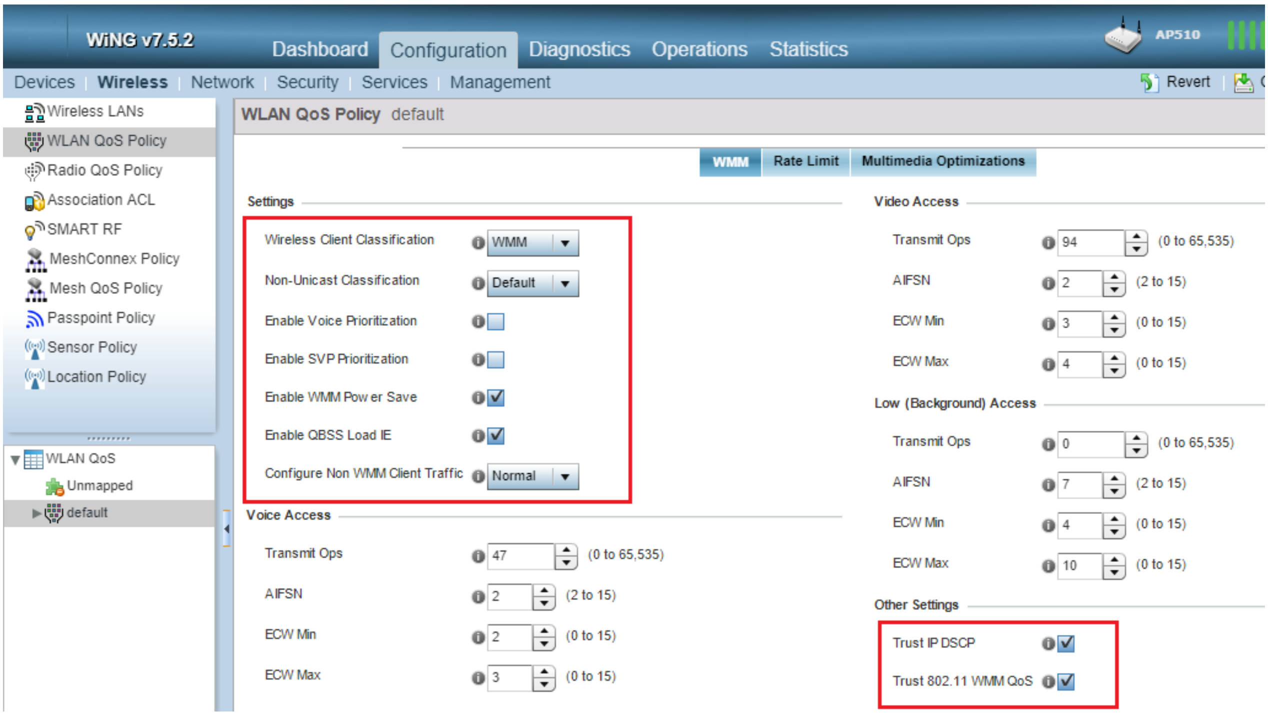
RF Management Policy

- Make sure a 3 –channel plan is used on the 2.4GHz radio
- Note that Tx power level and channel was manually set for test purpose.

General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac/ax environments:

1. **For environments not utilizing 802.11k Neighbor Report - Enabling more than 8 channels will degrade roaming performance. (In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed) Ascom does not recommend exceeding this limit unless 802.11k is in use.**
2. **Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80 MHz channel bonding as it severely reduces the number of available non overlapping channels.**
3. **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)



WLAN QoS Policy default

Settings

Wireless Client Classification: WMM
Non-Unicast Classification: Default
Enable Voice Prioritization: □
Enable SVP Prioritization: □
Enable WMM Pow er Save: ☑
Enable QBSS Load IE: ☑
Configure Non WMM Client Traffic: Normal

Voice Access

Transmit Ops: 47 (0 to 65,535)
AIFSN: 2 (2 to 15)
ECW Min: 2 (0 to 15)
ECW Max: 3 (0 to 15)

Video Access

Transmit Ops: 94 (0 to 65,535)
AIFSN: 2 (2 to 15)
ECW Min: 3 (0 to 15)
ECW Max: 4 (0 to 15)

Low (Background) Access

Transmit Ops: 0 (0 to 65,535)
AIFSN: 7 (2 to 15)
ECW Min: 4 (0 to 15)
ECW Max: 10 (0 to 15)

