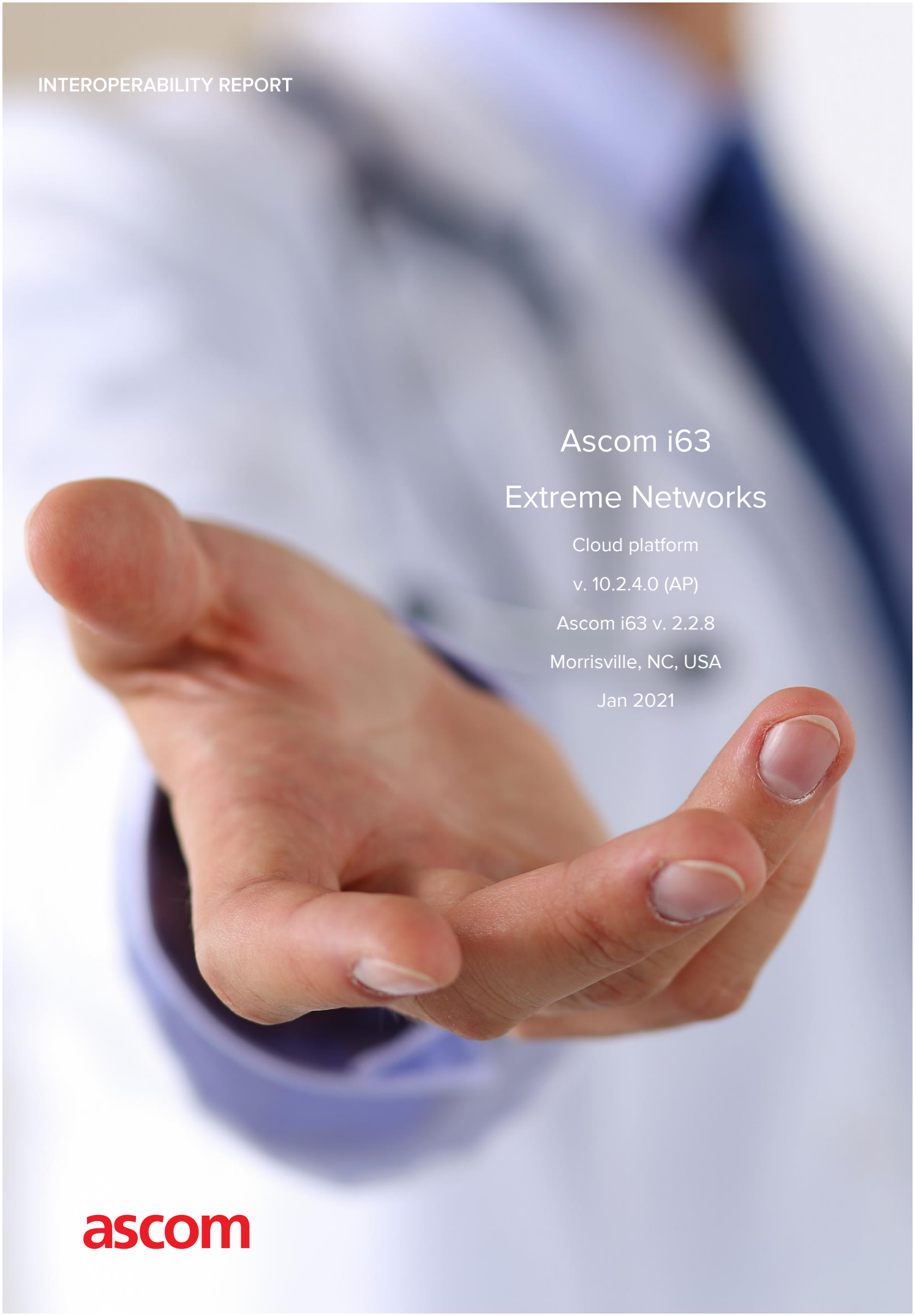
INTEROPERABILITY REPORT



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

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

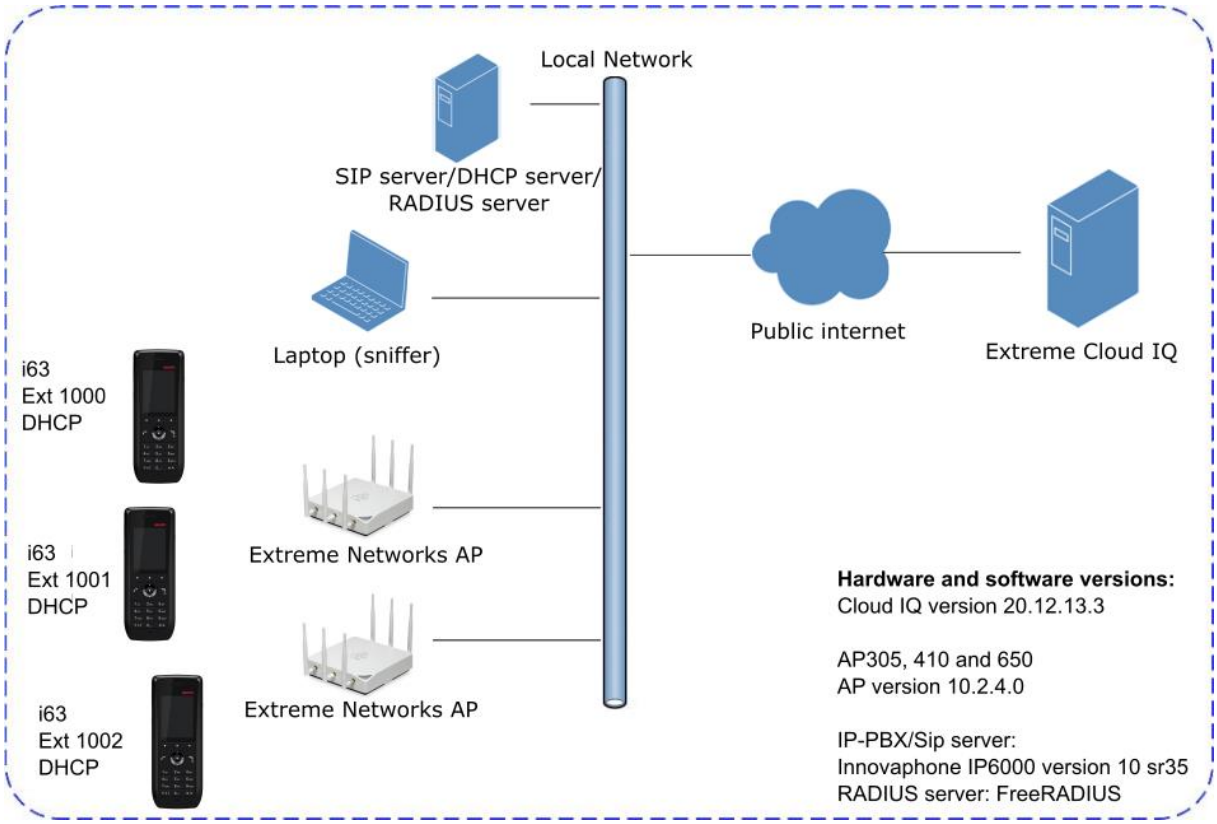
Verification site

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

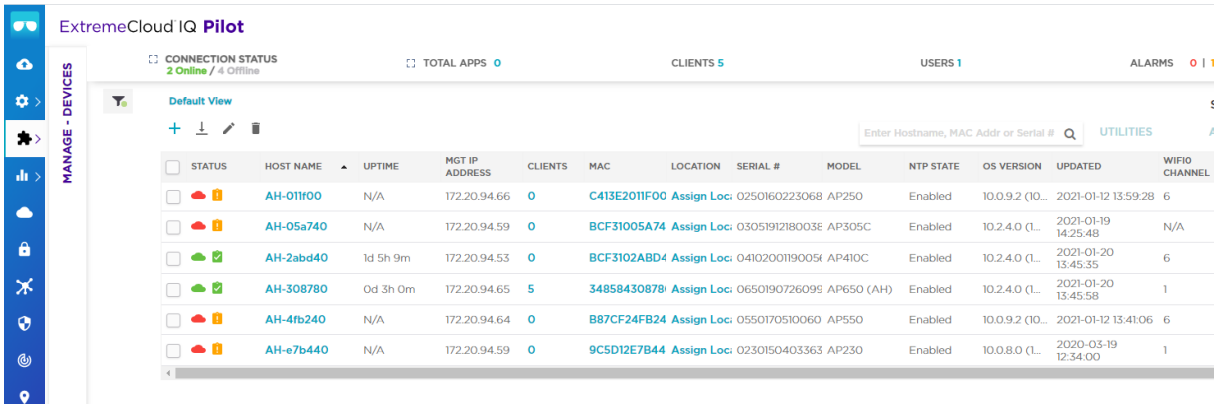
Appendix A: Verification Configurations

Extreme Networks Cloud and Access Points configurations.

