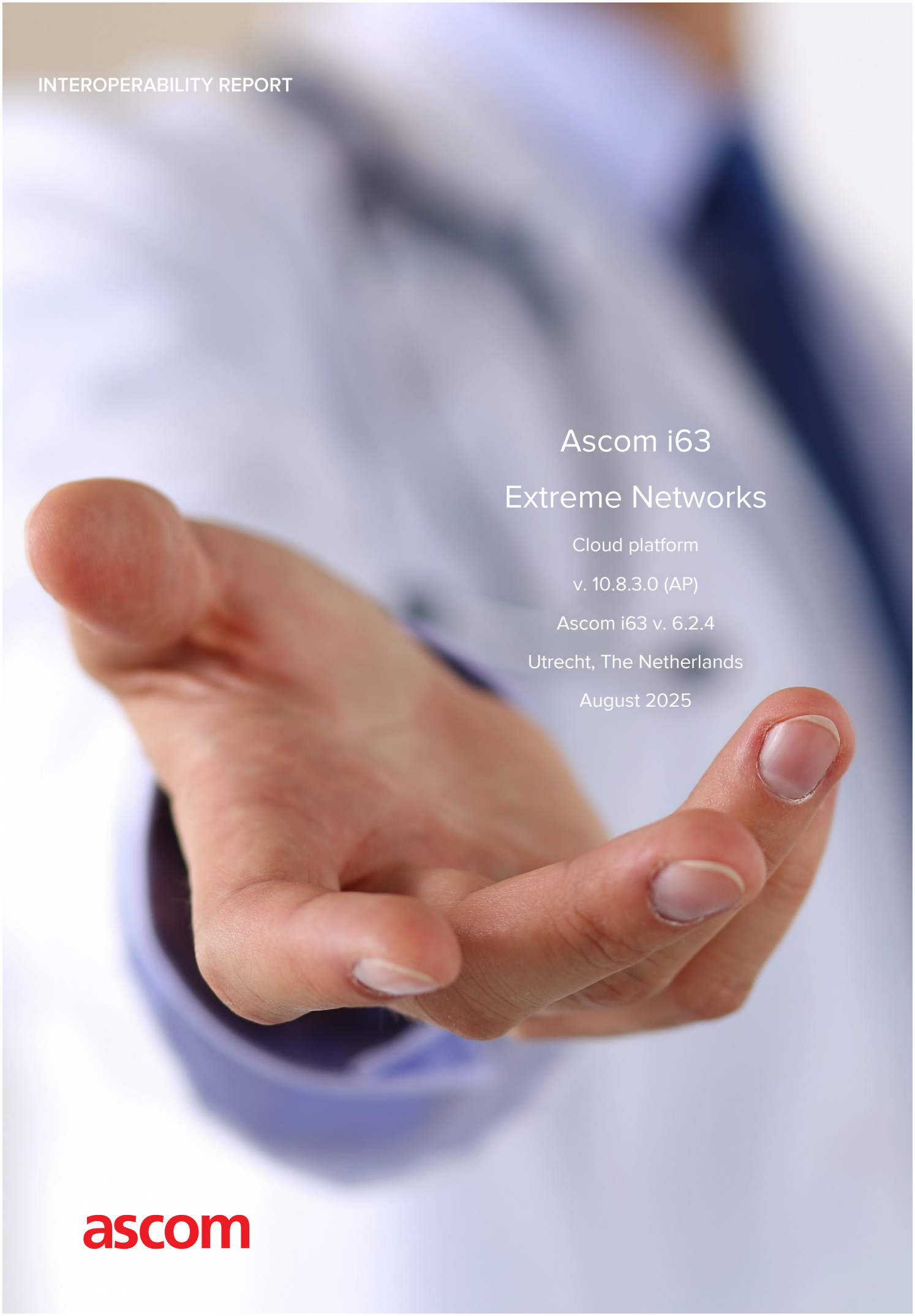
INTEROPERABILITY REPORT



Ascom i63

Extreme Networks

Cloud platform

v. 10.8.3.0 (AP)

Ascom i63 v. 6.2.4

Utrecht, The Netherlands

August 2025

ascom

Contents

Introduction **3**

About Ascom 3

About Extreme Networks 3

Verification site 4

Participants 4

Verification topology 4

Summary **5**

General conclusions 5

Verification overview 6

Known limitations 7

Appendix A: Verification Configurations **8**

Extreme Networks Cloud and Access Points configurations. 8

WPA2 PSK (Personal) 8

WPA3 SAE (Personal) 10

WPA2 802.1X (Enterprise) 11

WPA3 802.1X (Enterprise) 12

802.1X (Enterprise) – External Radius Server Configuration 13

Ascom i63 v. 6.2.4 Network Settings 21

Appendix B: Interoperability Verification Records **25**

Document History **25**

Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Extreme Networks CloudIQ 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 and retail sectors.