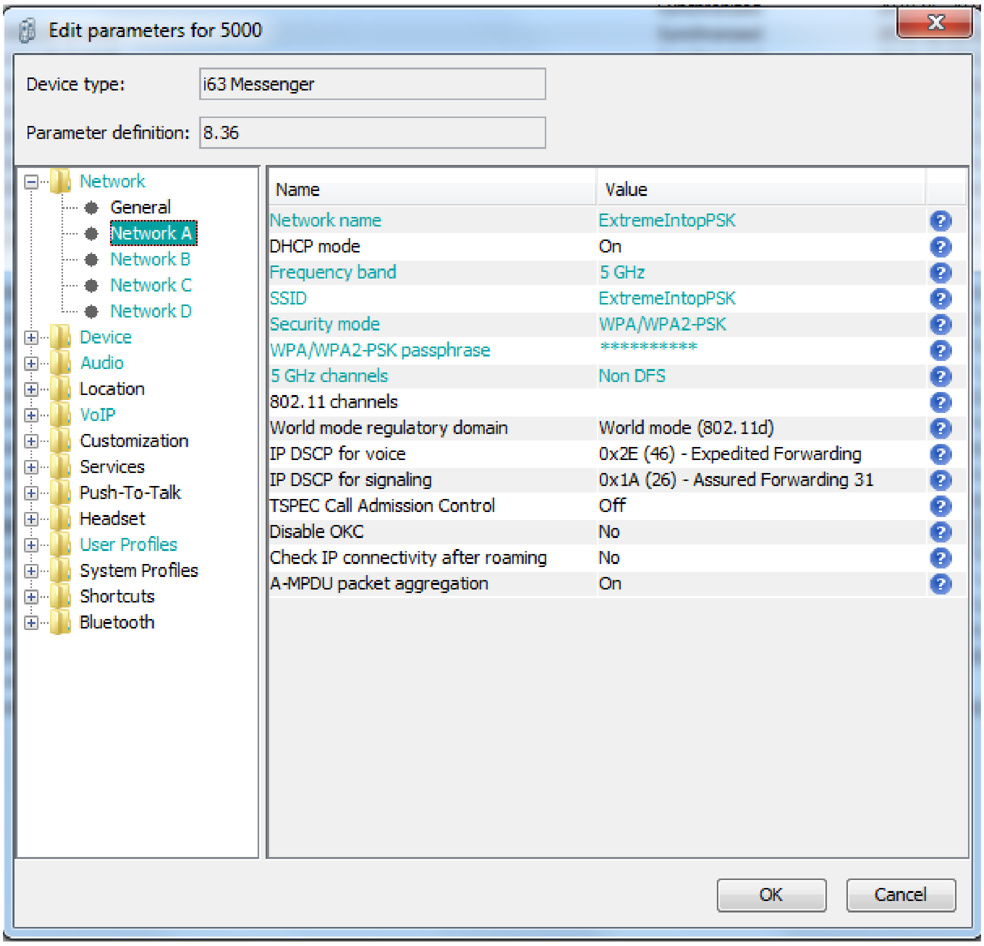
Other Settings

Trust IP DSCP: ☑
Trust 802.11 WMM QoS: ☑

Wireless-WLAN QoS Policy (**Wireless-WLAN QoS Policy**)

- Make sure WMM is selected as Wireless Client Classification.
- Enable WMM Power Save.
- Trust IP DSCP and 802.11 WMM QoS