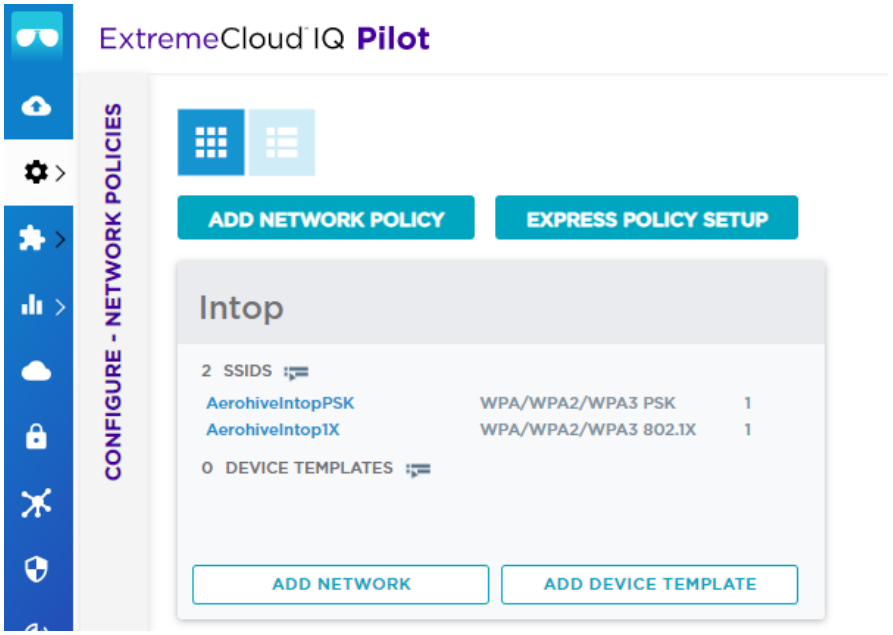
In the following chapter you will find screenshots and explanations of basic settings in order to get the Extreme Networks solution operational with Ascom i63. Please note that security settings were modified according to requirements in individual test cases.

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

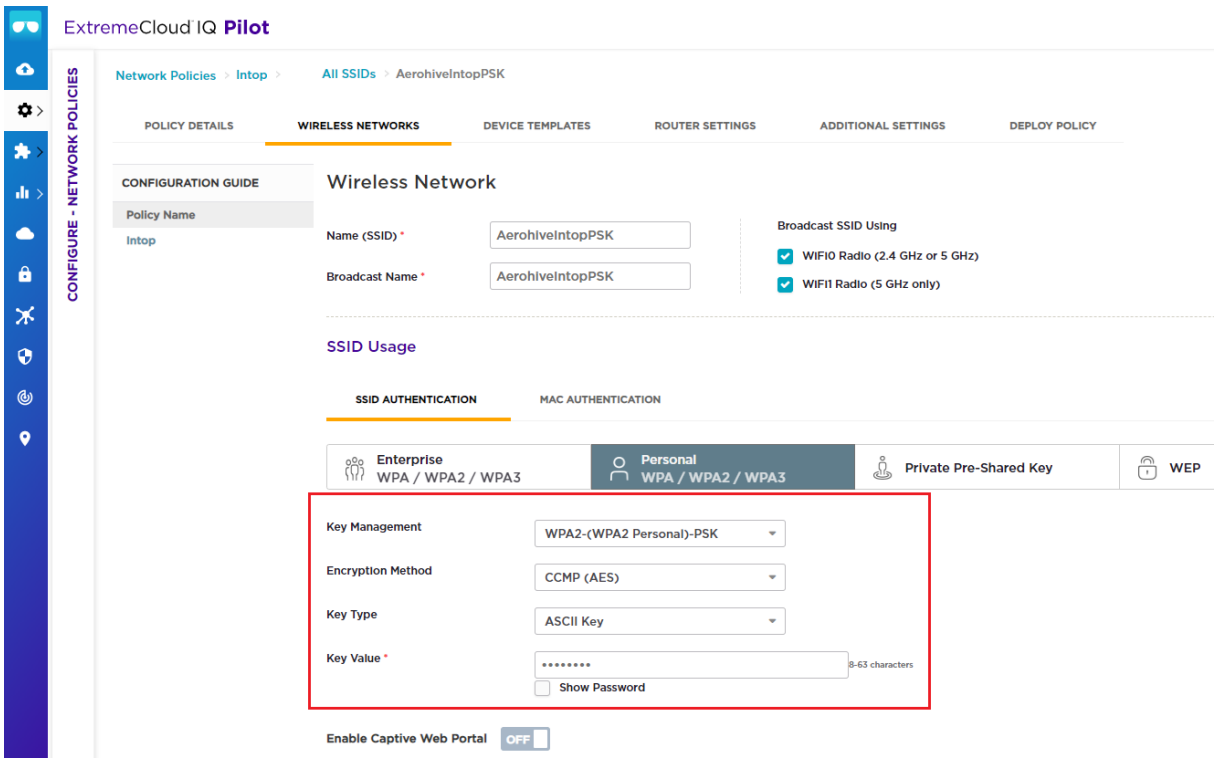
ESS, Security settings.



