

INTEROPERABILITY REPORT

Ascom i63  
Extreme Networks

Cloud platform

v. 10.2.4.0 (AP)

Ascom i63 v. 2.2.8

Morrisville, NC, USA

Jan 2021

**ascom**

# Contents

<b>Introduction</b> .....	<b>3</b>
About Ascom.....	3
About Extreme Networks .....	3
Verification site.....	4
Participants .....	4
Verification topology.....	4
<b>Summary</b> .....	<b>5</b>
General conclusions .....	5
Verification overview .....	6
Known limitations.....	7
<b>Appendix A: Verification Configurations</b> .....	<b>8</b>
<i>Extreme Networks Cloud and Access Points configurations</i> .....	8
Ascom i63 .....	19
<b>Appendix B: Interoperability Verification Records</b> .....	<b>21</b>
<b>Document History</b> .....	<b>21</b>

# Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Aerohive networks platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Aerohive Networks's 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 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) delivers software-driven networking solutions from the wireless and IoT edge to the data center that are agile, adaptive, and secure to enable the digital transformation of our enterprise customers. 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

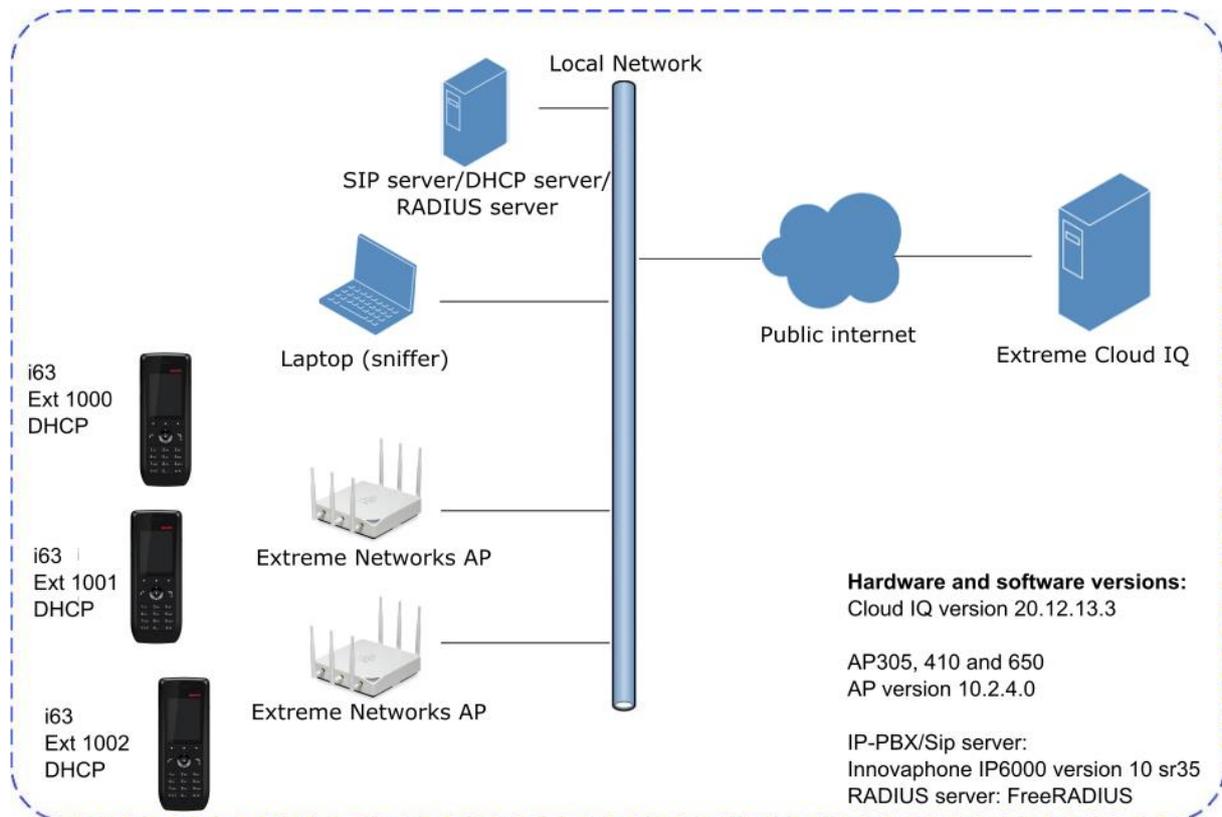
## Verification site

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

## Participants

Karl-Magnus Olsson, Ascom, Morrisville

## Verification topology



# Summary

## General conclusions

The result of the verified test areas, such as authentication, association, handover and call stability test, produced very good results. The roaming times for PSK, 802.1x (FT and non-FT) were excellent and were in the range of 30 ms for all combinations.

