

INTEROPERABILITY REPORT

Ascom i63
Extreme Networks

Wireless platform

v. 10.51.10

Ascom i63 v. 1.0.8

Morrisville, NC, USA

Feb 2020

ascom

Contents

Introduction	Error! Bookmark not defined.
About Ascom.....	Error! Bookmark not defined.
About Extreme Networks	3
Site Information	Error! Bookmark not defined.
Verification site.....	4
Participants	4
Summary	5
General conclusions	5
Compatibility information	5
Verification overview	6
Known limitations.....	7
Appendix A: Verification Configurations	8
Extreme Networks V2110 Controller v. 10.51.10	8
Ascom i63	23
Appendix B: Detailed Verification Records	25
Document History	25

Site Information

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

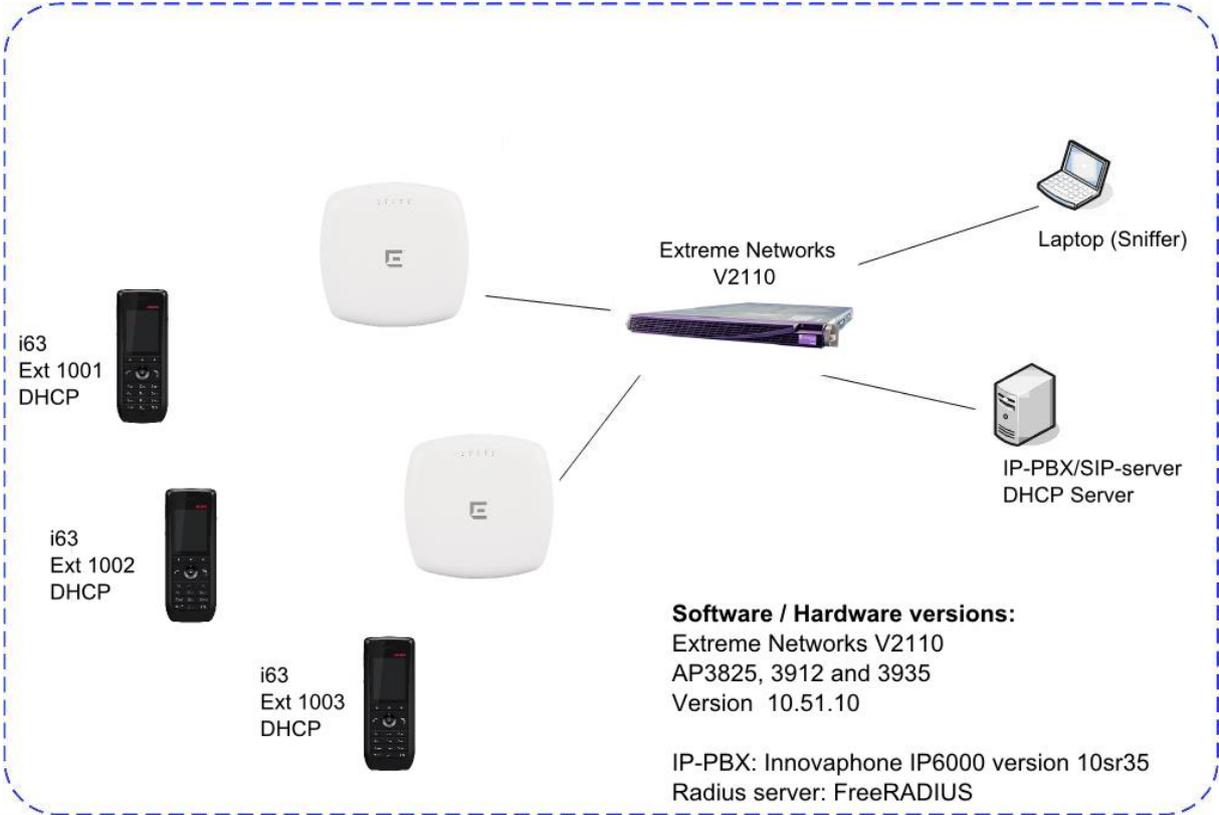
Verification site

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 even though a couple of less severe issues were observed (documented under Known Limitations section)

Roaming times were measured in the range of around 50ms when using both WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES) and around 30ms when using 802.11r/FT together with PEAP-MSCHAPv2.