Dashboard overview (Monitor) of active access points

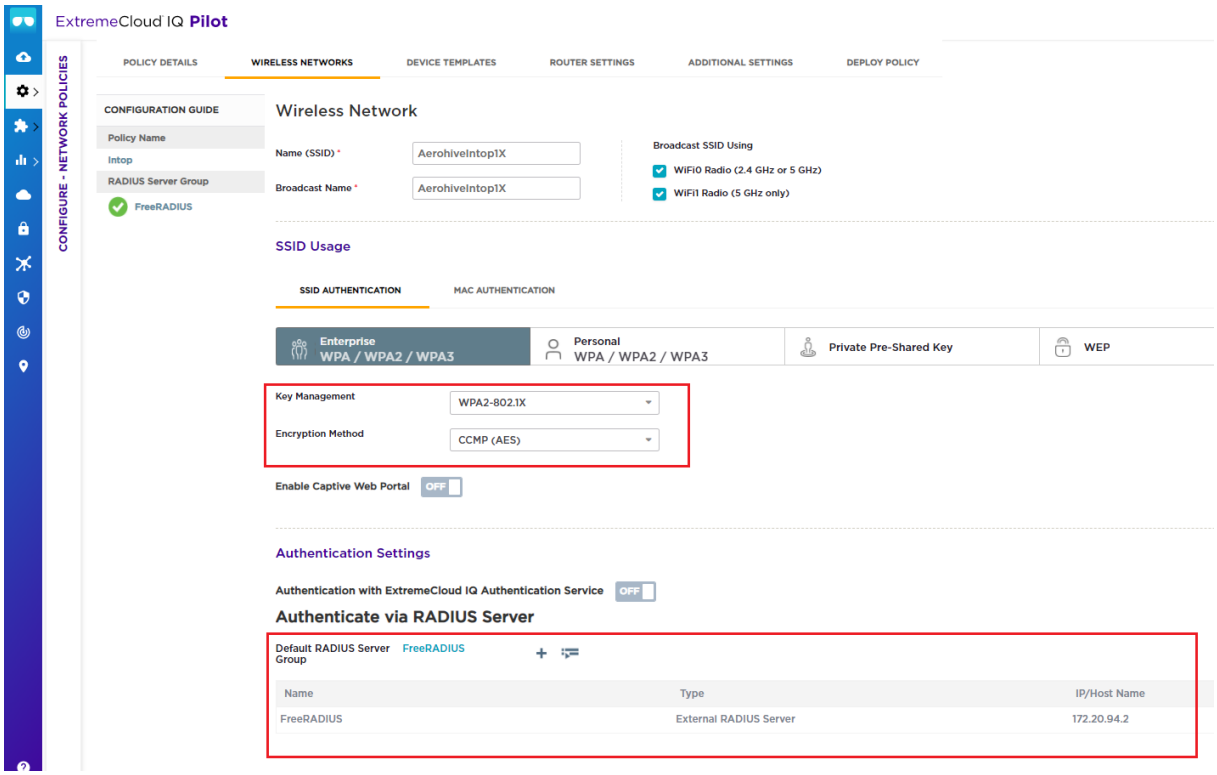


List of all configured SSIDs



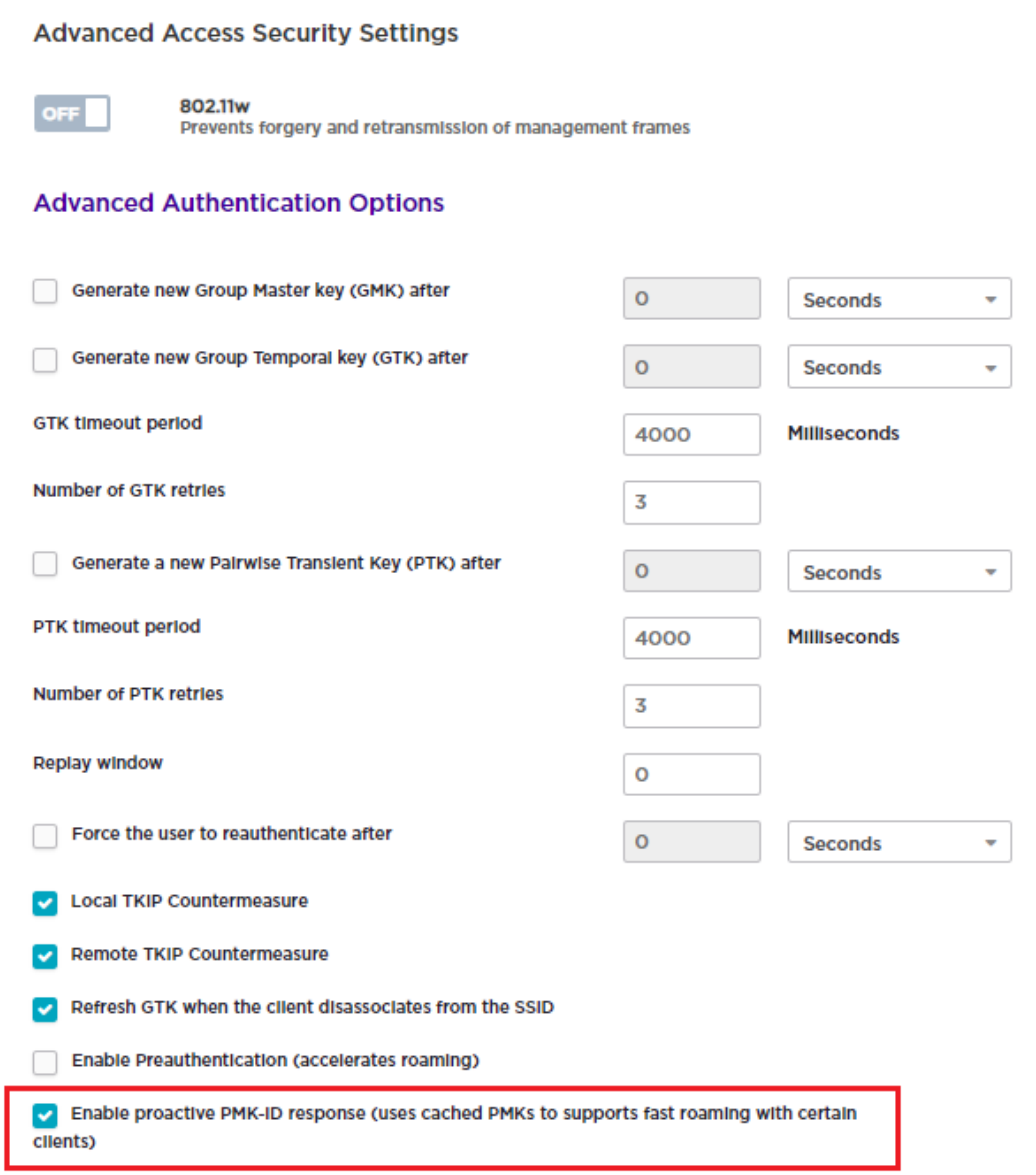
WPA2 PSK (Personal)

- 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.