## Compatibility information

One Access point model from every product generation/product group has been selected as a representation (305, 410 and 650). By testing these access points we are considered cover all below listed access point models

### Supported Partner Access Points running version 10.2.4.0:

305c/305cx

410c

460c

510c/510cx

650/650x

## 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	Avg. typical roaming time 32 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Avg. typical roaming time 26 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK *	Avg. typical roaming time 28 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Avg. typical roaming time 28 ms

Average roaming times are measured using on the 5GHz band. 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
Authentication with 802.11w (Protected Management Frames) does not work in conjunction with 802.11r	Disable Protected Management Frames in system.	WH2-2356
Call Admission Control not working in conjunction with 802.11w (Protected Management Frames)	Disable Protected Management Frames in system.	WH2-2363

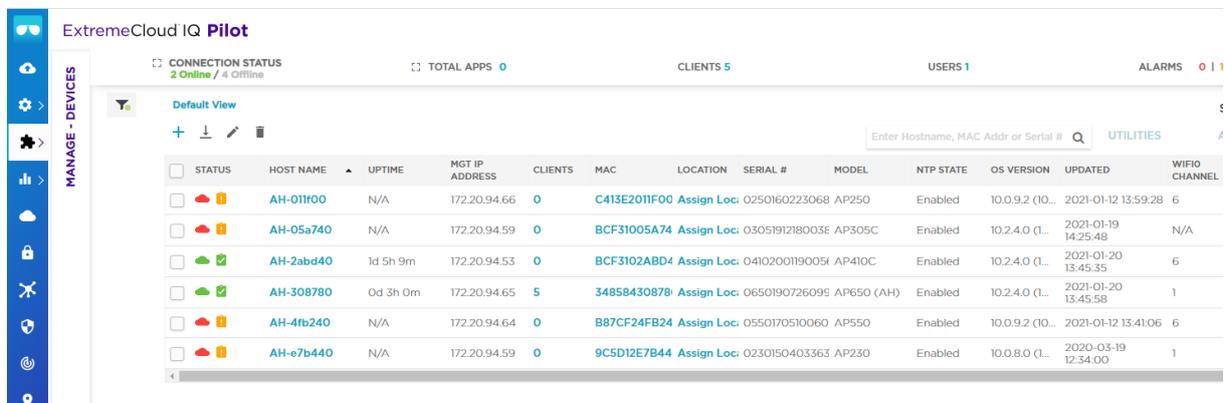
# Appendix A: Verification Configurations

## Extreme Networks Cloud and Access Points configurations.

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

The configuration file is found at the bottom of this chapter.

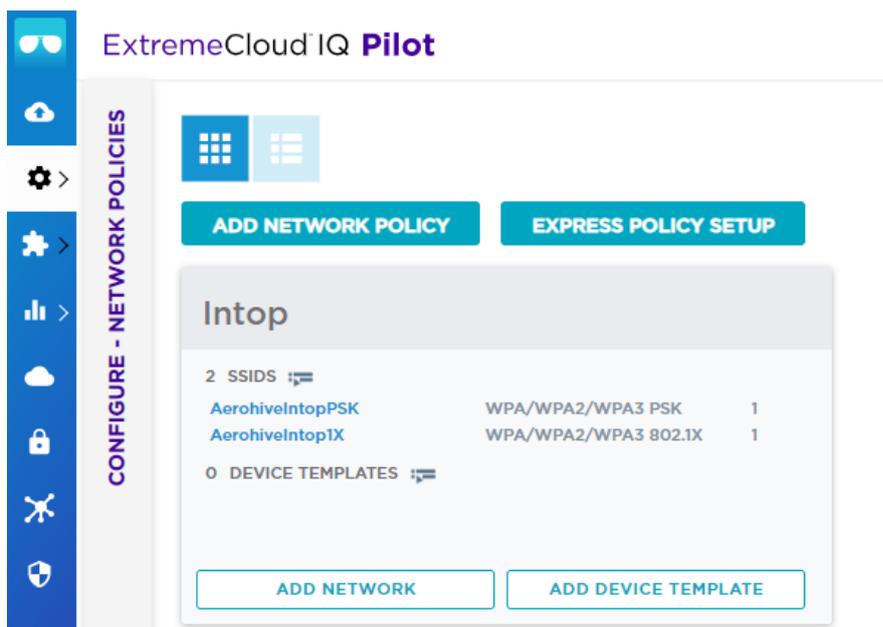
### ESS, Security settings.