The majority of the test cases were performed in B@AP mode.

Compatibility information

Based on the test of 3825, 3912 and 3935 we consider following list of access point models to be covered.

Supported Partner Access Points with Extreme Networks version 10.51.10:

AP3801, 3805, 3825, 3865

AP 3912, 3915, 3935

Supported controller platforms with Extreme Networks 10.51.10:

C25

C35

V2110

C5110

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 44 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	N/A	802.11r not supported with PSK
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK **	Typical roaming time 45 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 28ms

Average roaming times are measured using 802.11a/n. 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
Open authentication not working. To be corrected in next Ascom i63 release.		WH2-2382
Authentication with 802.11w (Protected Management Frames) does not work in conjunction with 802.11r	Disable or set Protected Management Frames to optional in the Cisco WLC	WH2-2356
Call Admission Control not working in conjunction with 802.11w (Protected Management Frames)	Disable Protected Management Frames in the Cisco WLC if CAC is being used.	WH2-2363
2 second delay before call is set up when Call Admission Control is enabled.		WH2-2362

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

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

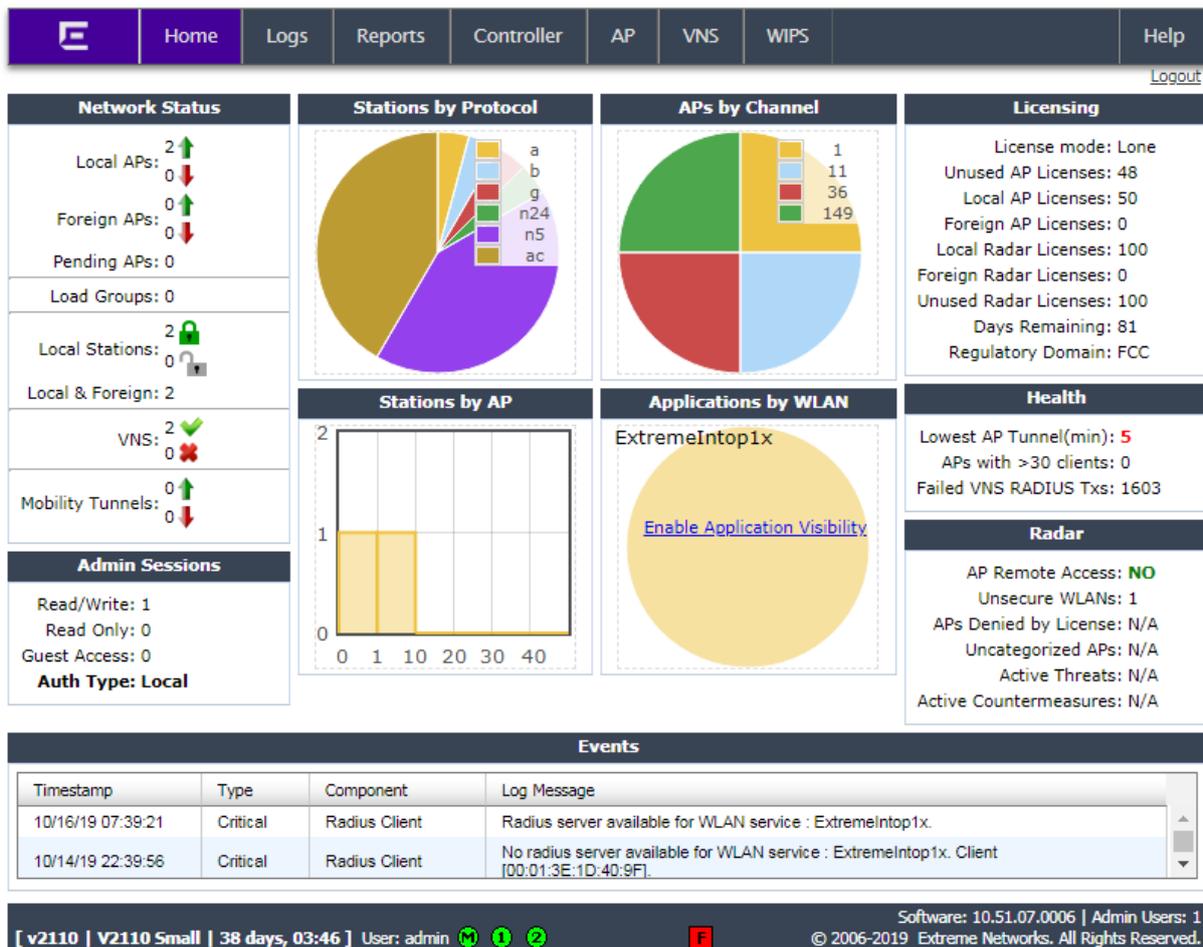
Appendix A: Verification Configurations

Extreme Networks V2110 Controller v. 10.51.10

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.

Overview

Extreme Networks controller overview.



Security settings (PSK)

E
Home
Logs
Reports
Controller
AP
VNS
WIPS
Help

[Logout](#)

New...

Global

Sites

Virtual Networks

WLAN Services

