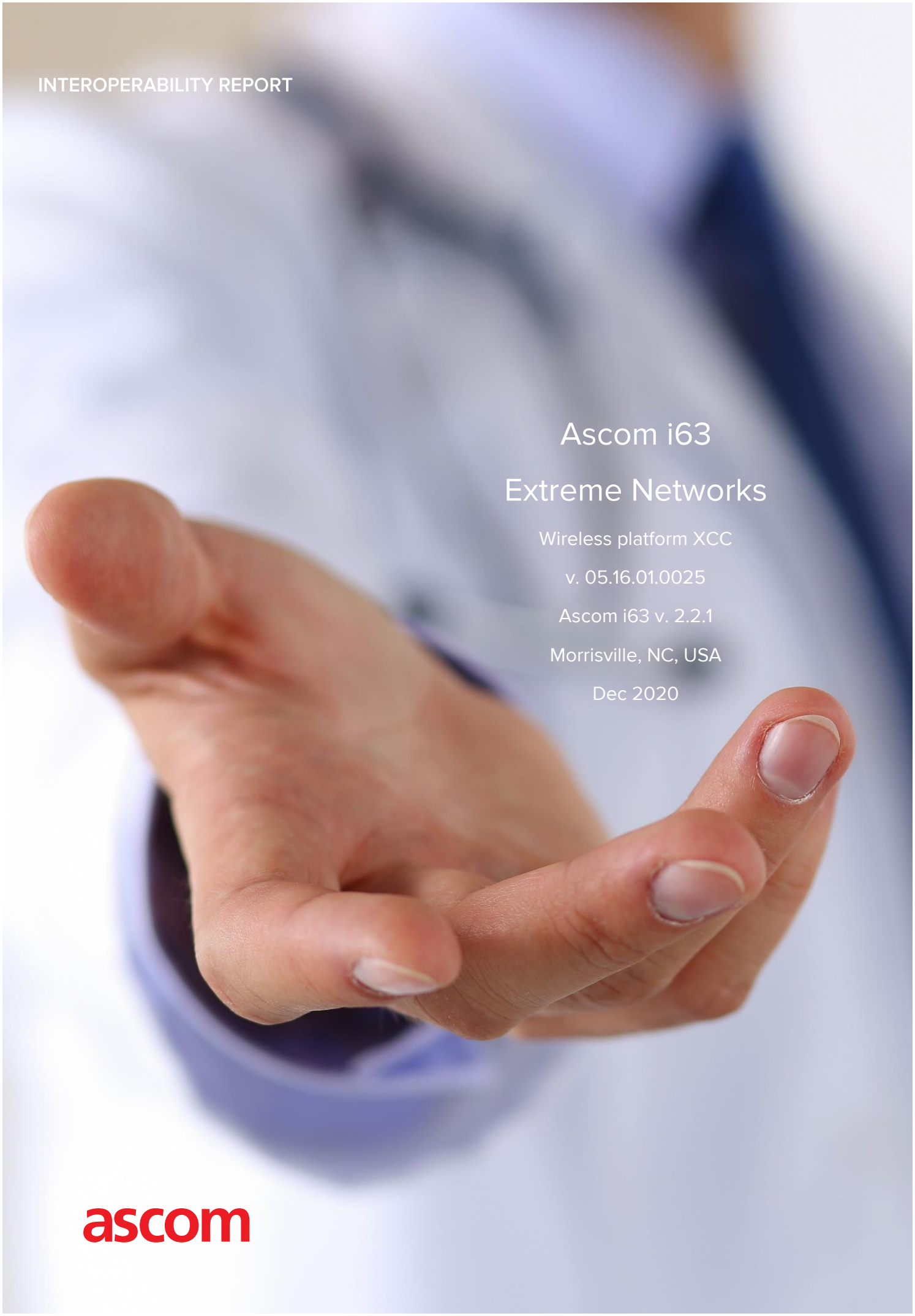
INTEROPERABILITY REPORT



Ascom i63

Extreme Networks

Wireless platform XCC

v. 05.16.01.0025

Ascom i63 v. 2.2.1

Morrisville, NC, USA

Dec 2020

ascom

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

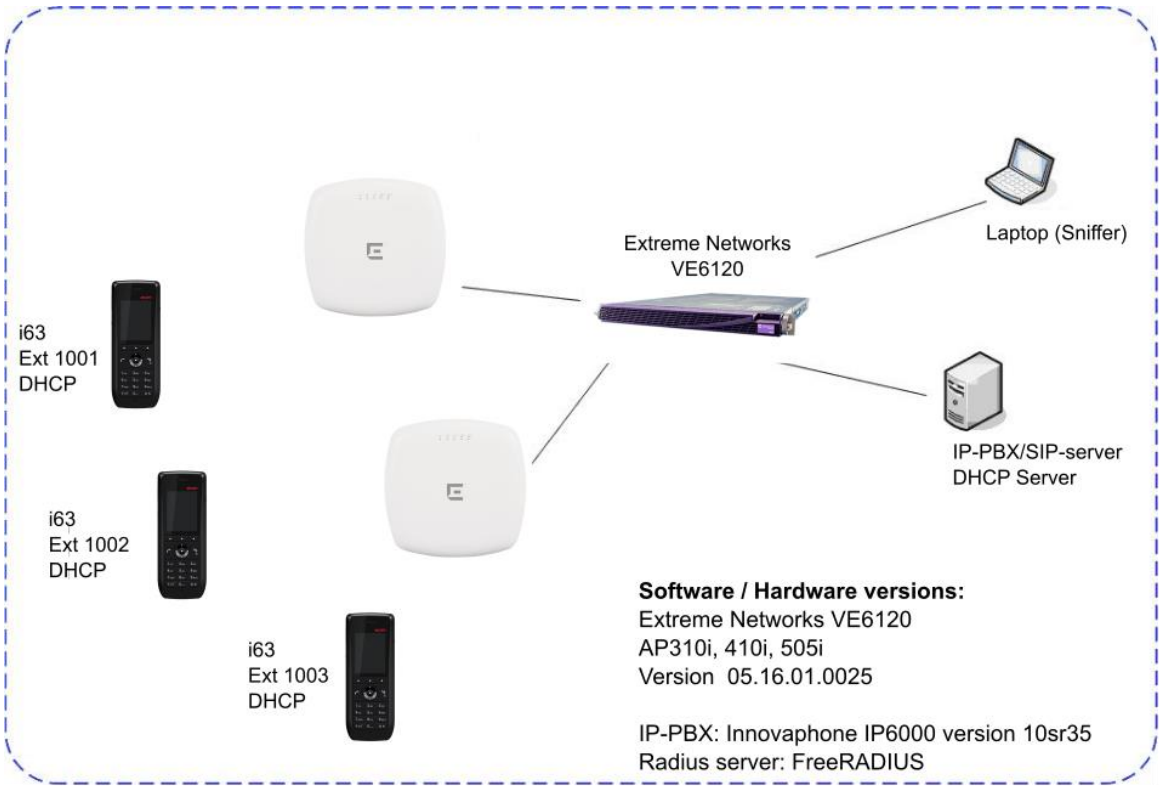
Verification site

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 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 802.11r/FT together with PEAP-MSCHAPv2. A problem was discovered using OKC fast roaming hence 11r/FT is mandatory for .1X based Authentication.

Compatibility information

Based on the test of 310i, 410i and 505i we consider following list of access point models to be covered.

Supported Partner Access Points with Extreme Networks version 05.16.01.0025:

AP310i/e

AP410i/e

AP505 and 510 i/e

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

Supported controller platforms with Extreme Networks 05.16.01.0025:

E1120

E2120

E3120

VE6120/VE6125

VE6120H

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	NOK	See known issue
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 43 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	N/A	Extreme does not support FT with PSK.
