

INTEROPERABILITY REPORT

Ascom i63  
Ruckus Wireless

Ruckus SmartZone

Ruckus SZ v. 5.2.0.0

Ascom i63 v. 1.0.8

Morrisville, NC, USA

April 2020

**ascom**

# Contents

- Introduction..... 3**
  - About Ascom..... 3
  - About Ruckus Networks ..... 3
  - About CommScope & Ruckus..... 3
  
- Site Information..... 4**
  - Verification site..... 4
  - Participants ..... 4
  - Verification topology..... 4
  
- Summary ..... 5**
  - General conclusions ..... 5
  - Compatibility information ..... 5
  - Verification overview ..... 6
  - Known limitations..... 7
  
- Appendix A: Verification Configurations..... 8**
  - Ruckus Wireless SmartZone version 5.2.0.0.699 ..... 8
  - Ascom i63 ..... 17
  
- Appendix B: Detailed Verification Records..... 19**
  
- Document History ..... 19**

# Introduction

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

Ruckus Networks, an ARRIS company, is redefining connectivity around the globe. With our partners, we build secure wired and wireless access networks for organizations that place a premium on connectivity experiences for end users as well as simplicity. Follow Ruckus on Twitter, Facebook, LinkedIn, Instagram, YouTube and subscribe to our blog.

## About CommScope & Ruckus

CommScope (NASDAQ: COMM) and the recently acquired ARRIS and Ruckus Networks are redefining tomorrow by shaping the future of wired and wireless communications. Our combined global team of employees, innovators and technologists have empowered customers in all regions of the world to anticipate what's next and push the boundaries of what's possible. Discover more at [www.commscope.com](http://www.commscope.com). Site Information