The screenshot shows the 'ExtremeCloud IQ Pilot' dashboard. At the top, it displays 'CONNECTION STATUS' with '2 Online / 4 Offline', 'TOTAL APPS 0', 'CLIENTS 5', 'USERS 1', and 'ALARMS 0 | 1'. Below this is a table of active access points. The table has columns for STATUS, HOST NAME, UPTIME, MGT IP ADDRESS, CLIENTS, MAC, LOCATION, SERIAL #, MODEL, NTP STATE, OS VERSION, UPDATED, and WIFI CHANNEL. There are 7 rows of data.

STATUS	HOST NAME	UPTIME	MGT IP ADDRESS	CLIENTS	MAC	LOCATION	SERIAL #	MODEL	NTP STATE	OS VERSION	UPDATED	WIFI CHANNEL
	AH-011F00	N/A	172.20.94.66	0	C413E2011F00	Assign Loc: 0250160223068	AP250	Enabled	10.0.9.2 (10...	2021-01-12 13:59:28	6	
	AH-05a740	N/A	172.20.94.59	0	BCF31005A74	Assign Loc: 0305191218003E	AP305C	Enabled	10.2.4.0 (L...	2021-01-19 14:25:48	N/A	
	AH-2abd40	1d 5h 9m	172.20.94.53	0	BCF3102ABD4	Assign Loc: 04102001190054	AP410C	Enabled	10.2.4.0 (L...	2021-01-20 13:45:35	6	
	AH-308780	0d 3h 0m	172.20.94.65	5	34858430878	Assign Loc: 0650190726099	AP650 (AH)	Enabled	10.2.4.0 (L...	2021-01-20 13:45:58	1	
	AH-4fb240	N/A	172.20.94.64	0	B87CF24FB24	Assign Loc: 0550170510060	AP550	Enabled	10.0.9.2 (10...	2021-01-12 13:41:06	6	
	AH-e7b440	N/A	172.20.94.59	0	9C5D12E7B44	Assign Loc: 0230150403363	AP230	Enabled	10.0.8.0 (L...	2020-03-19 12:34:00	1	

Dashboard overview (Monitor) of active access points



The screenshot shows the 'ExtremeCloud IQ Pilot' configuration page for 'NETWORK POLICIES'. It features two main buttons: 'ADD NETWORK POLICY' and 'EXPRESS POLICY SETUP'. Below these is a card for a policy named 'Intop'. The card shows '2 SSIDS' and '0 DEVICE TEMPLATES'. The SSIDs are listed with their security protocols and counts.

SSID	Security Protocol	Count
AerohiveIntopPSK	WPA/WPA2/WPA3 PSK	1
AerohiveIntop1X	WPA/WPA2/WPA3 802.1X	1

List of all configured SSIDs

ExtremeCloud IQ **Pilot**

Network Policies > Intop > All SSIDs > AerohiveIntopPSK

POLICY DETAILS    **WIRELESS NETWORKS**    DEVICE TEMPLATES    ROUTER SETTINGS    ADDITIONAL SETTINGS    DEPLOY POLICY

CONFIGURATION GUIDE

Policy Name: Intop

Name (SSID) \* : AerohiveIntopPSK

Broadcast Name \* : AerohiveIntopPSK

Broadcast SSID Using

- WiFi Radio (2.4 GHz or 5 GHz)
- WiFi Radio (5 GHz only)

SSID Usage

SSID AUTHENTICATION    MAC AUTHENTICATION

Enterprise WPA / WPA2 / WPA3    **Personal WPA / WPA2 / WPA3**    Private Pre-Shared Key    WEP

Key Management: WPA2-(WPA2 Personal)-PSK

Encryption Method: CCMP (AES)

Key Type: ASCII Key

Key Value \* : ..... 8-63 characters

Show Password

Enable Captive Web Portal  OFF

WPA2 PSK (Personal)

- Select WPA/WPA2 PSK (Personal)
- Select WPA2-PSK and CCMP and Key Management and Encryption Method
- Key can be entered in HEX or in ASCII format. Example shows a key entered in ASCII format.