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	NOK	See known issue
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 40ms

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

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
Problem with Opportunistic Key Caching (OKC). Full Key exchange triggered when roaming resulting in longer roaming times (1s+). Affecting .1X/EAP Authentication only Under investigation by Extreme Networks.	Make sure 11r/FT is enabled for your .1X based SSID	Contact Ascom or Extreme Wireless support
802.11k/v Neighbor report contains no data rendering the added benefit of the feature not useful. Under investigation		Contact Ascom or Extreme Wireless support
Low Tx power level issue on ch36 with AP 310.	Use AP image AP3xx-LEAN-7.5.1.0-015R.img (or later)	
Authentication with 802.11w (Protected Management Frames) does not work in conjunction with 802.11r	11w not recommended.	WH2-2356

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

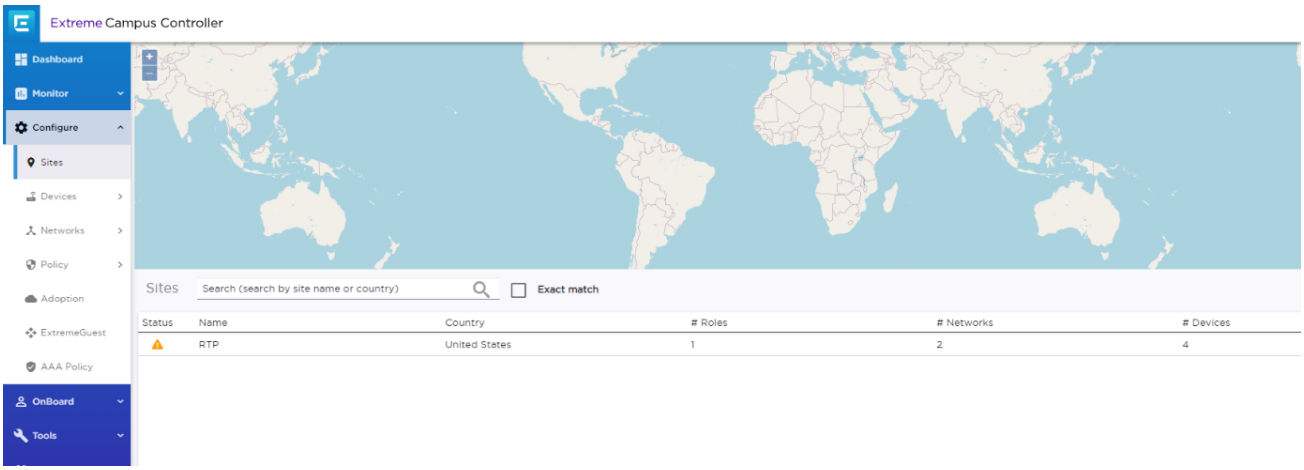
For detailed verification results, refer to Appendix B: Detailed Verification Records.