# Site Information

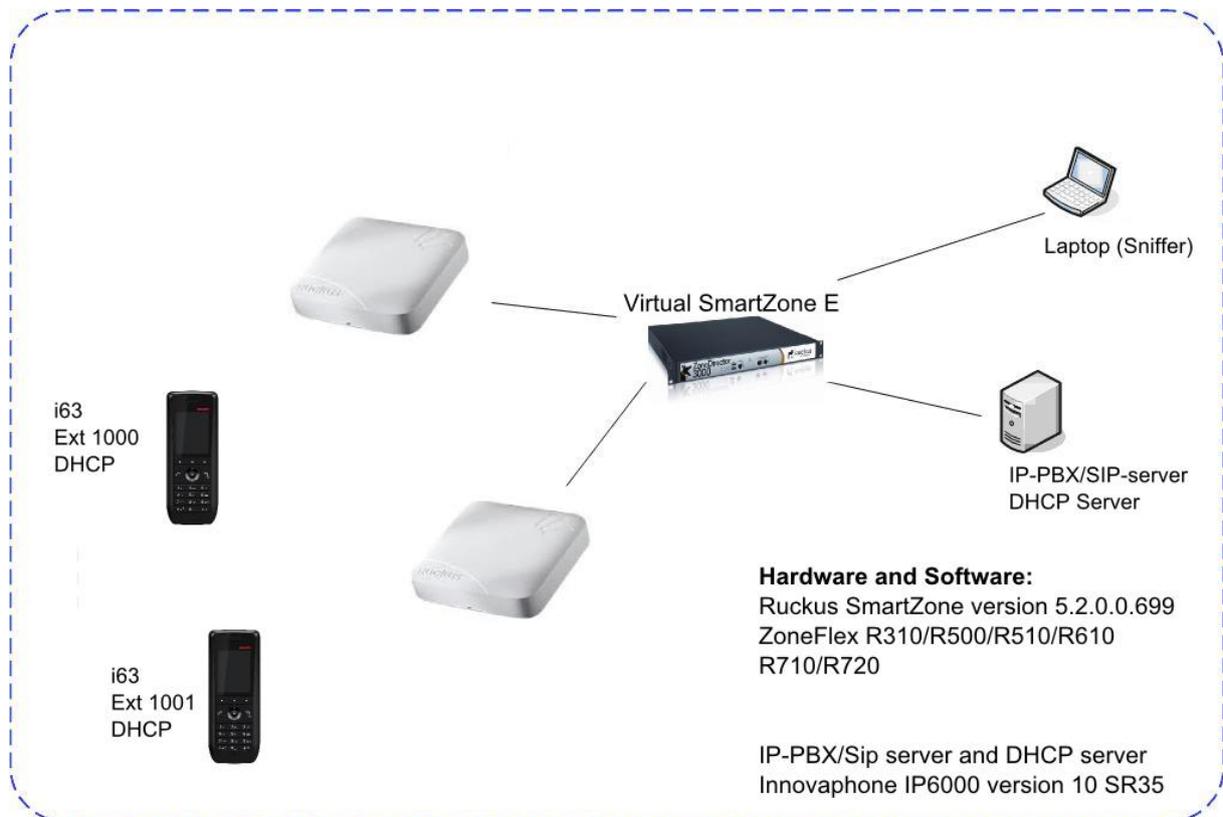
## Verification site

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

## Participants

Karl-Magnus Olsson, Ascom, Morrisville

## Verification topology



# Summary

## General conclusions

Validation includes new access point R720 which has undergone the complete test. The previously already validated access points has undergone a less extensive test. For example, capacity test and battery measurements have been left out. For test cases left out we consider the test results from previous full test valid.

Test cases, such as authentication and roaming and power save have however all been successful across the board.

## Compatibility information

All test were performed using a Virtual SmartZone E. We ensure compatibility/interoperability with all the access points and controllers listed below given that they run the software tested.

### **Supported Partner Access Points with Ruckus Wireless version SmartZone 5.2.0.0.699:**

ZoneFlex R300, R310, R500, R510, R600, R610, R710, R720, T310

### **Supported controller platforms with Ruckus Wireless version SmartZone 5.2.0.0.699:**

Virtual SmartZone H (vSZ-H)

Virtual SmartZone E (vSZ-E)

Virtual SmartZone D (vSZ-D)

SmartZone 100 & 300

## Verification overview

### WLAN Compatibility and Performance

High Level Functionality	Result	Comments
Association, Open with No Encryption	NOK	
Association, WPA2-PSK / AES Encryption	OK	
Association, WPA2-PSK, AES Encryption, 802.11r/FT	OK	
Association, PEAP-MSCHAPv2 Auth, AES Encryption	OK	
Association, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	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 75-100 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Avg. typical roaming time 20-35 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK *	Avg. typical roaming time 75-100 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Avg. typical roaming time 20-35 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
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 Protected Management Frames in system.	WH2-2356

For additional information regarding the known limitations please contact [interop@ascom.com](mailto:interop@ascom.com) or [support@ascom.com](mailto:support@ascom.com).

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

# Appendix A: Verification Configurations

## Ruckus Wireless SmartZone version 5.2.0.0.699

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

### Security settings (PSK)

The screenshot shows the Ruckus SmartZone management interface. The top navigation bar includes the Ruckus logo, the text 'Virtual SmartZone - Essentials', the user 'Interop' with a timestamp '2019-08-27 14:34:35', a 'default' dropdown menu, and a user profile icon for 'admin'. The left sidebar contains navigation links: Dashboard, System, Access Points, Switches, **Wireless LANs**, Clients, Applications, Services & Profiles, and Report. The main content area is titled 'Wireless LANs' and shows a 'System' overview with a tree view containing 'System' and 'Default Zone'. Below this is a table of wireless LAN configurations.

Name	Alerts	SSID	Auth Method	Encryption Method	Clients	Traffic
RuckusIntop1X	0	RuckusIntop1X	802.1X	WPA2	0	2.4KB
RuckusIntopPSK	0	RuckusIntopPSK	OPEN	WPA2	3	1.8MB

At the bottom right of the table, it indicates '2 records' and a page navigation '1'.

Wireless LAN overview.