ExtremeCloud IQ Pilot

POLICY DETAILS WIRELESS NETWORKS DEVICE TEMPLATES ROUTER SETTINGS ADDITIONAL SETTINGS DEPLOY POLICY

CONFIGURATION GUIDE

Policy Name Intop

RADIUS Server Group FreeRADIUS

Wireless Network

Name (SSID) \* AerohiveIntop1X

Broadcast SSID Using

WiFi Radio (2.4 GHz or 5 GHz)

WiFi1 Radio (5 GHz only)

Broadcast Name \* AerohiveIntop1X

SSID Usage

SSID AUTHENTICATION MAC AUTHENTICATION

Enterprise WPA / WPA2 / WPA3

Personal WPA / WPA2 / WPA3

Private Pre-Shared Key

WEP

Key Management WPA2-802.1X

Encryption Method CCMP (AES)

Enable Captive Web Portal OFF

Authentication Settings

Authentication with ExtremeCloud IQ Authentication Service OFF

Authenticate via RADIUS Server

Default RADIUS Server FreeRADIUS

Name	Type	IP/Host Name
FreeRADIUS	External RADIUS Server	172.20.94.2

WPA2 802.1X (Enterprise)

- Select WPA/WPA2 802.1X (Enterprise)
- Select WPA2-802.1X and CCMP and Key Management and Encryption Method
- Select RADIUS server (defined in step below)

## Advanced Access Security Settings

WPA2  
802.1X



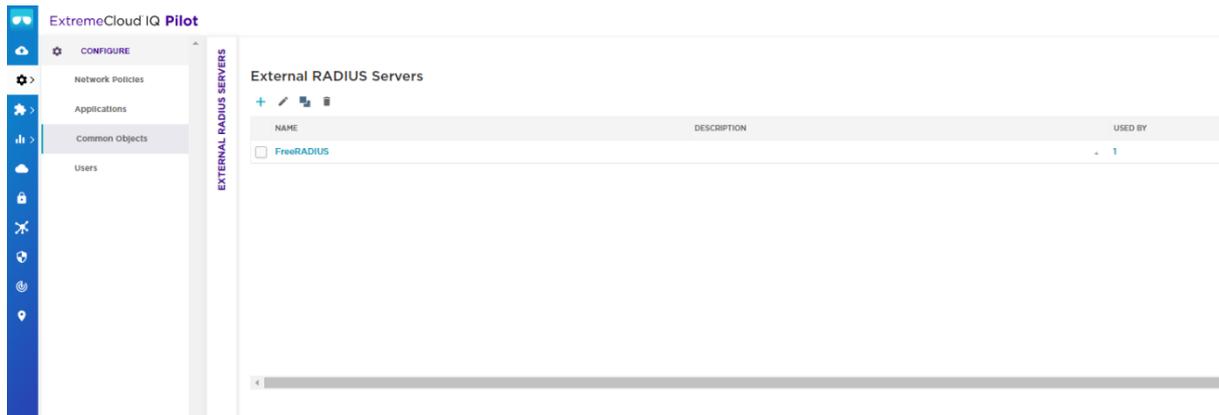
**802.11w**  
Prevents forgery and retransmission of management frames