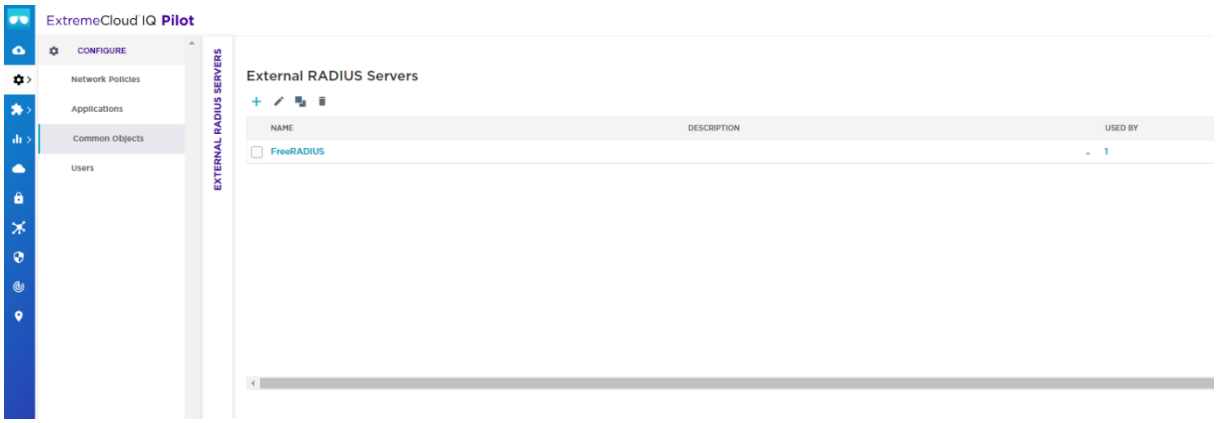
WPA2 802.1X (Enterprise)

- 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)