Ascom i63



Device type: i63 Messenger

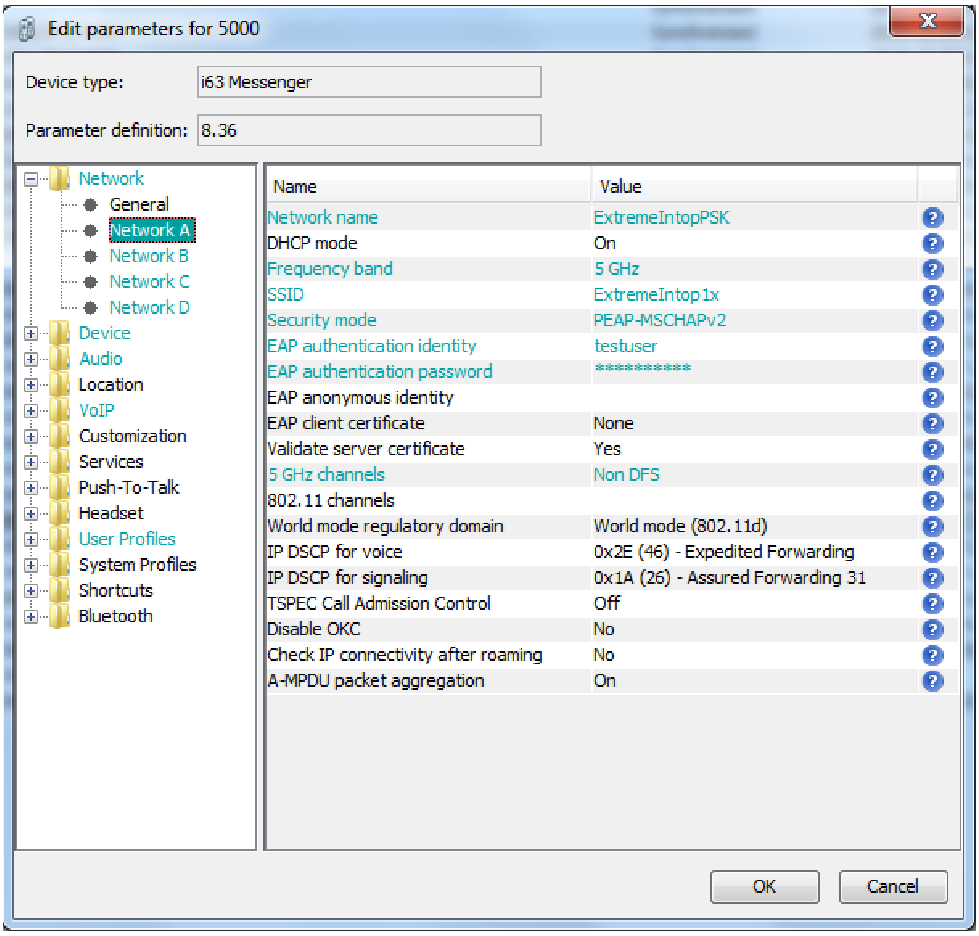
Parameter definition: 8.36

Name	Value
Network name	ExtremeIntopPSK
DHCP mode	On
Frequency band	5 GHz
SSID	ExtremeIntopPSK
Security mode	WPA/WPA2-PSK
WPA/WPA2-PSK passphrase	***********
5 GHz channels	Non DFS
802.11 channels	
World mode regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
Disable OKC	No
Check IP connectivity after roaming	No
A-MPDU packet aggregation	On

Network settings for WPA2-PSK

Note. Make sure that the enabled channels in the i63 handset match the channel plan used in the system.

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



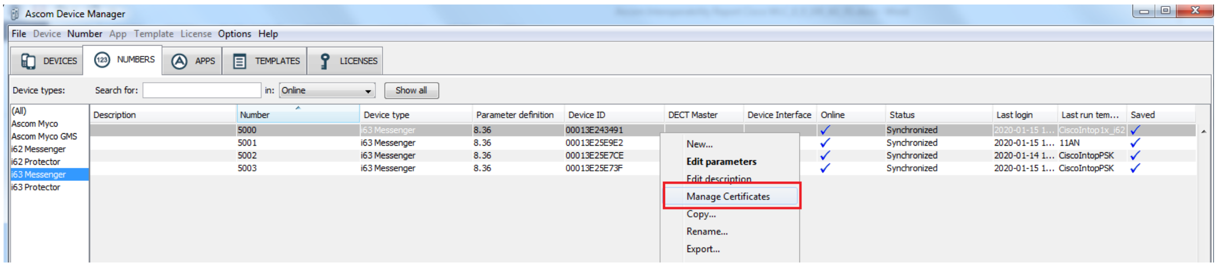
Device type: i63 Messenger

Parameter definition: 8.36

Name	Value
Network name	ExtremeIntopPSK
DHCP mode	On
Frequency band	5 GHz
SSID	ExtremeIntop1x
Security mode	PEAP-MSCHAPv2
EAP authentication identity	testuser
EAP authentication password	***********
EAP anonymous identity	
EAP client certificate	None
Validate server certificate	Yes
5 GHz channels	Non DFS
802.11 channels	
World mode regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
Disable OKC	No
Check IP connectivity after roaming	No
A-MPDU packet aggregation	On

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

Note. Avoid setting 5GHz channels to “802.11k” due to previously described issue (Known Issues)



Device types: Search for: in: Online

Description	Number	Device type	Parameter definition	Device ID	DECT Master	Device Interface	Online	Status	Last login	Last run tem...	Saved
	5000	i63 Messenger	8.36	00013E243491			✓	Synchronized	2020-01-15 1...	CiscoIntop1x_i62	✓
	5001	i63 Messenger	8.36	00013E25E9E2			✓	Synchronized	2020-01-15 1...	11AN	✓
	5002	i63 Messenger	8.36	00013E25E7CE			✓	Synchronized	2020-01-14 1...	CiscoIntopPSK	✓
	5003	i63 Messenger	8.36	00013E25E73F			✓	Synchronized	2020-01-15 1...	CiscoIntopPSK	✓

802.1X Authentication requires a CA certificate to be uploaded to the phone by “right clicking” - > Edit certificates. EAP-TLS will require both a CA and a client certificate.

Note that both a CA and a client certificate are needed for TLS. Otherwise only a CA certificate is needed.

Appendix B: Interoperability Verification Records

Pass	19
Fail	1
Comments	2
Not verified	3
Total	25

Refer to the attached file for detailed verification results.

Refer to the verification specification for explicit information regarding each verification case.
The specification can be found here (requires login):
https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability/Templates/

Document History

Rev	Date	Author	Description
P1	12-April-2021	SEKMO	Draft
R1	23-April-2021	SEKMO	Corrections after review