## Edit WLAN Config: [RuckusIntopPSK]

The screenshot displays the configuration interface for a WLAN named 'RuckusIntopPSK'. It is divided into three main sections: General Options, Authentication Options, and Encryption Options. Red boxes highlight the specific settings for PSK security.

- General Options:** Name, SSID, and Description are all set to 'RuckusIntopPSK'. The Zone is 'Default Zone' and the WLAN Group is 'default'.
- Authentication Options:** The Authentication Type is 'Standard usage (For most regular wireless networks)'. The Method is set to 'Open'.
- Encryption Options:** The Method is 'WPA2', the Algorithm is 'AES', and the Passphrase is masked with dots. The '802.11r Fast Roaming' toggle is turned 'ON'. The Mobility Domain ID is '1'.

Example of how to configure the system for PSK security (WPA2-AES)

- Select open Authentication
- Select WPA2 and AES
- It is strongly recommended to use Fast Transition (802.11r) for enhanced roaming performance.
- Note. 802.11r is not supported by Ascom i62 and Myco 1 & 2 but the devices have no problem operating on a SSIDs were 802.11r (FT) is advertised in conjunction with a legacy method.

## Edit WLAN Config: [RuckusIntopPSK]

**Advanced Options**

User Traffic Profile: System Default +

L2 Access Control: Disable +

OS Policy: Disable +

Application Recognition & Control: OFF

URL Filtering: OFF

Wi-Fi Calling: OFF

Client Fingerprinting: ON

[?] Access VLAN: VLAN ID 1  
Enable VLAN Pooling OFF  
If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP profile(s).

Hide SSID: OFF

Client Load Balancing:  Disable client load balancing for this WLAN service

Proxy ARP: ON

ND Proxy: OFF Suppress NS

RA Proxy: OFF RS/RA Guard  
OFF RA Throttling

### Advanced WLAN configuration

- Make sure Client Load Balancing is disabled
- Enable Proxy ARP

## Edit WLAN Config: [RuckusIntopPSK]

Minutes):

\* Max Clients: Allow up to  clients per AP radio to associate with this WLAN

802.11d:  ON

802.11k Neighbor Report:  ON

Anti-spoofing:  OFF

OFF ARP request rate limit  ppm

OFF DHCP request rate limit  ppm

Force DHCP:  OFF Disconnect client if it does not obtain a valid IP address after  seconds

DHCP Option 82:  OFF

DTIM Interval:  (1-255) Defines the frequency of beacons that will include a DTIM

[?] Directed MC/BC Threshold:  (0-128) Defines the per radio client count at which an AP will stop converting group addressed data traffic to unicast.

Client TX/RX Statistics:  Ignore statistics from unauthorized clients

\* Inactivity Timeout: Terminate user sessions that are idle for  seconds (60-1000) of inactivity

OFDM Only:  OFF

\* [?] BSS Min Rate:  mbps

Mgmt Tx Rate:  mbps

\* Time Schedule:  Always On  Always Off  Specific

Band Balancing:  Disable band balancing for this WLAN service

QoS Map Set:  OFF

[?] SSID Rate Limiting: Uplink:  OFF  mbps (1-200) Rate limiting in user traffic profile will not work if SSID rate limiting is enabled.

### Advanced WLAN configuration (Continued)

- Enable 802.11d
- Enable 802.11k Neighbour report.  
Note that i62 Channels parameter needs to be set to enable 802.11k on handset side. See i63 configuration section below.
- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- Set BSS Min Rate to 12mbps
- Make sure Band Balancing is disabled

Note. Ascom i62 and Myco 1 & 2 do not support 11k but have no problem operating on an SSID were these settings are enabled. (Assuming i62 version 6.0.0 and later)