ExtremeIntop1X
 ExtremeIntopPSK

Roles

Classes of Service

Topologies

WLAN: ExtremeIntopPSK

WLAN Services
Privacy
Auth & Acct
QoS

Core

Name:

Service Type: Standard

SSID:

Default Topology: Bridged at AP untagg...

Default CoS: No CoS

Default Traffic Mirror: Prohibited

Application Visibility:

Wireless APs

Select APs:

Radio 1	Radio 2	Ports	AP Name
<input checked="" type="checkbox"/> a/n	<input checked="" type="checkbox"/> g/n		13251116085A
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n		14252471085C
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n		1548Y-128680
<input checked="" type="checkbox"/> a/n/ac	<input checked="" type="checkbox"/> g/n	<input type="checkbox"/> p1 <input type="checkbox"/> p2 <input type="checkbox"/> p3	1649Y-111540

Status

Enable:

* Traffic Mirror configure in WLAN service applied to tcp/udp only

General SSID settings.

New...
Global
Sites
Virtual Networks
WLAN Services
ExtremeIntop1X
ExtremeIntopPSK

Roles
Classes of Service
Topologies

WLAN: ExtremeIntopPSK

WLAN Services	Privacy	Auth & Acct	QoS
<input type="radio"/> None <input type="radio"/> Static Keys (WEP) <input type="radio"/> Dynamic Keys (WEP) <input type="radio"/> WPA <input checked="" type="radio"/> WPA - PSK	<input type="checkbox"/> WPA v.1 Encryption: TKIP only <input checked="" type="checkbox"/> WPA v.2 Encryption: AES only <input checked="" type="checkbox"/> Broadcast re-key interval: 3600 (30 - 86400 seconds) <input type="checkbox"/> Group Key Power Save Retry Management Frame Protection: Enabled Input Method: <input checked="" type="radio"/> Input String <input type="radio"/> Input Hex Pre-shared key String: <input type="button" value="Unmask"/> (min 8 characters; max 63)		

Note: using WEP or WPAv1 privacy will limit 11n and 11ac performance to legacy AP rates.