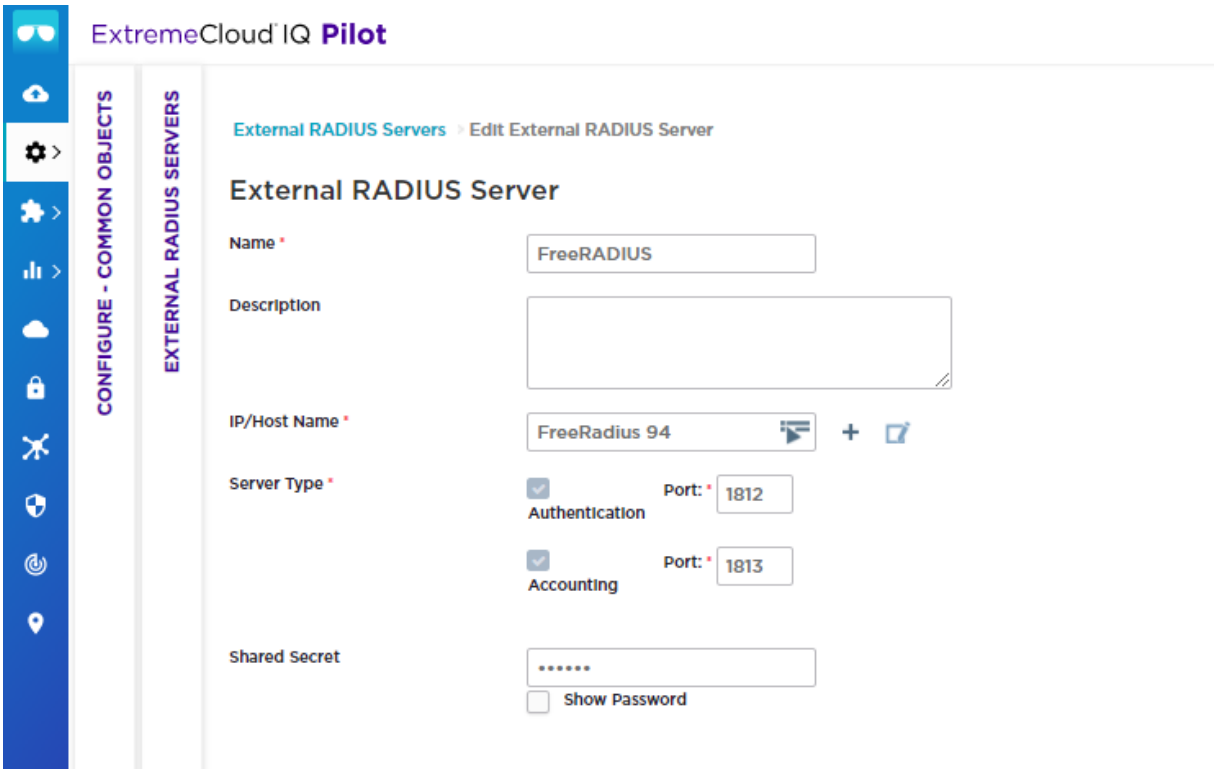


(Enterprise) - Additional settings - Advanced Access Security Controls

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

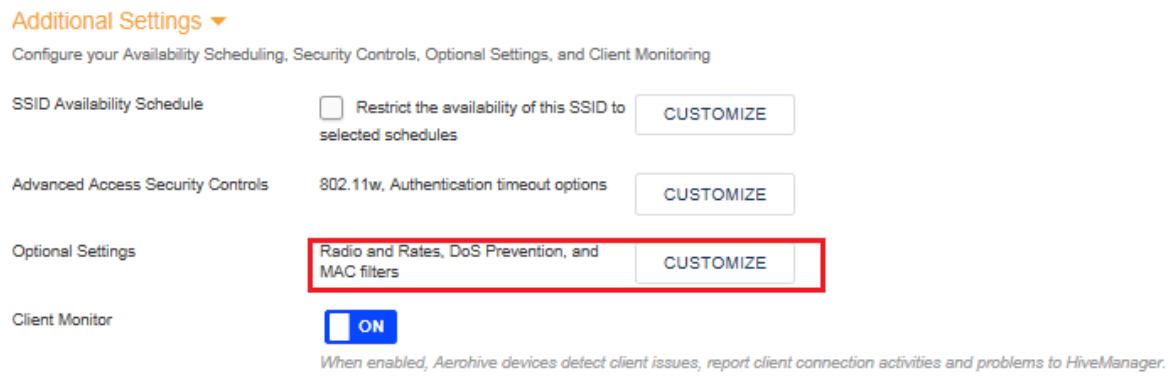


WPA2 802.1X (Enterprise) – RADIUS configuration



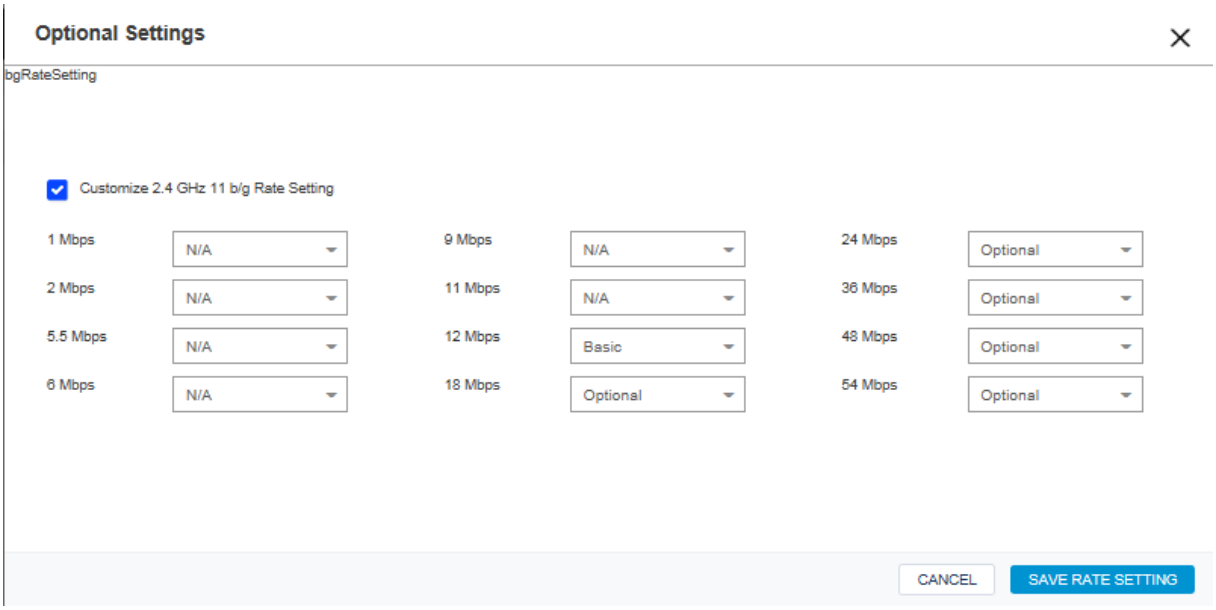
WPA2 802.1X (Enterprise) – RADIUS configuration

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



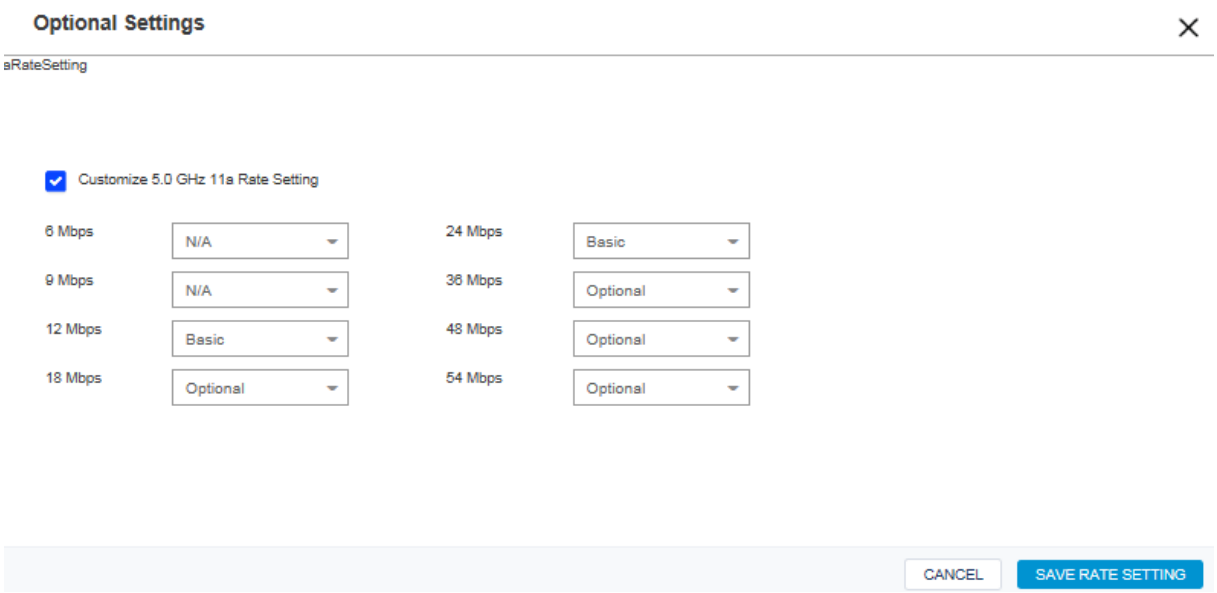
Data rate configuration. (Per SSID)