Appendix A: Verification Configurations

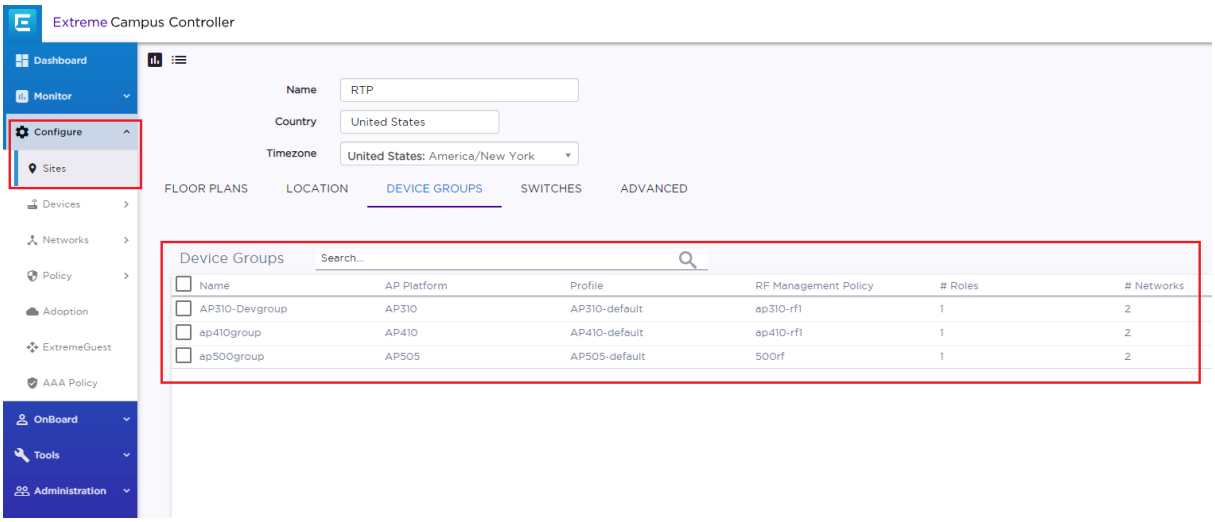
Extreme Networks XCC v. 05.16.01.0025

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.