### Advanced Authentication Options

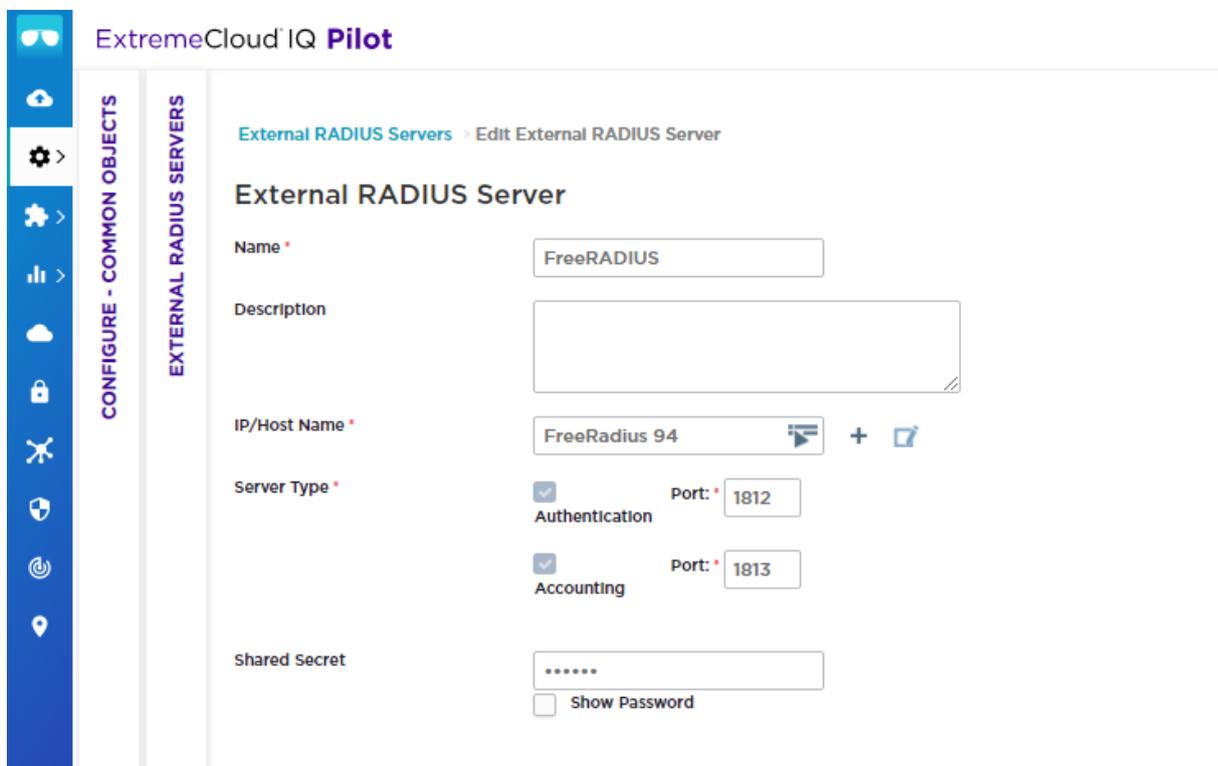
<input type="checkbox"/> Generate new Group Master key (GMK) after	<input type="text" value="0"/>	Seconds
<input type="checkbox"/> Generate new Group Temporal key (GTK) after	<input type="text" value="0"/>	Seconds
GTK timeout period	<input type="text" value="4000"/>	Milliseconds
Number of GTK retries	<input type="text" value="3"/>	
<input type="checkbox"/> Generate a new Pairwise Transient Key (PTK) after	<input type="text" value="0"/>	Seconds
PTK timeout period	<input type="text" value="4000"/>	Milliseconds
Number of PTK retries	<input type="text" value="3"/>	
Replay window	<input type="text" value="0"/>	
<input type="checkbox"/> Force the user to reauthenticate after	<input type="text" value="0"/>	Seconds
<input checked="" type="checkbox"/> Local TKIP Countermeasure		
<input checked="" type="checkbox"/> Remote TKIP Countermeasure		
<input checked="" type="checkbox"/> Refresh GTK when the client disassociates from the SSID		
<input type="checkbox"/> Enable Preauthentication (accelerates roaming)		
<input checked="" type="checkbox"/> Enable proactive PMK-ID response (uses cached PMKs to supports fast roaming with certain clients)		

(Enterprise) - Additional settings - Advanced Access Security Controls

- Make sure that Enable Proactive PMK ID response is checked. (Not needed if 802.11r/FT is enabled)



WPA2 802.1X (Enterprise) – RADIUS configuration



WPA2 802.1X (Enterprise) – RADIUS configuration

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

### Additional Settings ▾

Configure your Availability Scheduling, Security Controls, Optional Settings, and Client Monitoring

SSID Availability Schedule	<input type="checkbox"/> Restrict the availability of this SSID to selected schedules	CUSTOMIZE
Advanced Access Security Controls	802.11w, Authentication timeout options	CUSTOMIZE
Optional Settings	Radio and Rates, DoS Prevention, and MAC filters	CUSTOMIZE
Client Monitor	<input checked="" type="checkbox"/> ON	

*When enabled, Aerohive devices detect client issues, report client connection activities and problems to HiveManager.*

Data rate configuration. (Per SSID)

- Go to optional Settings

### Optional Settings ✕

bgRateSetting

Customize 2.4 GHz 11 b/g Rate Setting

1 Mbps	N/A	9 Mbps	N/A	24 Mbps	Optional
2 Mbps	N/A	11 Mbps	N/A	36 Mbps	Optional
5.5 Mbps	N/A	12 Mbps	Basic	48 Mbps	Optional
6 Mbps	N/A	18 Mbps	Optional	54 Mbps	Optional

Data rate configuration.2.4GHz

- To improve the performance in the wireless system it is recommended to disable the lowest data rates.

## Optional Settings



aRateSetting

Customize 5.0 GHz 11a Rate Setting

6 Mbps	<input type="text" value="N/A"/>	24 Mbps	<input type="text" value="Basic"/>
9 Mbps	<input type="text" value="N/A"/>	36 Mbps	<input type="text" value="Optional"/>
12 Mbps	<input type="text" value="Basic"/>	48 Mbps	<input type="text" value="Optional"/>
18 Mbps	<input type="text" value="Optional"/>	54 Mbps	<input type="text" value="Optional"/>

CANCEL

SAVE RATE SETTING

### Data rate configuration.5GHz

- To improve the performance in the wireless system it is recommended to disable the lowest data rates.