- Go to optional Settings



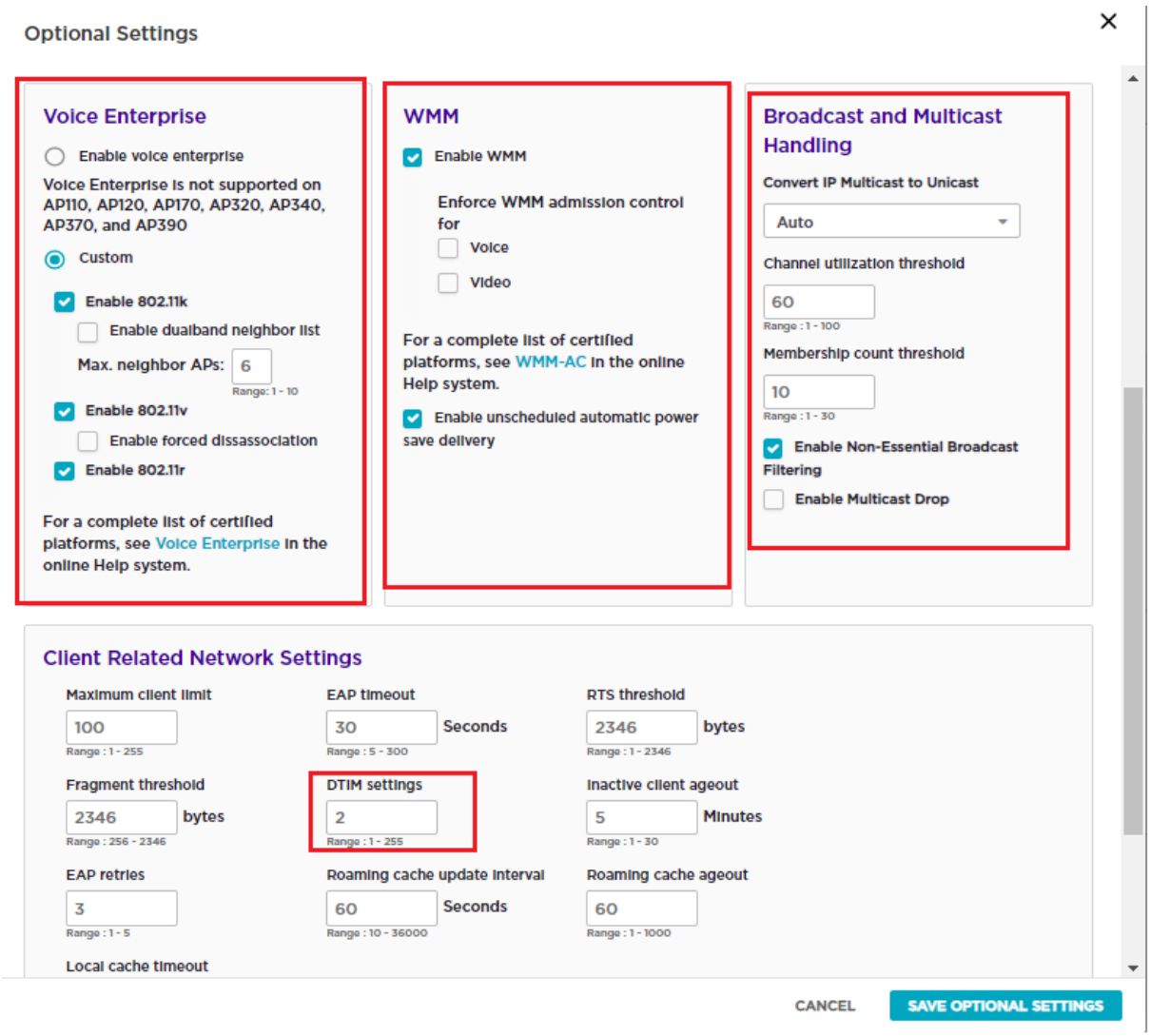
Data rate configuration.2.4GHz

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



Data rate configuration.5GHz

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

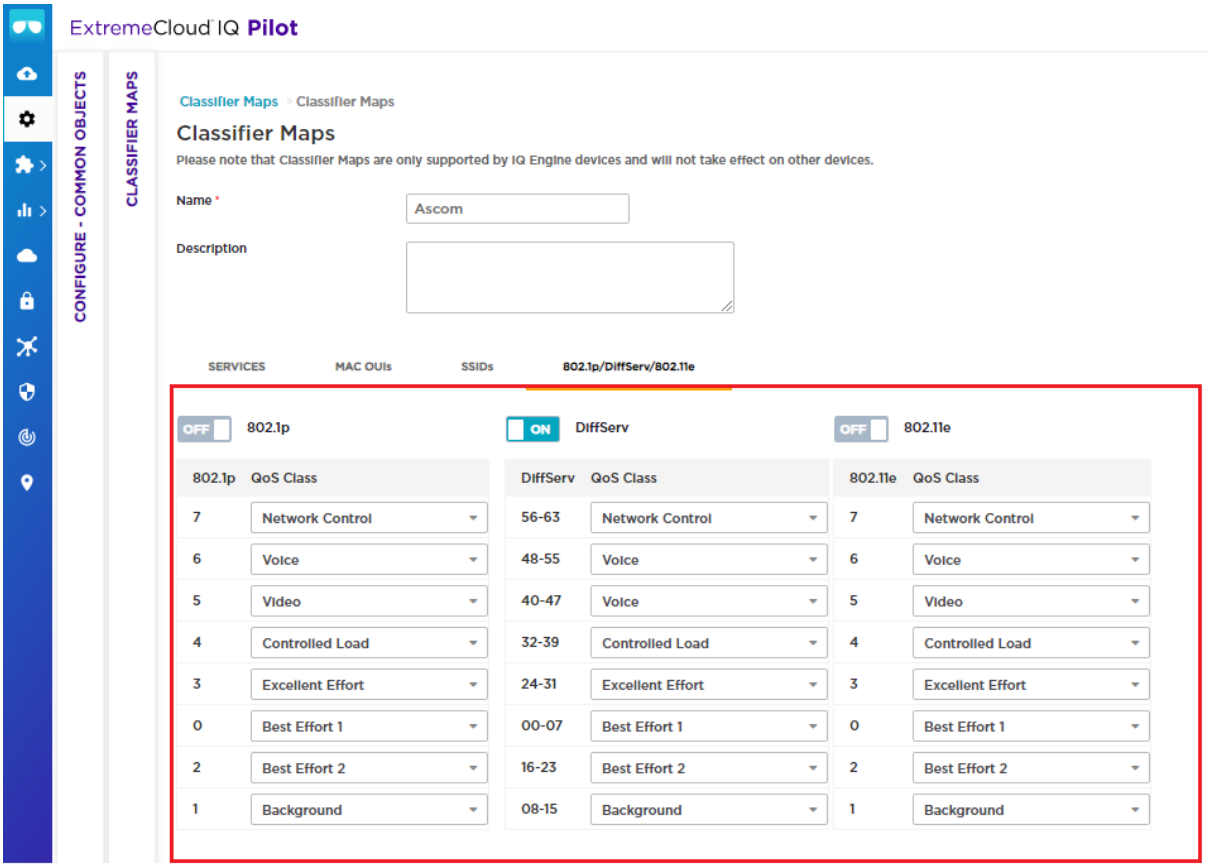


Optional SSID settings

- 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.