Security profile WPA2-PSK, AES encryption

- Select WPA v.2

Security settings (802.1X / PEAP-MSCHAPv2)

The screenshot shows the configuration page for 'WLAN: ExtremeIntop1x'. The interface includes a top navigation bar with 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', 'WIPS', and 'Help'. A left sidebar contains a tree view with 'WLAN Services' selected. The main content area is divided into tabs: 'WLAN Services', 'Privacy', 'Auth & Acct', and 'QoS'. Under the 'Privacy' tab, several radio buttons are visible: 'None', 'Static Keys (WEP)', 'Dynamic Keys (WEP)', 'WPA', and 'WPA - PSK'. The 'WPA' option is selected and highlighted with a red box. To the right, the 'WPA v.2' configuration section is also highlighted with a red box, showing 'Encryption: AES only', 'Key Management Options: Opportunistic Keying', 'Broadcast re-key interval: 3600 (30 - 86400 seconds)', 'Group Key Power Save Retry' (unchecked), 'Management Frame Protection: Disabled', and 'Fast Transition' (checked). A red note at the bottom of the configuration area states: 'Note: using WEP or WPAv1 privacy will limit 11n and 11ac performance to legacy AP rates.' At the bottom of the page, a status bar shows system information: '[v2110 | V2110 Small | 09 days, 00:33] User: admin', software version '10.51.10.0006', and copyright '© 2006-2019 Extreme Networks. All Rights Reserved.'

Configuration of authentication using external Radius server, 802.1X (Step 1). In this example is WPA2-AES/CCMP used.

- Select WPA v.2
- It is strongly recommended to use Fast Transition (802.11r) for enhanced roaming performance.

Compatibility Note. Enabling Fast Transition will allow both 802.1X and FT 802.1X. This means that i62 and Myco 1 and 2 can operate on the same SSID even when Fast Transition is enabled.

New...
Global
Sites
Virtual Networks
WLAN Services
ExtremeIntop1x
ExtremeIntopPSK

Roles
Classes of Service
Topologies

WLAN: ExtremeIntop1x

WLAN Services Privacy **Auth & Acct** QoS

Authentication
Mode: 802.1x no HTTP Redirection
 Enable MAC-based authentication
 Enable RADIUS Accounting

RADIUS Servers

Auth	
FreeRadius	<input type="button" value="Select Radius"/> <input type="button" value="New"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Configure"/> <input type="button" value="Test"/> <input type="button" value="Summary"/> <input type="button" value="Remove"/> <input type="button" value="Radius TLVs"/>

Collect Accounting Information of Wireless Controller

Configuration of authentication using external Radius server (Step 2). Select the server to use. The server is created/configured in next step.

Add RADIUS Server [?] [X]

RADIUS Server

Server Alias:

Hostname/IP:

Shared Secret:

Default Protocol: ▼

Authentication

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Port:

Accounting

Priority:

Total Number of Tries:

RADIUS Request Timeout: (seconds)

Interim Accounting Interval: (minutes)

Port:

Health Monitoring

Polling Mechanism: ▼

Test Request Timeout: (seconds)

Configuration of authentication using external Radius server (Step 3).

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

Note. Depending on which Authentication method used it might be necessary to add a certificate into the i63. PEAP-MSCHAPv2 requires a Root certificate and EAP-TLS requires both a Root certificate and a client certificate.

Note. To enable fast inter-controller roaming with opportunistic key caching, the “pair” option under “Wireless controller -> availability” has to be enabled. Please consult Extreme Networks for details.

General settings (SSID, QoS, Radio)

The screenshot shows the configuration page for 'WLAN: Extremelntop1x'. The interface includes a top navigation bar with 'VNS' selected, and a left sidebar with 'WLAN Services' highlighted. The main content area is divided into four tabs: 'WLAN Services', 'Privacy', 'Auth & Acct', and 'QoS'. The 'QoS' tab is active, displaying the following settings:

- Wireless QoS** (highlighted with a red box):
 - WMM
 - 802.11e
 - Turbo Voice
 - U-APSD
- Admission Control**:
 - Use Global Admission Control for Voice (VO)
 - Use Global Admission Control for Video (VI)
 - Use Global Admission Control for Best Effort (BE)
 - Use Global Admission Control for Background (BK)

* Global admission controls are configured through Global Settings
- Flexible Client Access**:
 - Flexible Client Access

* Flexible Client Access may not work if Global Admission Controls for Voice and Video (Advanced QoS settings) are enabled. Enabling Flexible Client Access will cause the AP to reboot.