## Security settings (802.1X / PEAP-MSCHAPv2)

The screenshot shows the Ruckus Virtual SmartZone Essentials web interface. The top navigation bar includes the Ruckus logo, a hamburger menu, the text "Interop 2019-08-27 14:54:00", a "default" dropdown menu, and a user profile icon labeled "admin". The left sidebar contains a navigation menu with the following items: Dashboard, System, Access Points, Switches, Wireless LANs, Clients, Applications, Services & Profiles (expanded), Hotspots & Portals, Access Control, Application Control, URL Filtering, Wi-Fi Calling, and Authentication (highlighted in blue). The main content area is titled "Non-Proxy (AP Authenticator)" and "Proxy (SZ Authenticator)". Below the title, there are action buttons: "Create", "Configure", "Clone", "Test AAA", and "Delete". A search bar labeled "search table" is also present. The main content area displays a tree view on the left with "System" and "Default Zone" under it. On the right, a table lists the configuration:

Name	Type	Description
FreeRadius	RADIUS	FreeRadius

At the bottom right of the table, it indicates "1 records" with navigation arrows.

Example of how to configure the system for .1X authentication.

See next screen shot for configuration of the profile "InteropFreeRADIUS".

## Edit AAA Server: [FreeRadius]

**General Options** ▼

\* Name:

Description:

\* Type:  RADIUS  Active Directory  LDAP

Backup RADIUS:  OFF  Enable Secondary Server

**Primary Server** ▼

\* IP Address:

\* Port:

\* Shared Secret:

\* Confirm Secret:

**User Role Mapping** ▼

Group Attribute Value ▲	User Role	User Traffic Profile

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

## Edit WLAN Config: [RuckusIntop1X]

The screenshot displays the configuration page for a WLAN profile named 'RuckusIntop1X'. The interface is divided into four main sections, each with a dropdown arrow on the right:

- General Options:** Contains fields for Name (RuckusIntop1X), SSID (RuckusIntop1X), Description (RuckusIntopPSK), Zone (Z Default Zone), and WLAN Group (default).
- Authentication Options:** Shows Authentication Type with radio buttons for Standard usage (selected), Hotspot (WISPr), Guest Access, and Web Authentication. Below are radio buttons for Hotspot 2.0 Access, Hotspot 2.0 Onboarding, and WeChat. The Method section has radio buttons for Open, 802.1X EAP (selected), MAC Address, and 802.1X EAP & MAC.
- Encryption Options:** Features radio buttons for Method (WPA2 selected, WPA-Mixed, WEP-64 (40 bits), WEP-128 (104 bits), None) and Algorithm (AES selected, AUTO). It also includes a toggle for 802.11r Fast Roaming (ON) and a Mobility Domain ID field (1).
- Authentication & Accounting Server:** Shows the Authentication Server set to OFF with 'Use the Controller as Proxy' and 'FreeRadius' selected. The Accounting Server is also set to OFF with 'Use the Controller as Proxy' and 'Disable' selected.

Configuration of ESS profile for utilization of 802.1X authentication.

- Select 802.1X EAP
- Select WPA2 and AES
- It is strongly recommended to use Fast Transition (802.11r) for enhanced roaming performance.
- Authentication server "InteropFreeRADIUS" corresponds to the server configured in previous step.

Note. 802.11r is not supported by Ascom i62 and Myco 1 & 2 but the devices have no problem operating on a SSIDs were 802.11r (FT) is advertised in conjunction with a legacy method.

## General settings (QoS, Radio)

### Configure Group

Name:  Description:

Type:  Zone  AP Group

Parent Group:

**Configuration**

Enable mesh networking

**Radio Options**

Channel Range (2.4G): 1 2 3 4 5 6 7 8 9 10 11

DFS Channels:  Allow DFS channels (allow ZoneFlex APs to use DFS channels)

Channel Range (5G) Indoor: 36 40 44 48 149 153 157 161

Channel Range (5G) Outdoor: 36 40 44 48 149 153 157 161

Radio Options (2.4 GHz)

Channelization:

Channel:

Auto Cell Sizing:  Enable

TX Power Adjustment:

Radio Options a/n/ac (5 GHz)

Channelization:

Channel:

Indoor:

Outdoor:

Auto Cell Sizing:  Enable

TX Power Adjustment:

Access Points Common Settings per AP group.

Ascom recommended settings for 802.11b/g/n are to only use channel 1, 6 and 11. For 802.11a/n/ac use channels according to the infrastructure manufacturer and country regulations.