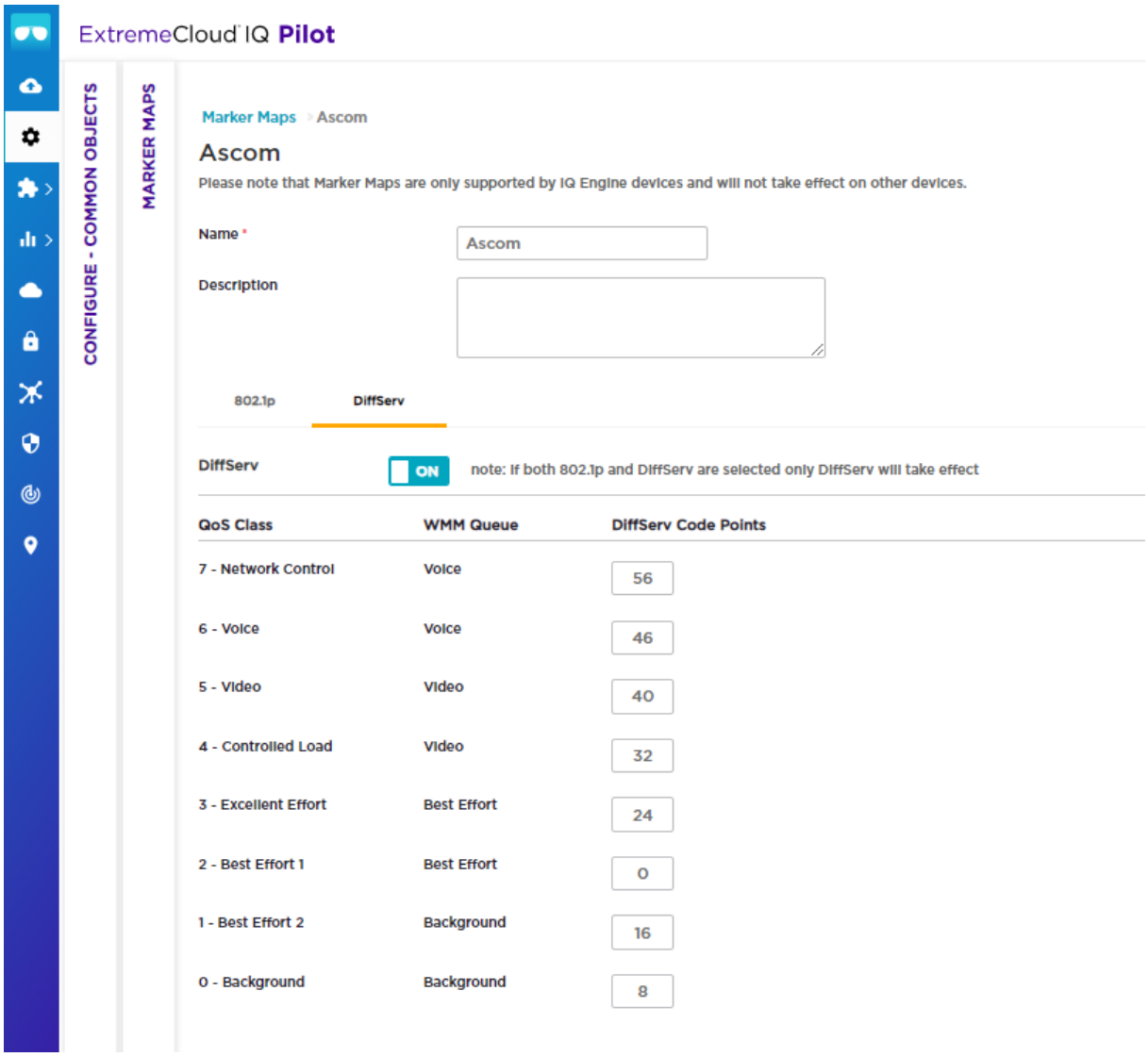
- Make sure Enable WMM is checked.
- Make sure Unscheduled Automatic Power Save Delivery is checked.
- Make sure “Convert IP Multicast to Unicast” is enabled

- Ascom recommends a DTIM period of at least 2 but no higher than 5.



Classifier Maps

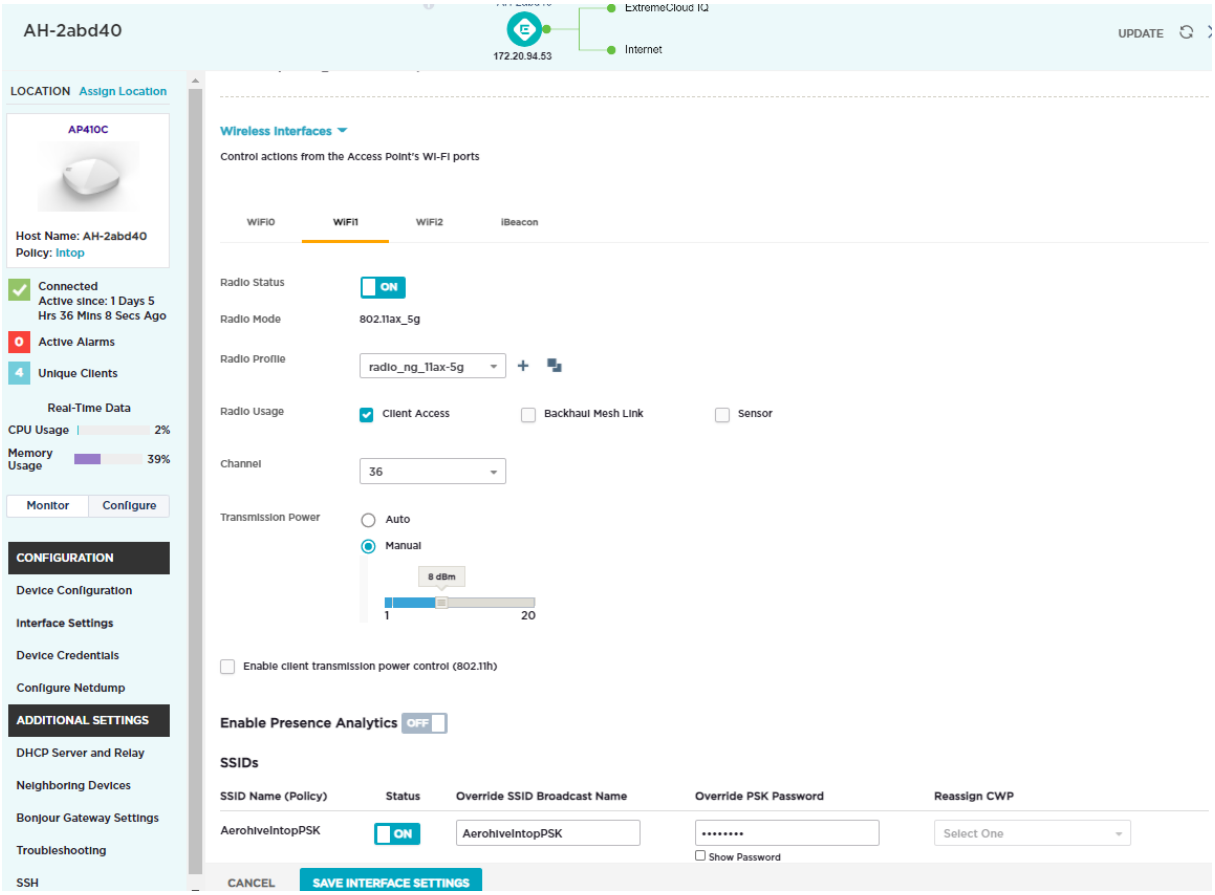
- Create classifier map according to the screenshot and enable DiffServ and 802.11e
- **Important. For DiffServ 40-47 select QoS Class: 6 – Voice.**