## Optional Settings



### Voice Enterprise

Enable voice enterprise  
Voice Enterprise is not supported on AP110, AP120, AP170, AP320, AP340, AP370, and AP390

Custom

Enable 802.11k  
 Enable dualband neighbor list  
Max. neighbor APs:   
Range: 1 - 10

Enable 802.11v  
 Enable forced disassociation

Enable 802.11r

For a complete list of certified platforms, see [Voice Enterprise](#) in the online Help system.

### WMM

Enable WMM

Enforce WMM admission control for

Voice  
 Video

For a complete list of certified platforms, see [WMM-AC](#) in the online Help system.

Enable unscheduled automatic power save delivery

### Broadcast and Multicast Handling

Convert IP Multicast to Unicast

Channel utilization threshold  
  
Range: 1 - 100

Membership count threshold  
  
Range: 1 - 30

Enable Non-Essential Broadcast Filtering  
 Enable Multicast Drop

### Client Related Network Settings

Maximum client limit <input type="text" value="100"/> <small>Range: 1 - 255</small>	EAP timeout <input type="text" value="30"/> Seconds <small>Range: 5 - 300</small>	RTS threshold <input type="text" value="2346"/> bytes <small>Range: 1 - 2346</small>
Fragment threshold <input type="text" value="2346"/> bytes <small>Range: 256 - 2346</small>	<b>DTIM settings</b> <input type="text" value="2"/> <small>Range: 1 - 255</small>	Inactive client ageout <input type="text" value="5"/> Minutes <small>Range: 1 - 30</small>
EAP retries <input type="text" value="3"/> <small>Range: 1 - 5</small>	Roaming cache update interval <input type="text" value="60"/> Seconds <small>Range: 10 - 36000</small>	Roaming cache ageout <input type="text" value="60"/> <small>Range: 1 - 1000</small>
Local cache timeout		

CANCEL **SAVE OPTIONAL SETTINGS**

## Optional SSID settings

- Enable 802.11k support.
- Enable 802.11v support. (Enable 802.11v support. (802.11v is not really needed for i63, but still recommended if mixing with other Ascom products))
- It is strongly recommended to use Fast Transition (802.11r) for enhanced roaming performance.
  
- Make sure Enable WMM is checked.
- Make sure Unscheduled Automatic Power Save Delivery is checked.
- Make sure “Convert IP Multicast to Unicast” is enabled
  
- Ascom recommends a DTIM period of at least 2 but no higher than 5.

## Quality of Service (QoS)

ExtremeCloud IQ Pilot

Classifier Maps > Classifier Maps

### Classifier Maps

Please note that Classifier Maps are only supported by IQ Engine devices and will not take effect on other devices.

Name:

Description:

SERVICES    MAC OUIs    SSIDs    **802.1p/DiffServ/802.11e**

OFF 802.1p		ON DiffServ		OFF 802.11e	
802.1p	QoS Class	DiffServ	QoS Class	802.11e	QoS Class
7	Network Control	56-63	Network Control	7	Network Control
6	Voice	48-55	Voice	6	Voice
5	Video	40-47	Voice	5	Video
4	Controlled Load	32-39	Controlled Load	4	Controlled Load
3	Excellent Effort	24-31	Excellent Effort	3	Excellent Effort
0	Best Effort 1	00-07	Best Effort 1	0	Best Effort 1
2	Best Effort 2	16-23	Best Effort 2	2	Best Effort 2
1	Background	08-15	Background	1	Background

### Classifier Maps

- Create classifier map according to the screenshot and enable DiffServ and 802.11e
- **Important. For DiffServ 40-47 select QoS Class: 6 – Voice.**



CONFIGURE - COMMON OBJECTS

MARKER MAPS

Marker Maps > Ascom

### Ascom

Please note that Marker Maps are only supported by IQ Engine devices and will not take effect on other devices.

Name

Description

802.1p

DiffServ

DiffServ



note: If both 802.1p and DiffServ are selected only DiffServ will take effect

QoS Class	WMM Queue	DiffServ Code Points
7 - Network Control	Voice	<input type="text" value="56"/>
6 - Voice	Voice	<input type="text" value="46"/>
5 - Video	Video	<input type="text" value="40"/>
4 - Controlled Load	Video	<input type="text" value="32"/>
3 - Excellent Effort	Best Effort	<input type="text" value="24"/>
2 - Best Effort 1	Best Effort	<input type="text" value="0"/>
1 - Best Effort 2	Background	<input type="text" value="16"/>
0 - Background	Background	<input type="text" value="8"/>