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.**

# Edit AP: [30:87:D9:03:3D:50]

**AP Configuration** | Swap Configuration

161 |  163

---

**Radio Options (2.4 GHz)**

Channelization:  ON  Override: 20 ▼

Channel:  ON  Override: 6 ▼

Auto Cell Sizing:  ON  Override:  OFF Enable

TX Power Adjustment:  ON  Override: -8dB ▼

WLAN Group:  OFF  Override: default ▼ + ✎

WLAN Service:  ON

**Radio Options (5 GHz)**

Channelization:  ON  Override: 20 ▼

Channel:  ON  Override: Auto ▼

Auto Cell Sizing:  ON  Override:  OFF Enable

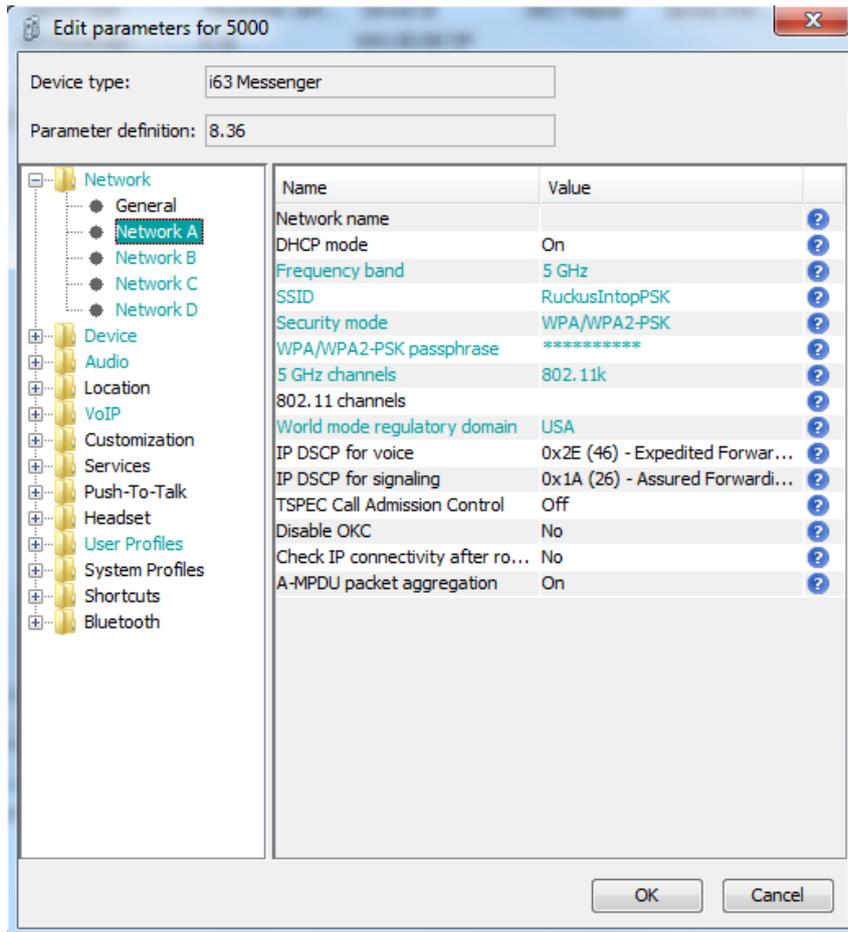
TX Power Adjustment:  ON  Override: -8dB ▼