Buttons for 'New', 'Delete', 'Advanced', and 'Save' are visible at the bottom of the configuration area.

- Make sure that WMM and U-APSD is enabled. U-APSD is strongly recommended in order to increase battery performance.

Advanced [?] [X]

Timeout

Idle: (pre) minutes

(post) minutes

Session: minutes

RF

Suppress SSID

Enable 11h support

Apply power reduction to 11h clients

Process client IE requests

Energy Save Mode

Radio Management (11k) support

Beacon Report

Quiet IE

Include AP Name Beacon/Probe

Egress Filtering Mode

Enforce explicitly defined "Out" rules

Apply "in" rules to "Out" direction traffic *

* When "In" filter rules are applied to "Out" traffic, the role of the source and destination address are reversed

Client Behavior

Block MU to MU traffic (not supported on Bridged at AP topologies)

Clear on disconnect

WLAN Services – Advanced Settings

- Enable 11h support
- Enable Radio Management (11k) support.
- Make sure Quiet IE is disabled.

Edit AP
?
✕

[<Back](#)

AP Properties	WLAN Assignment	Radio 1	Radio 2	Static Configuration	802.1x
Base Settings		BSS Info	D8:84:66:49:E9:08 ExtremeIntopP		
		Admin Mode	On ▼		
		Radio Mode	g/n ▼		
		Channel Width	20MHz ▼		
Basic Radio Settings		RF Domain	MyDomain		
		Current Channel ¹	1: (2412)		
		Last Requested Channel	1: (2412)		
		Request New Channel	- ▼		
		Auto Tx Power Ctrl (ATPC)	<input type="checkbox"/>		
		Current Tx Power Level	10 dBm		
		Max Tx Power	10 dBm ▼		
		Channel Plan	3-Channel Plan ▼		
			View		
		¹ AP may take up to 90 seconds to report the current channel			
		Advanced...			

Copy to Defaults
Reset to Defaults
Apply
Close

Ascom recommended settings for 802.11g/n are to use 3 channel plan (channel 1, 6 and 11). RoW might use custom channel plan (1, 7, and 13) according to Extreme Networks recommendation

Due to the limited number of non-overlapping channels using 802.11g/n it is recommended to use 20MHz channel width.

Advanced

Base Settings

DTIM Period	2
Beacon Period [ms]	100
RTS/CTS Threshold [Bytes]	2346
Frag. Threshold [Bytes]	2346
Maximum Distance [m]	100

Basic Radio Settings

Dynamic Channel Selection	Monitor Mode
DCS Noise Threshold [dBm]	-80
DCS Channel Occupancy Threshold	100 %
DCS Update Period [Minutes]	5

DCS Interference Event

Bluetooth	Disabled
Microwave	Disabled
Cordless Phone	Disabled
Constant Wave	Disabled
Video Bridge	Disabled
Interference Wait time [Seconds]	10

Multicast Settings

Min Basic Rate	12 Mbps
Probe Suppression	<input type="checkbox"/>
Max % of non-unicast traffic per Beacon period	100
Optimized for power save	<input type="checkbox"/>
Adaptable rate	<input type="checkbox"/>
Multicast to Unicast delivery	Disabled

11g Settings

Close

Radio 2 -> Advanced

- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- It is recommended to set the Min Basic Rate to 12Mbps to increase the performance.

Note that Tx Power was adjusted in order to test roaming.

11g Settings	
Protection Mode	Auto
Protection Rate	11 Mbps
Protection Type	CTS Only
11n Settings	
Guard Interval	Short
Protection Mode	Auto
Protection Type	CTS only
Aggregate MSDUs	Disabled
Aggregate MPDUs	Enabled
Aggregate MPDU Max Length	65535
Agg. MPDU Max # of Sub-frames	30
ADDBA Support	Enabled
LDPC	Enabled
STBC	Disabled

Radio 2 -> Advanced (continued). Additional settings left as default.