Marker Maps

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

Radio Configuration



Configuration of access points

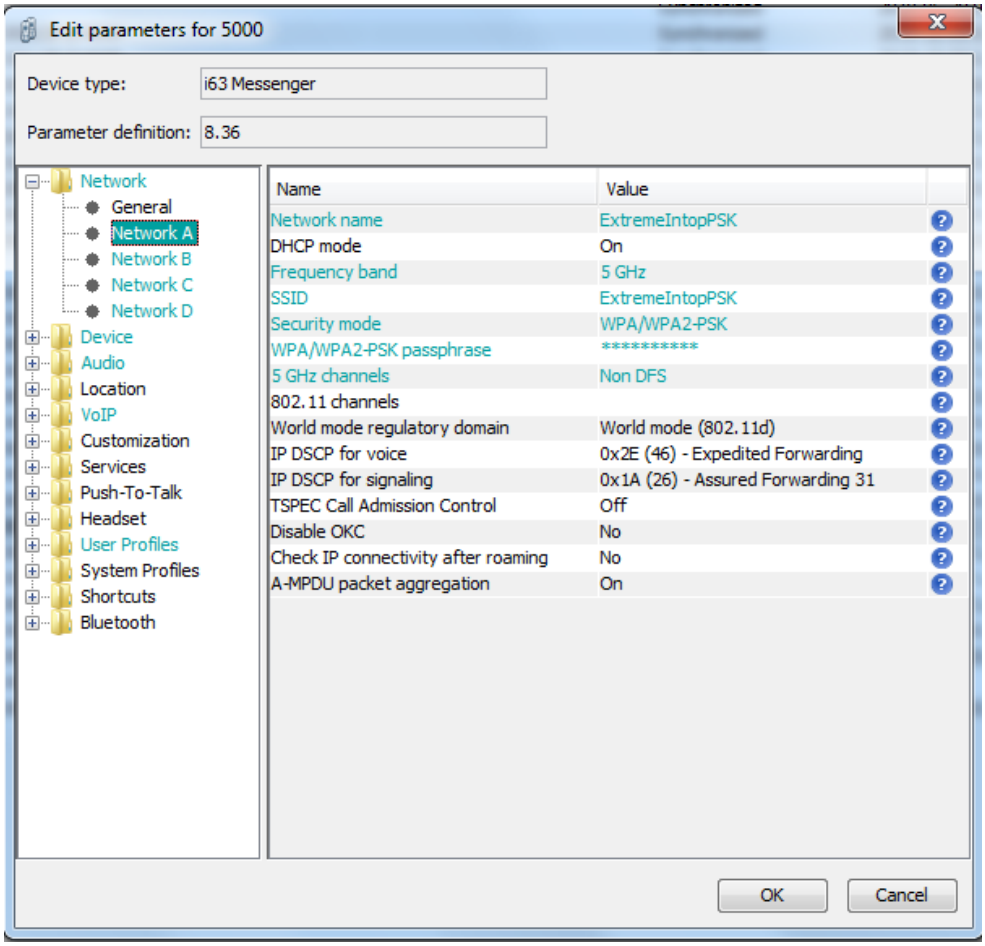
- Radio profiles used is the default (Default radio profiles **radio_ng_11ax-5g** and **radio_ng_11ax-2g** for WiFi0 interface).
- In the example channel and Transmission power has been set manually for each access point (for testing).

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)

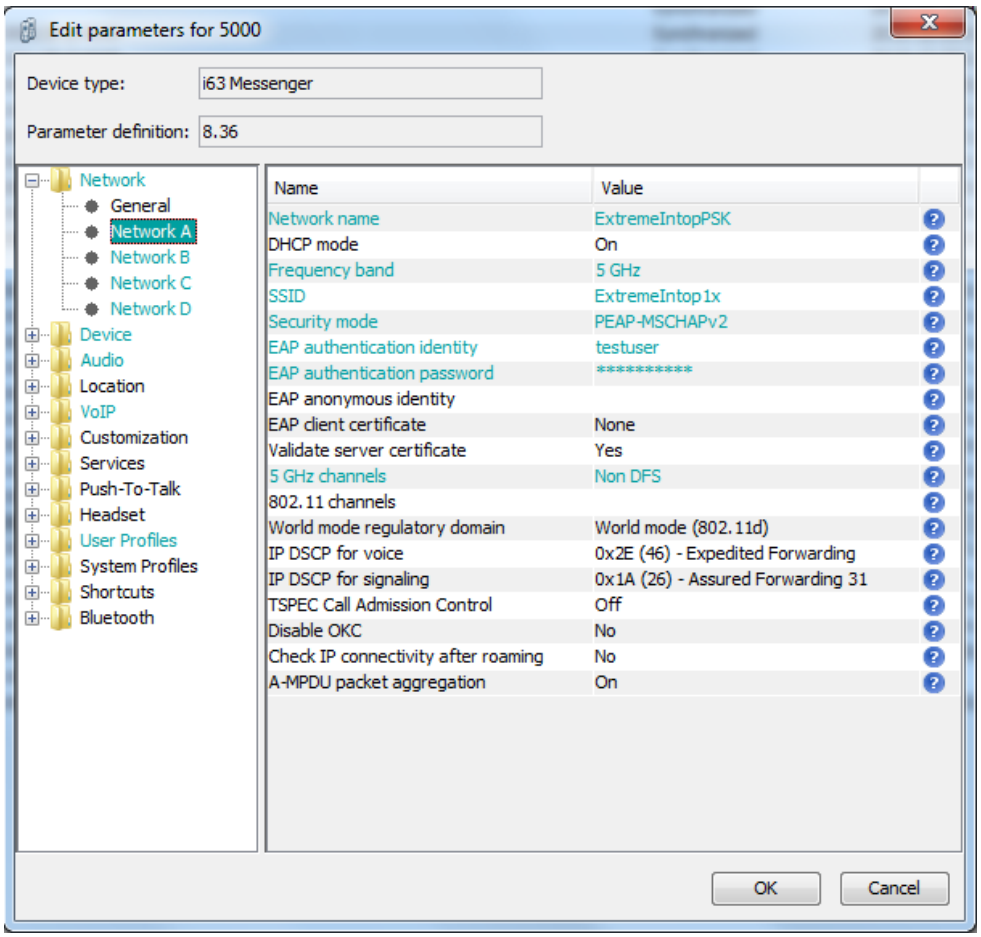
Ascom i63



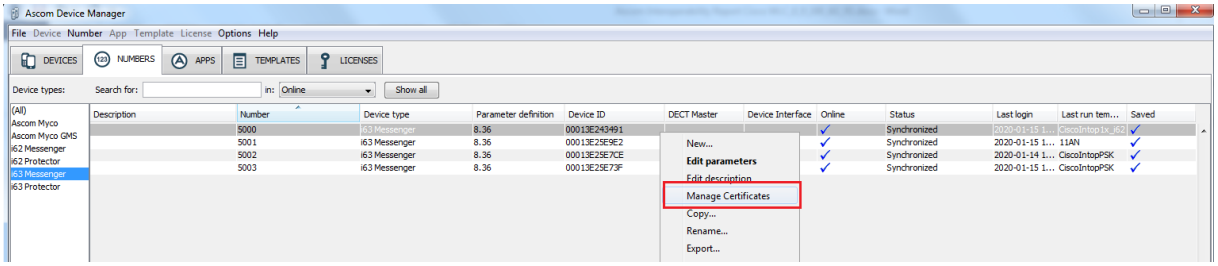
Network settings for WPA2-PSK

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: Interoperability Verification Records

Pass	18
Fail	0
Comments	4
Not verified	4
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	26-Jan-21	SEKMO	Draft
R1	02-Feb-21	SEKMO	Minor corrections after review.