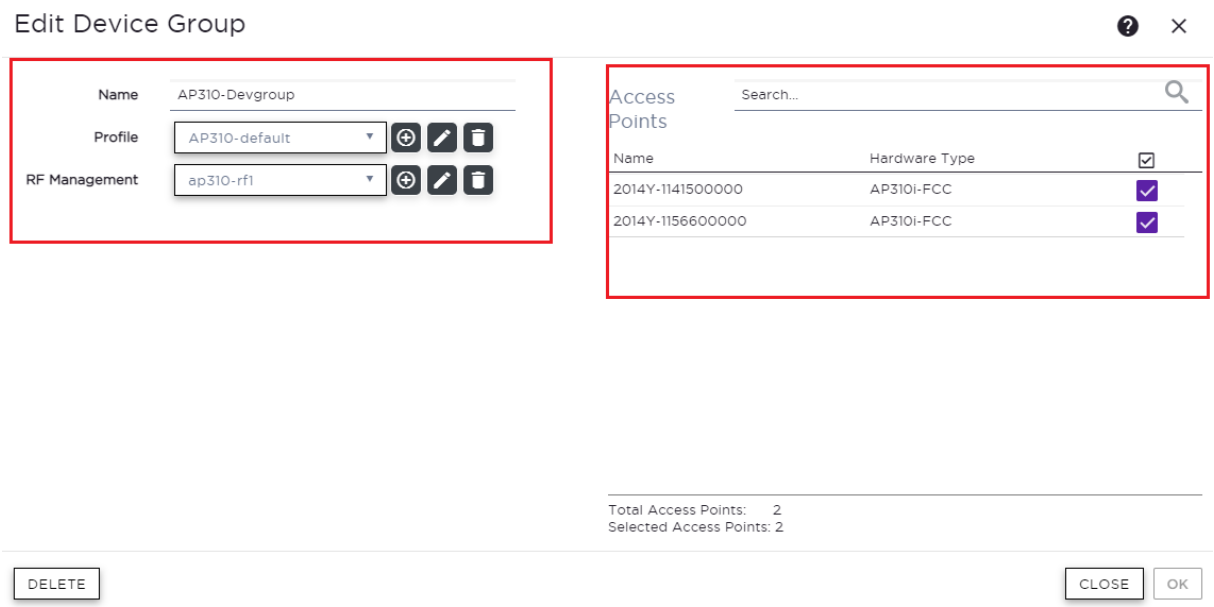
Site Setup



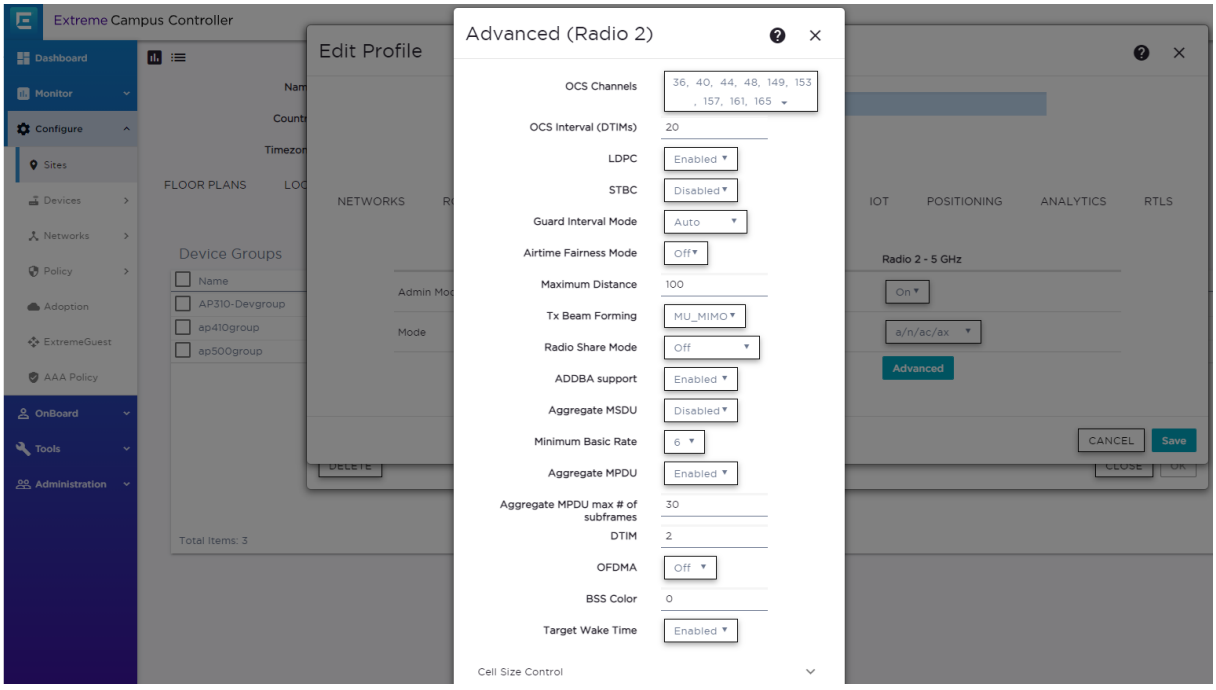
Site configuration. Here RTP



Add a device group per AP model. In this example AP 310, 410 and 500

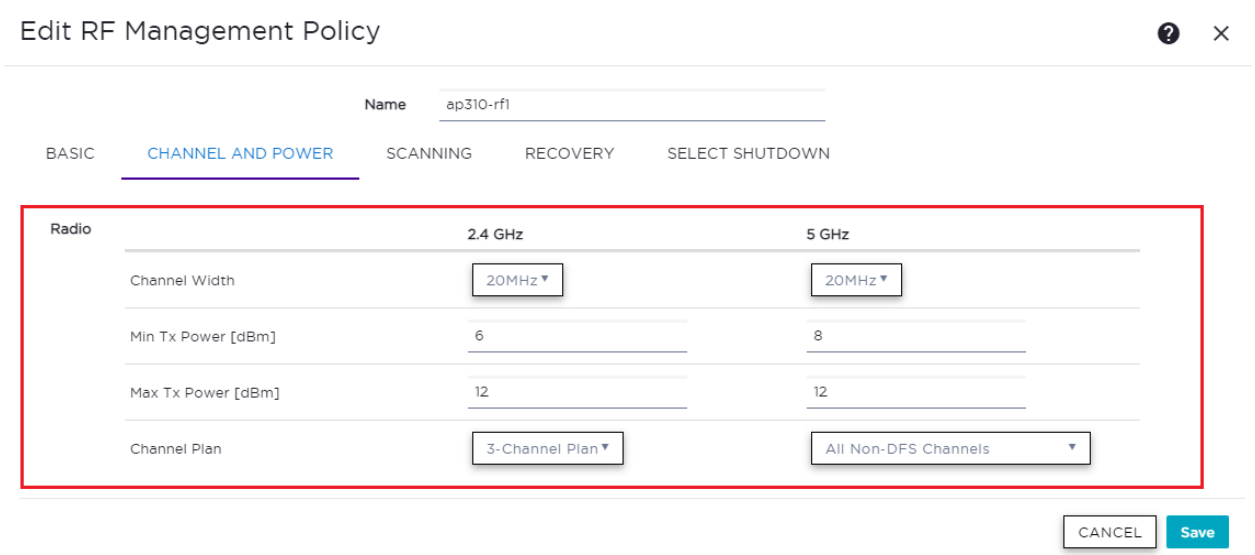


Add access points to device group and configure Profile and RF Management



The Profile Radio settings were left as default.

- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- For Radio 1 (2.4GHz) is recommended to set the Min Basic Rate to 12Mbps to increase the performance.



RF Management Policy

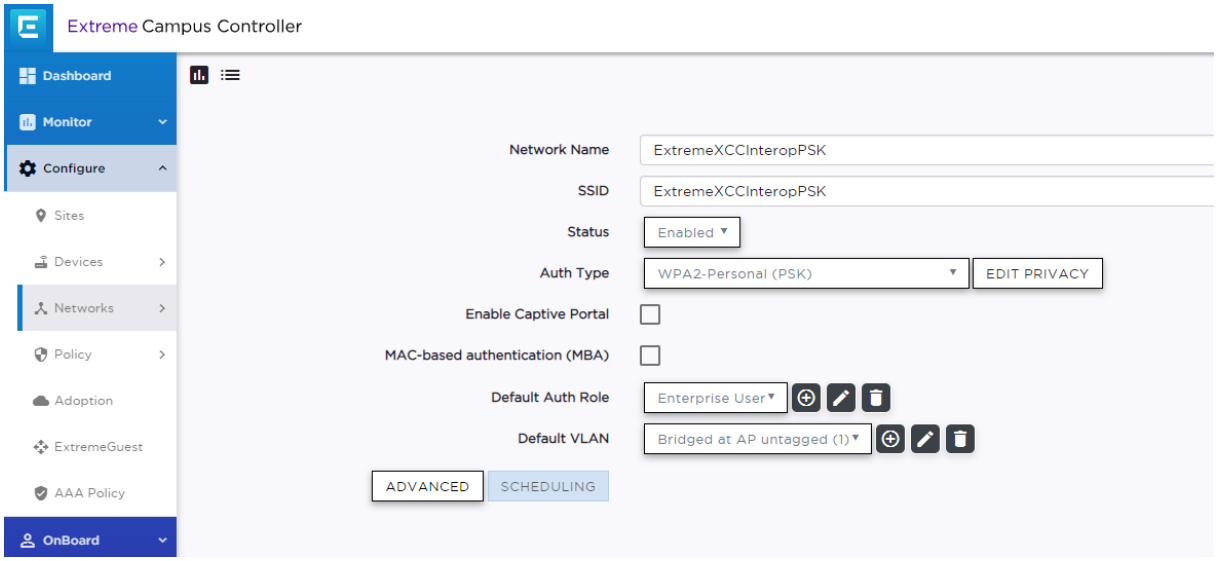
- Make sure a 3 –channel plan is used on the 2.4GHz radio
- Note that Tx power level and channel was manually set for test purpose.