Home Logs Reports Controller **AP** VNS Radar Help

Logout

APs

All

ExtremeIntop

ExtremeIntop1x

ExtremeIntopPSK

Load Groups

Mobile Stations

Bulk Configuration

Global Settings

APs

10280904235J000I

14252471085C000

WS-AP3715I

AP Properties | WLAN Assignment | **Radio 1** | Radio 2 | Static Configuration | 802.1x

Base Settings

BSS Info

20:B3:99:E6:EE:D0 ExtremeInt

20:B3:99:E6:EE:D1 ExtremeInt

20:B3:99:E6:EE:D2 ExtremeInt

Basic Radio Settings

Admin Mode On

Radio Mode a/n/ac

Channel Width 20MHz

RF Domain MyDomain

Current Channel ¹ 36: ([5180],5200)

Last Requested Channel 36: ([5180],5200)

Request New Channel -

Auto Tx Power Ctrl (ATPC)

Current Tx Power Level 14 dBm

Max Tx Power 14 dBm

Channel Plan All Non-DFS-Channels

View

Antenna Selection Left/Middle/Right

¹ AP may take up to 90 seconds to report the current channel

Advanced...

Copy to Defaults

Reset to Defaults

Add Wireless AP

Save

Configuration of 802.11a/n/ac: Refer to general guidelines on page 20.

Note that Tx Power was adjusted in order to test roaming.

Advanced
?
✕

Base Settings

DTIM Period	2
Beacon Period [ms]	100
RTS/CTS Threshold [Bytes]	2346
Frag. Threshold [Bytes]	2346
Maximum Distance [m]	100

Basic Radio Settings

Dynamic Channel Selection	Monitor Mode ▼
DCS Noise Threshold [dBm]	-80
DCS Channel Occupancy Threshold	100 %
DCS Update Period [Minutes]	5

DCS Interference Event

Bluetooth	Disabled ▼
Microwave	Disabled ▼
Cordless Phone	Disabled ▼
Constant Wave	Disabled ▼
Video Bridge	Disabled ▼
Interference Wait time [Seconds]	10

Min Basic Rate	12 Mbps ▼
Probe Suppression	<input type="checkbox"/>

Multicast Settings

Max % of non-unicast traffic per Beacon period	100
Optimized for power save	<input type="checkbox"/>
Adaptable rate	<input type="checkbox"/>
Multicast to Unicast delivery	Disabled ▼

11g Settings

Radio 1 -> Advanced

- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- It is recommended to set the Min Basic Rate to 12Mbps to increase the performance.

Note that Tx Power was adjusted in order to test roaming.

802.11a/n/ac

Non-DFS	
36:	([5180],5200)
40:	(5180,[5200])
44:	([5220],5240)
48:	(5220,[5240])
149:	([5745],5765)
153:	(5745,[5765])
157:	([5785],5805)
161:	(5785,[5805])
DFS	
52:	([5260],5280)
56:	(5260,[5280])
60:	([5300],5320)
64:	(5300,[5320])
100:	([5500],5520)
104:	(5500,[5520])
108:	([5540],5560)
112:	(5540,[5560])
132:	([5660],5680)
136:	(5660,[5680])
140:	([5700],5720)
144:	(5700,[5720])

Configuration of 802.11a/n/ac: Refer to general guidelines on page 18.

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 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)

Home | Logs | Reports | Controller | AP | **VNS** | Radar | Help [Logout](#)

VNS: ExtremeIntopPSK

General

Core
VNS Name: ExtremeIntopPSK

WLAN Service
WLAN Service: ExtremeIntopPSK [Edit] [New]

Default Roles
Non-Authenticated: Voice [Edit] [New]
 Action: Allow Class of Service: No CoS

Authenticated: <Same as non-authenticated> [Edit] [New]
 Action: Allow Class of Service: No CoS

Status
Enable:

[New] [Delete] [Save]

Virtual Network set up including the Roles.