#### Marker Maps

- Create a Marker Map and assign QoS Class 6 - voice to 46

## Radio Configuration

The screenshot displays the configuration page for an access point (AP) named AH-2abd40. The interface is divided into several sections:

- LOCATION:** Assign Location. The AP is identified as AP410C. Host Name: AH-2abd40, Policy: Intop.
- Real-Time Data:** CPU Usage: 2%, Memory Usage: 39%.
- CONFIGURATION:** Device Configuration, Interface Settings, Device Credentials, Configure Netdump.
- ADDITIONAL SETTINGS:** DHCP Server and Relay, Neighboring Devices, Bonjour Gateway Settings, Troubleshooting, SSH.
- Wireless Interfaces:** Control actions from the Access Point's Wi-Fi ports. The WiFi1 interface is selected.
- Radio Status:** Radio Status: ON, Radio Mode: 802.11ax\_5g, Radio Profile: radio\_ng\_11ax-5g.
- Radio Usage:** Client Access: checked, Backhaul Mesh Link: unchecked, Sensor: unchecked.
- Channel:** 36.
- Transmission Power:** Auto: unchecked, Manual: checked. A slider shows 8 dBm.
- Enable client transmission power control (802.11h):** unchecked.
- Enable Presence Analytics:** OFF.
- SSIDs:** A table with columns: SSID Name (Policy), Status, Override SSID Broadcast Name, Override PSK Password, Reassign CWP. One entry is shown: AerohiveIntopPSK, Status: ON, Broadcast Name: AerohiveIntopPSK, PSK Password: \*\*\*\*\*.

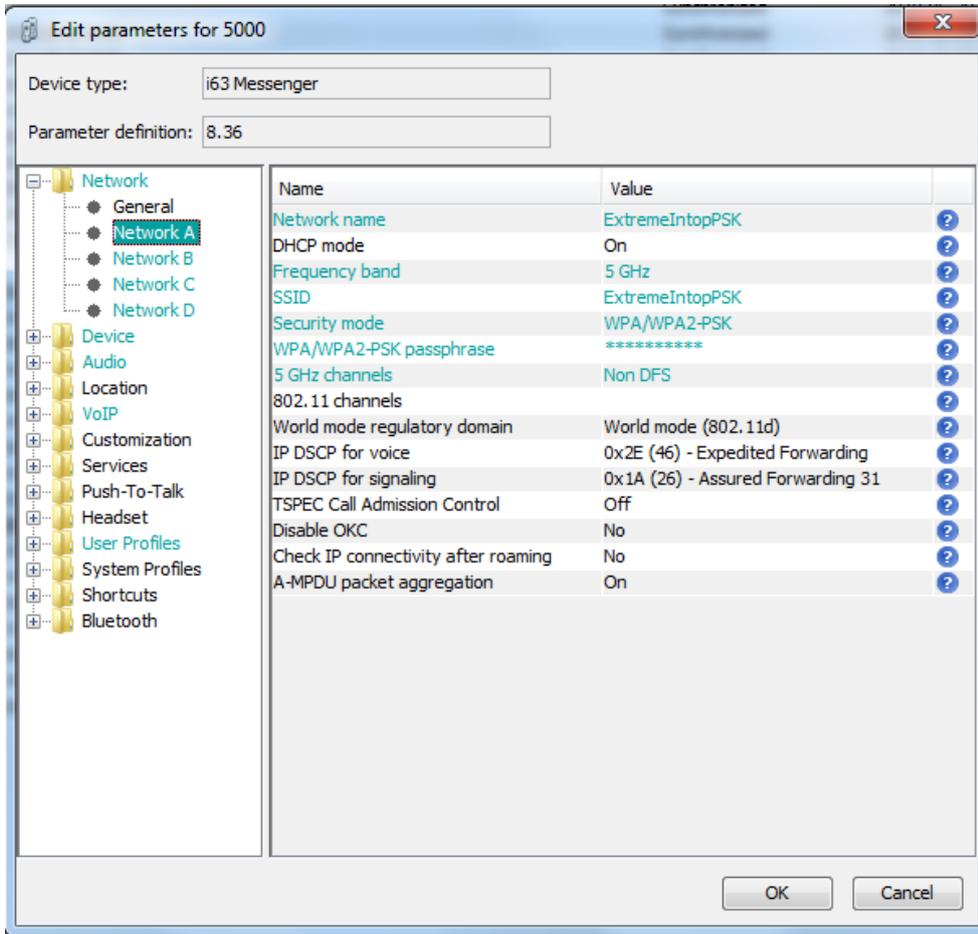
### Configuration of access points

- Radio profiles used is the default (Default radio profiles **radio\_ng\_11ax-5g** and **radio\_ng\_11ax-2g** for WiFi0 interface).
- In the example channel and Transmission power has been set manually for each access point (for testing).