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

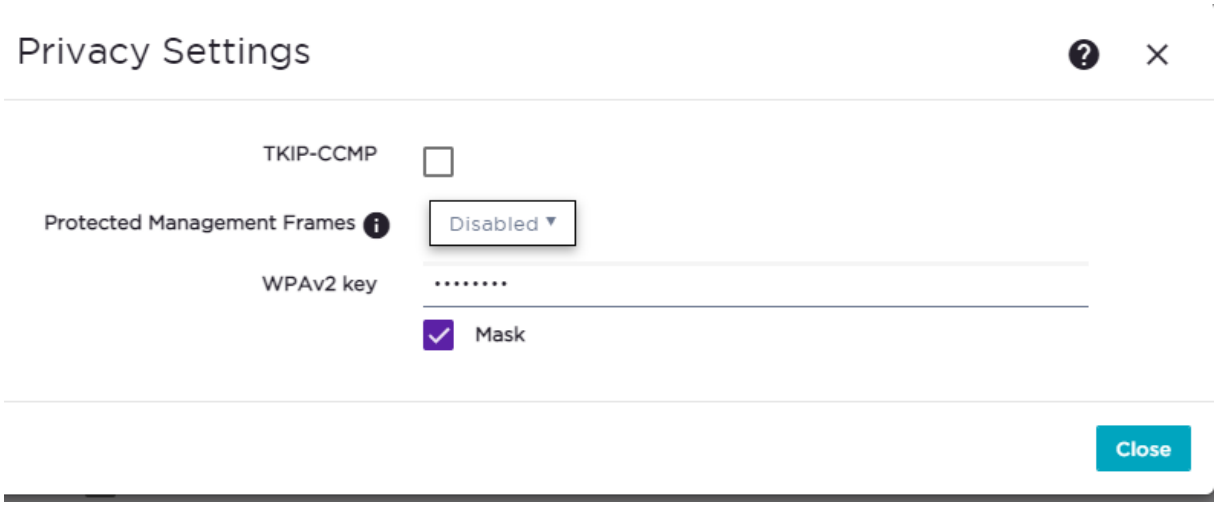
1. **For environments not utilizing 802.11k Neighbor Report - Enabling more than 8 channels will degrade roaming performance. (In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed) Ascom does not recommend exceeding this limit unless 802.11k is in use.**
2. **Ascom 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)

Security settings (PSK)

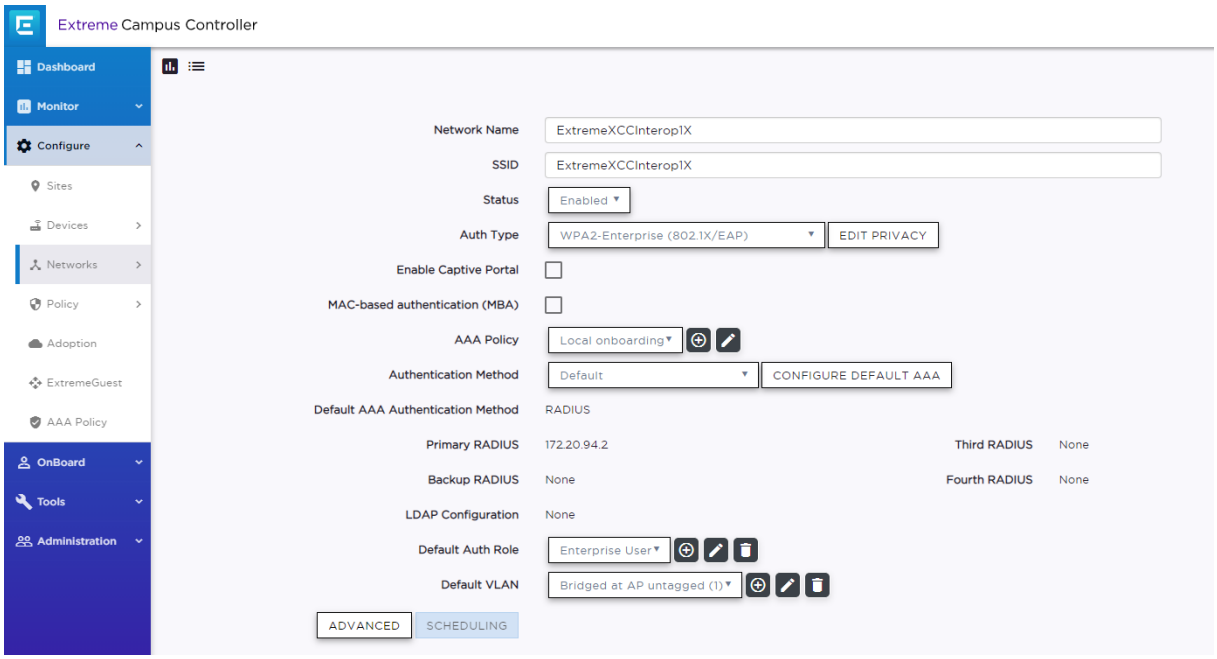


General SSID settings.



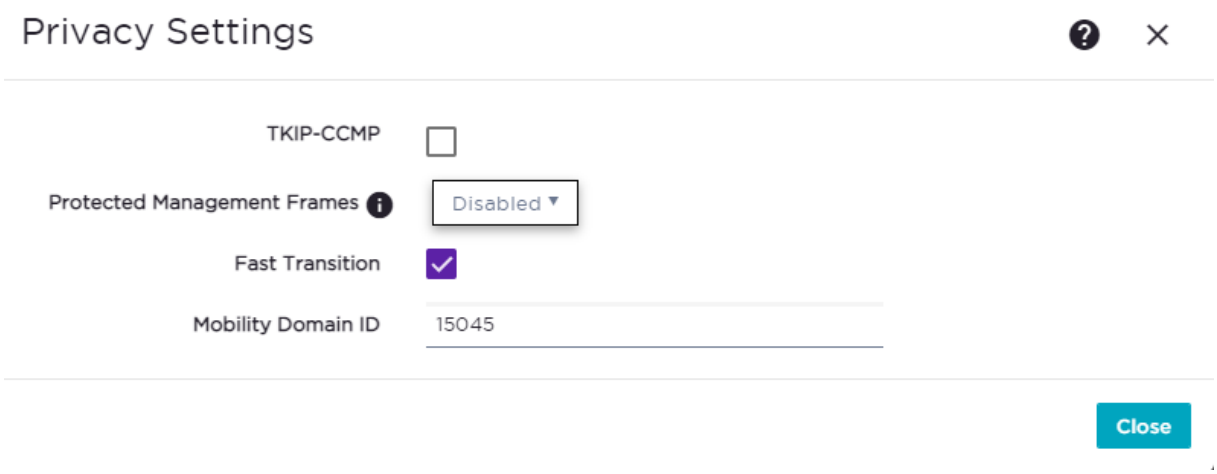
Privacy settings for WPA2-PSK, AES encryption.