Home | Logs | Reports | Controller | AP | **VNS** | Radar | Help [Logout](#)

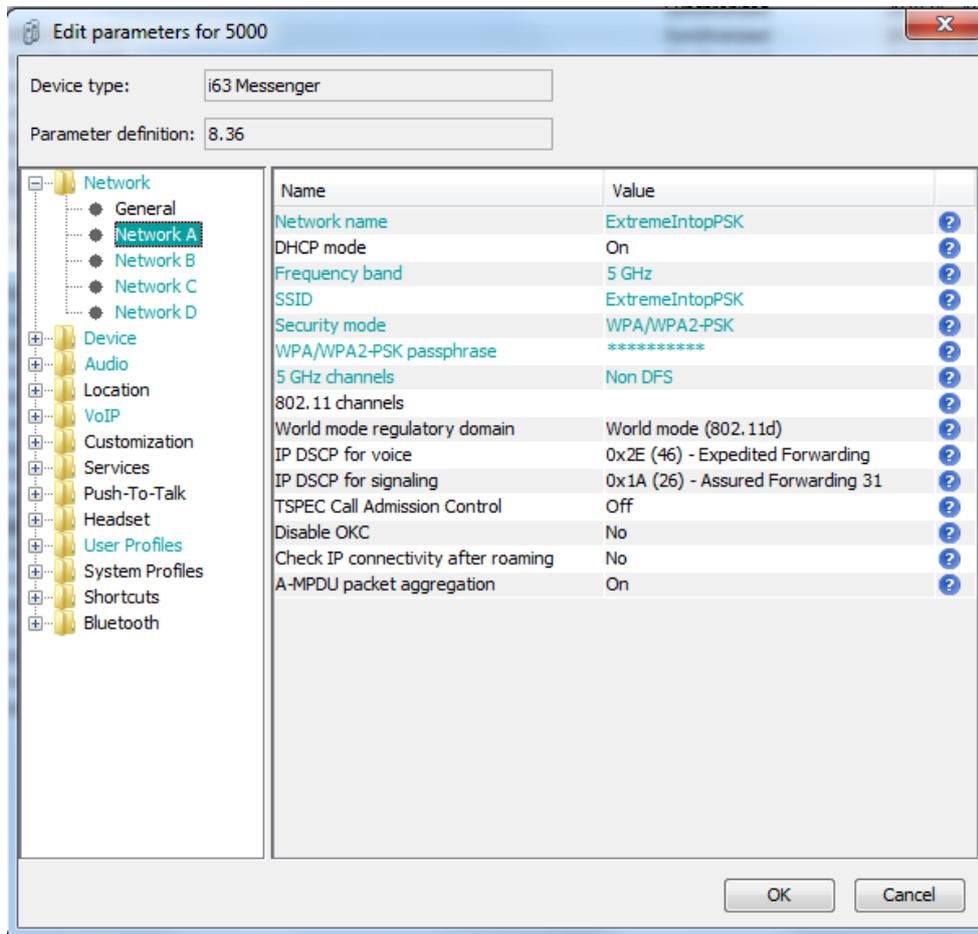
Role: Voice

VLAN & Class of Service | Policy Rules

Core
Role Name: Voice

Default Action
Access Control: Allow [Edit] [New]
Default Class of Service: No change
Traffic Mirror: None