### General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac 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.

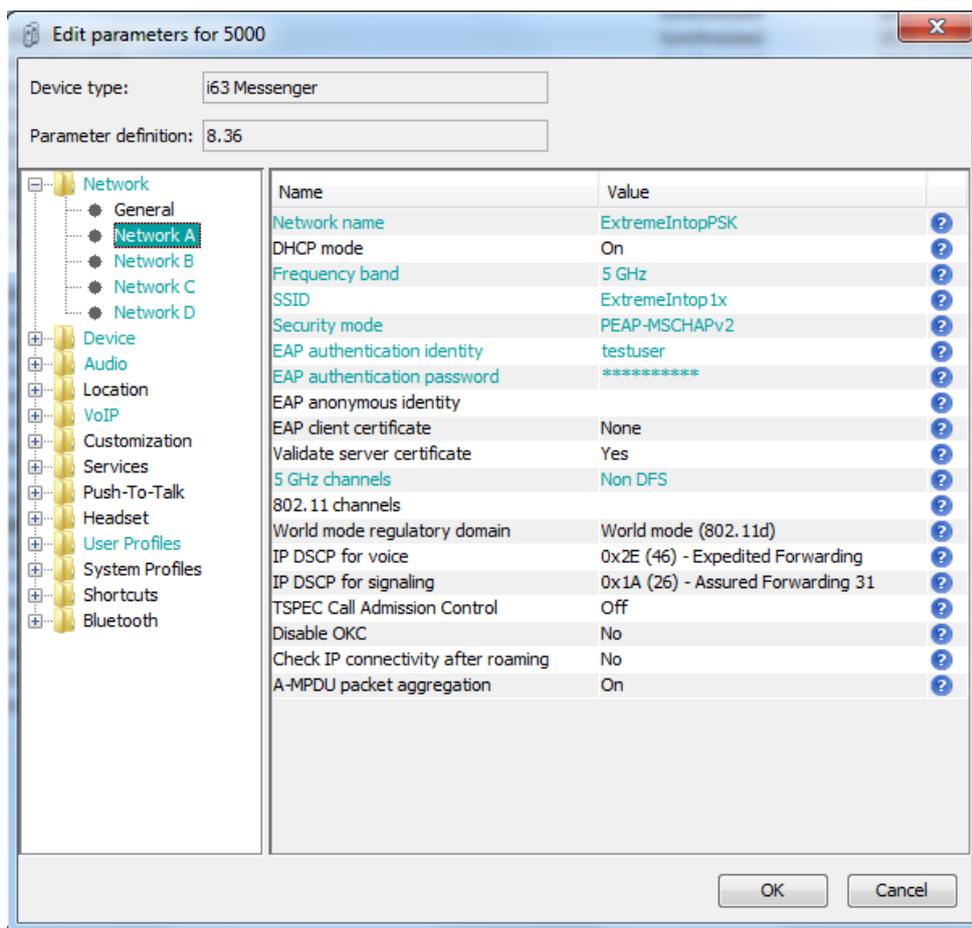
\*) Dynamic Frequency Selection (radar detection)



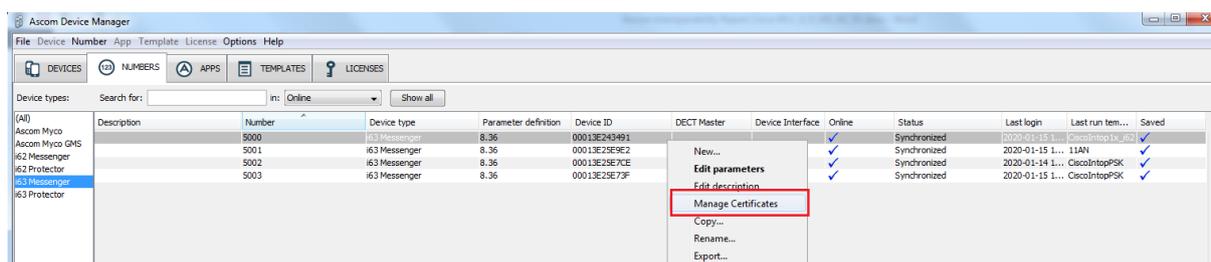
Network settings for WPA2-PSK

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".



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



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	18
Fail	0
Comments	4
Not verified	4
<b>Total</b>	26

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	26-Jan-21	SEKMO	Draft
R1	02-Feb-21	SEKMO	Minor corrections after review.