WLAN Group:  OFF  Override: default ▼ + ✎

WLAN Service:  ON

Individual AP configuration

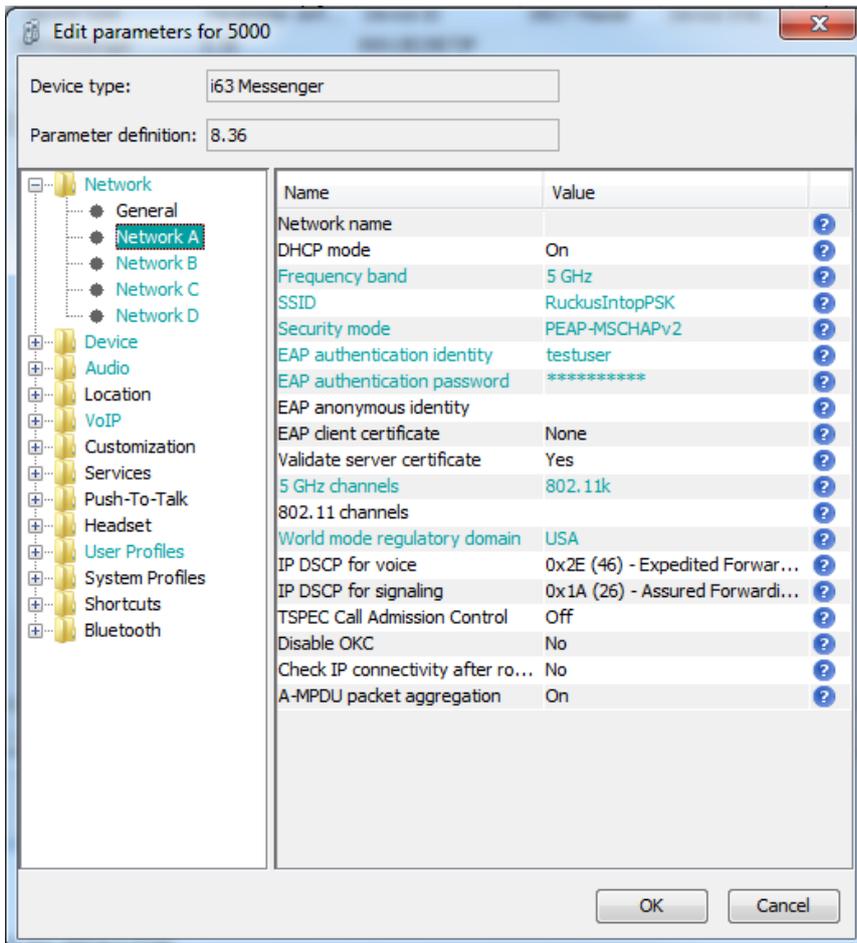
Channel and Tx power override was used to create suitable cell overlap for test purposes.



Network settings for WPA2-PSK

Note. Make sure that the enabled channels in the i63 handset match the channel plan used in the system. If 802.11k is enabled in the system the parameter 5GHz Channels needs to be set for 802.11k accordingly.

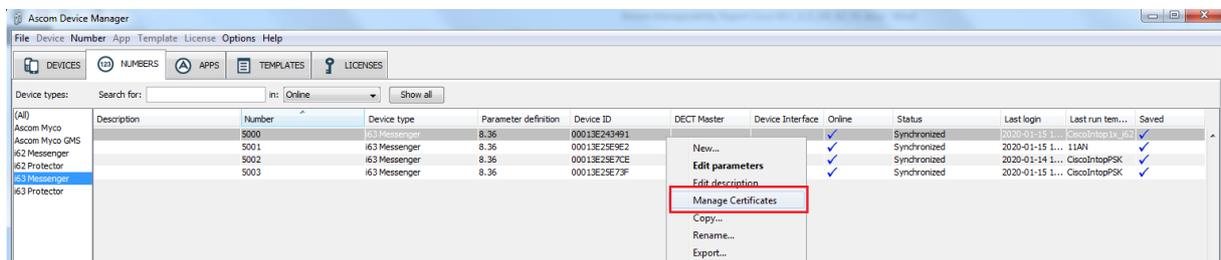
Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to "USA".



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

Note. Make sure that the enabled channels in the i63 handset match the channel plan used in the system. If 802.11k is enabled in the system the parameter 5GHz Channels needs to be set for 802.11k accordingly.

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



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	0
Not verified	5
Total	24

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	27-April-2020	SEKMO	Draft
R1	8-May-2020	SEKMO	Revision R1 after review.