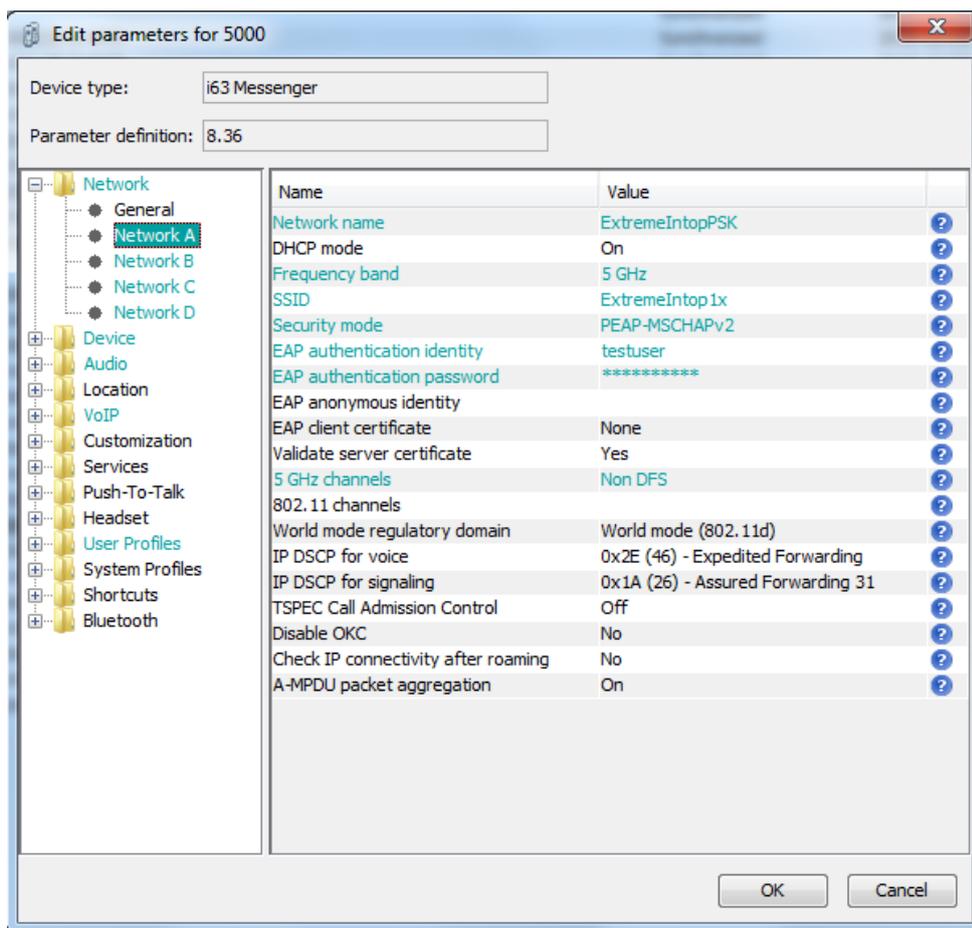
Voice role configuration.



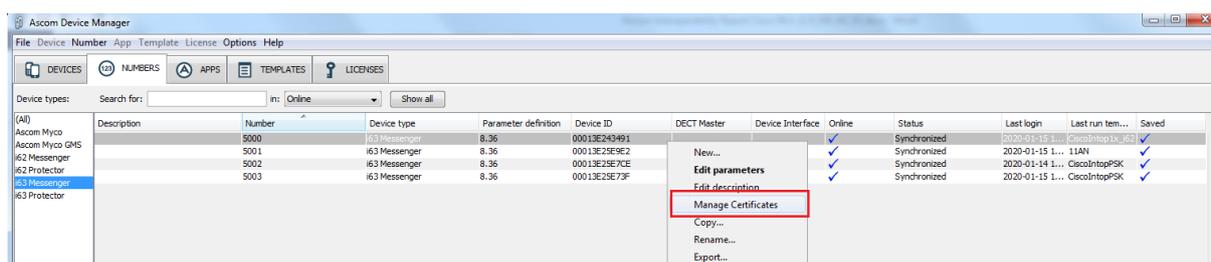
Network settings for WPA2-PSK

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: Detailed Verification Records

Pass	19
Fail	2
Comments	3
Not verified	1
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	17-Jan-20	SEKMO	Draft
R1	12-Feb-20	SEKMO	Minor adjustments after review. Revision R1