Security settings (802.1X / PEAP-MSCHAPv2)



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

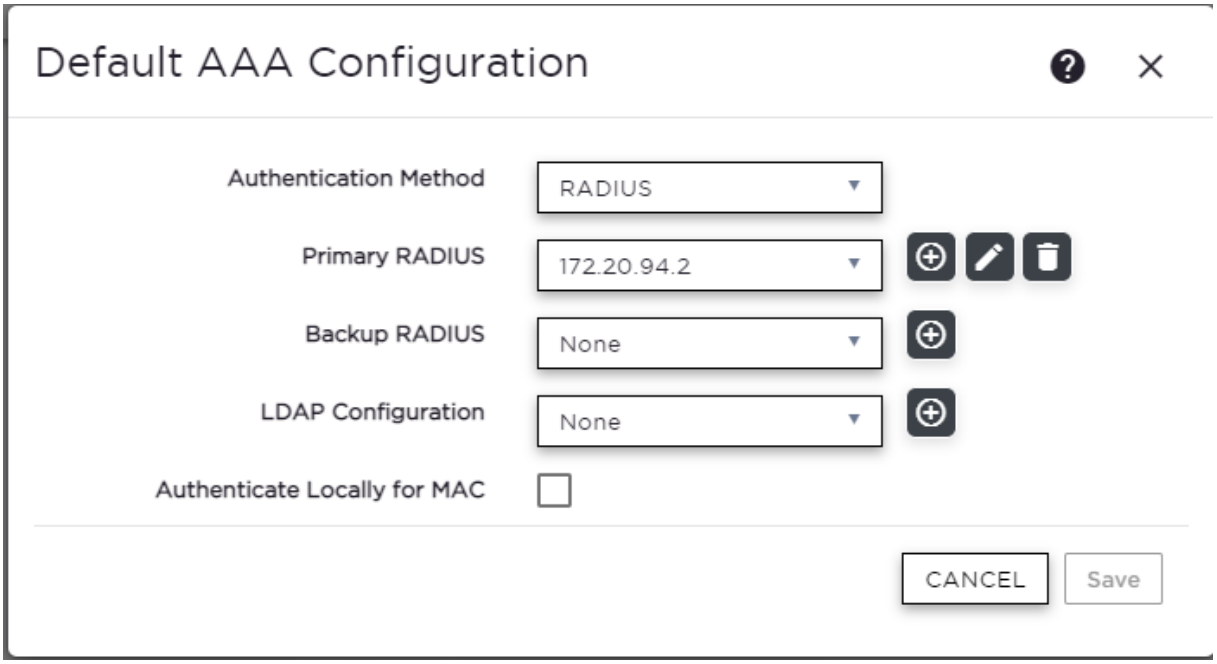
- Select WPA2-Enterprise (802.1X/EAP)



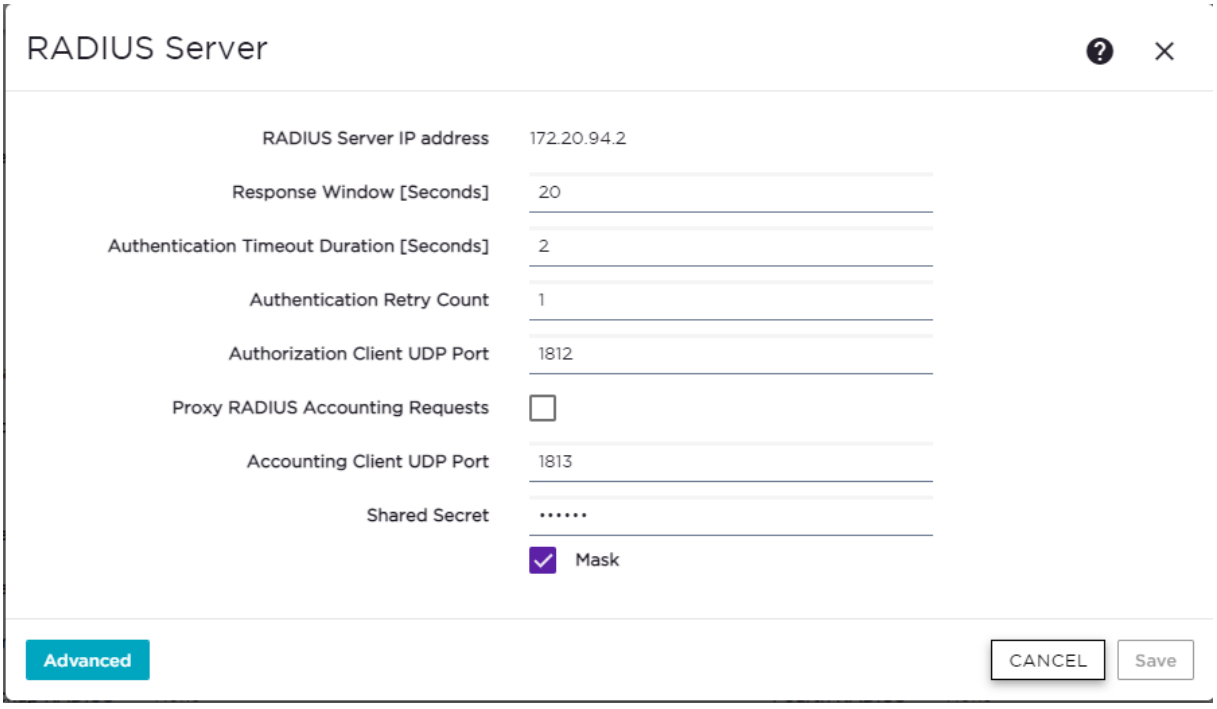
Privacy settings for WPA2-Enterprise (802.1X/EAP)

- Make sure Fast Transition is enabled (Mandatory given the documented problem with OKC)

.



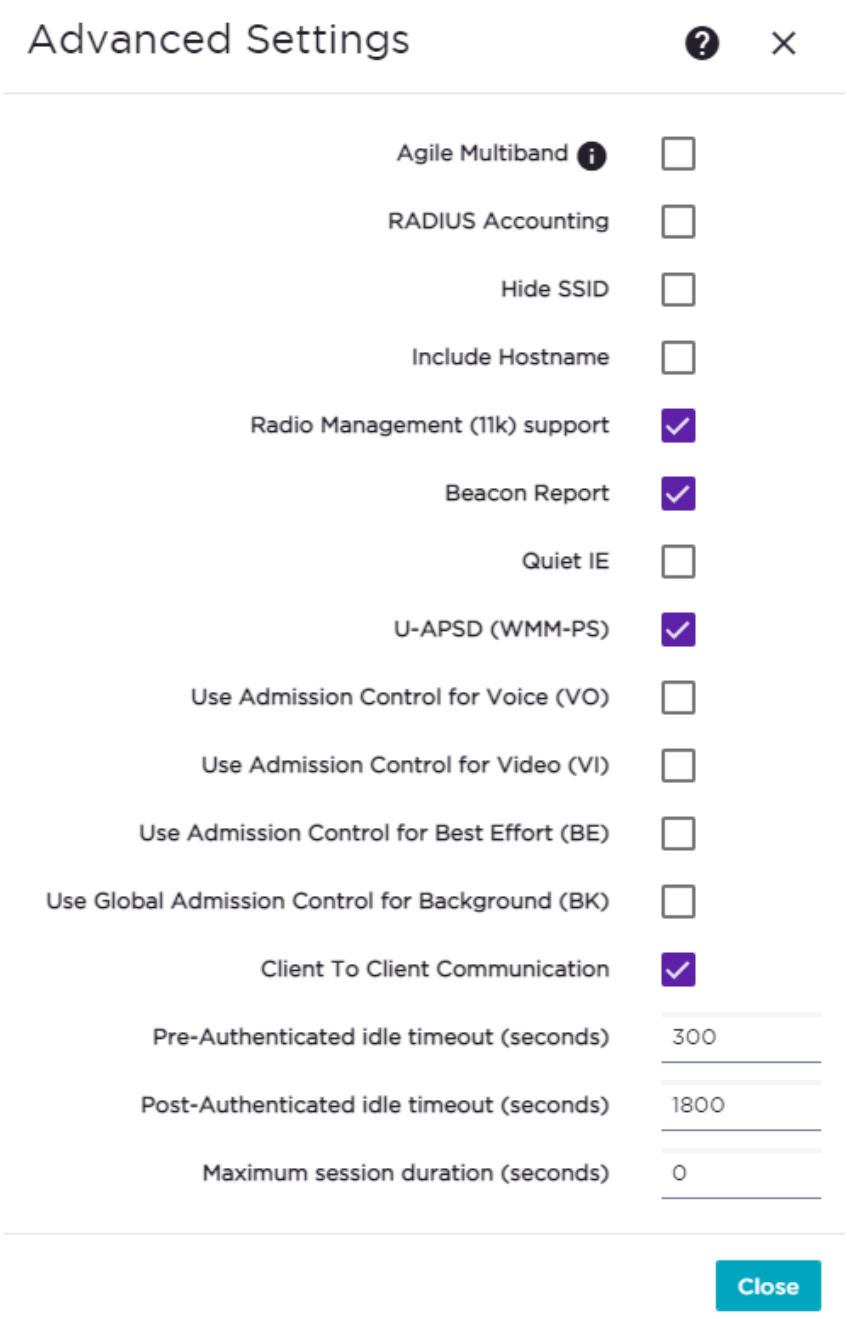
Configuration of authentication using external Radius server (Step 2). Select the server to use. The server is created/configured in next step.



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.

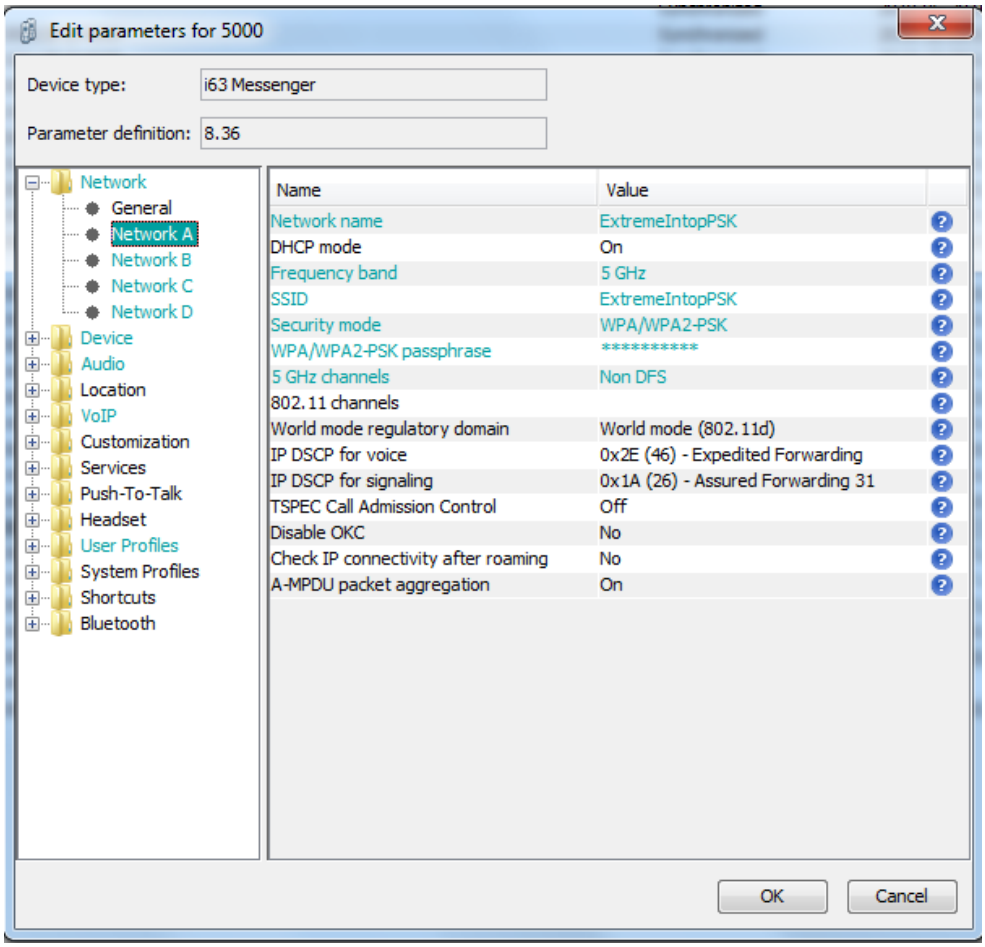
Note. Depending on which Authentication method used it might be necessary to add a certificate into the i63.



PEAP-MSCHAPv2 requires a Root certificate and EAP-TLS requires both a Root certificate and a client certificate.

- Make sure that –APSD (WMM-PS) is enabled. U-APSD is mandatory for optimal performance.

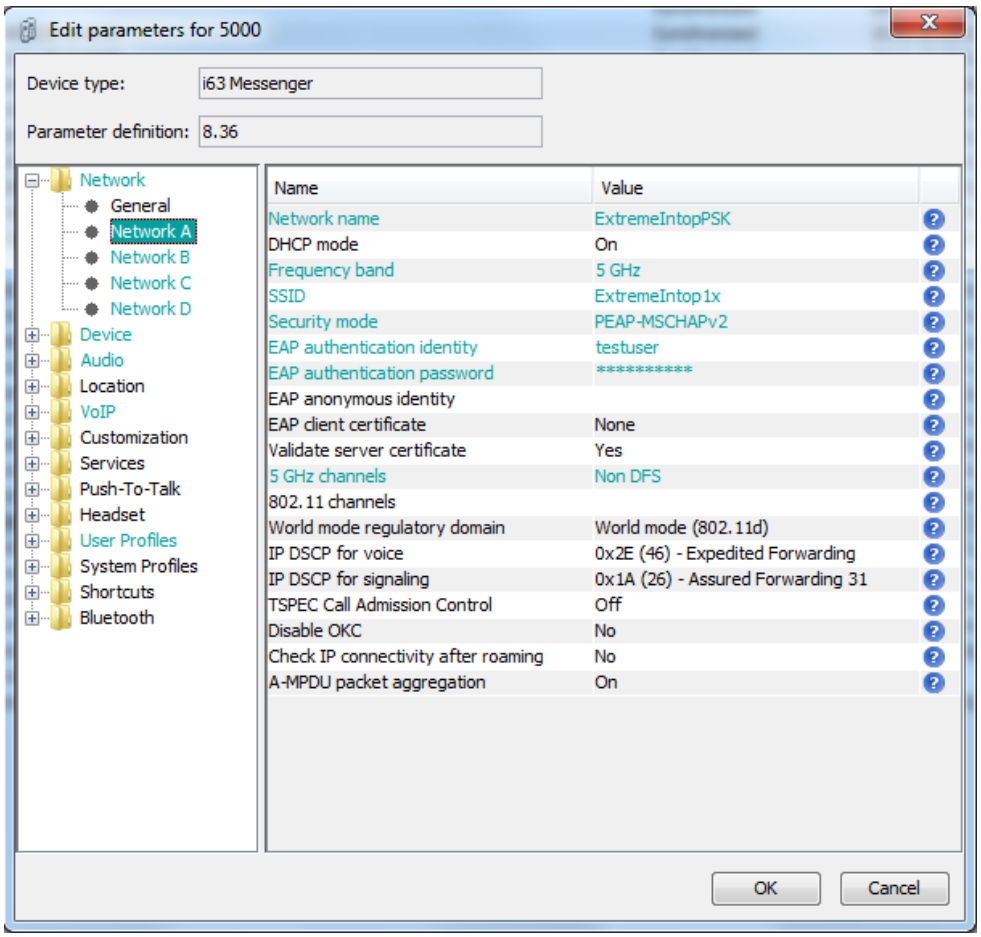
Ascom i63



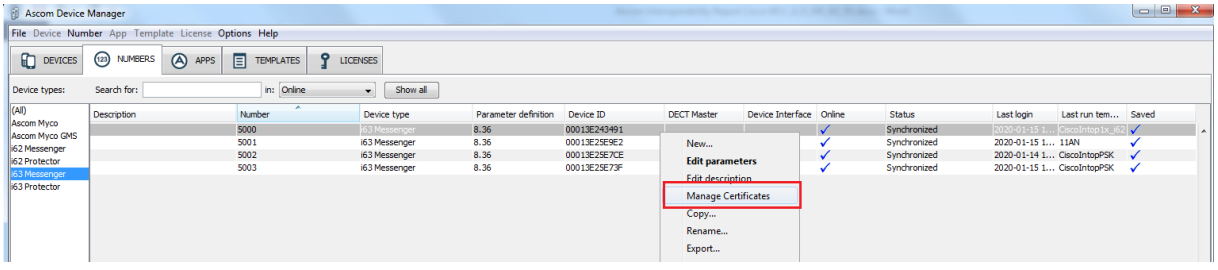
Network settings for WPA2-PSK

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	20
Fail	2
Comments	2
Not verified	2
Total	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	10-Dec-20	SEKMO	Draft
R1	18-Dec-20	SEKMO	Revision R1 after review.