Ascom is headquartered in Baar (Switzerland), has operating businesses in 19 countries and employs around 1,400 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

About Extreme Networks

Since our founding in Silicon Valley in 1996, Extreme Networks (EXTR) has been on the forefront of technological innovation. During the past 25+ years, we've grown to more than $1.3 billion in annual revenue and more than 2,700 dedicated employees worldwide.

At Extreme Networks, we simplify and secure connectivity to enhance value, drive innovation, accelerate growth, and provide peace of mind. Trusted by tens of thousands of customers globally, we deliver AI-native cloud networking solutions that seamlessly connect people, applications, data, and devices.

Our comprehensive portfolio includes intelligent cloud management, security, and analytics capabilities. Whether your needs are cloud-based, on-premises, or at the edge, our solutions are designed to run anywhere and can be managed through a single, unified platform. Our customer-first services and flexible licensing options ensure that you can easily adapt and scale your network as your business grows.

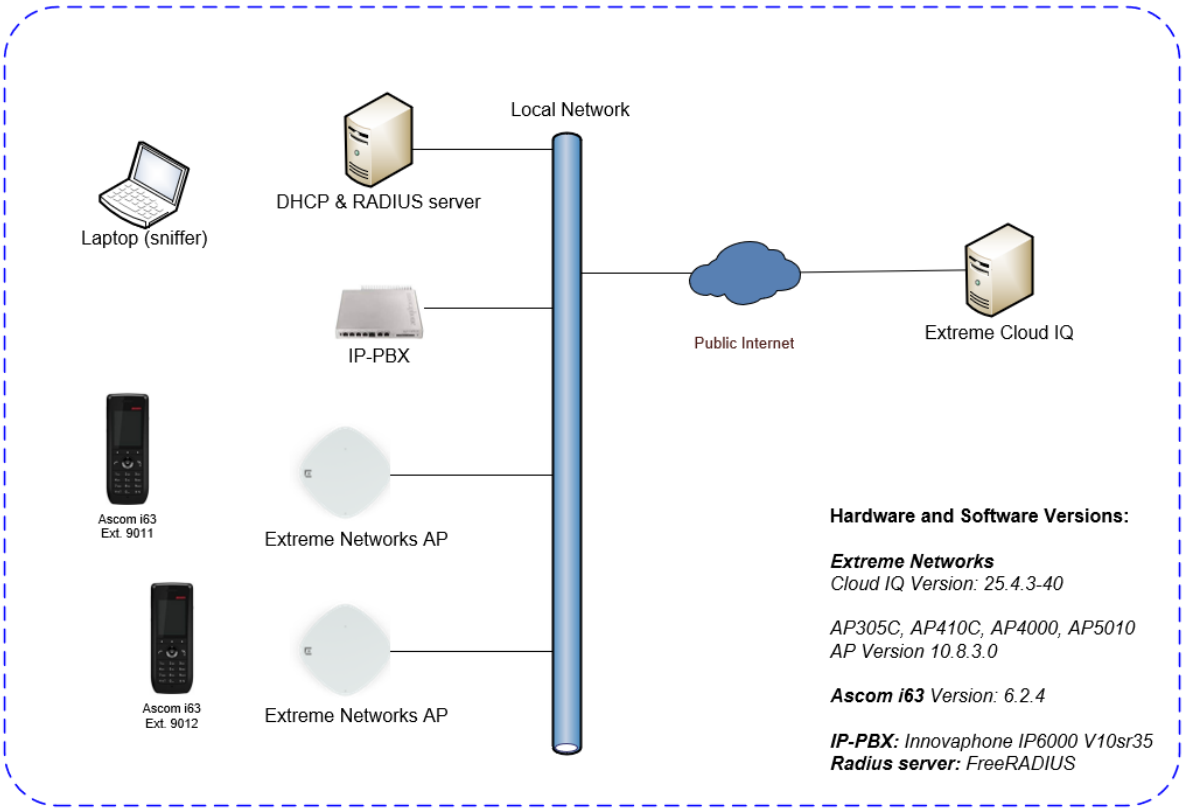
Verification site

Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

Participants

Remco van den Pangaart, Ascom,

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 WPA2, PSK and 802.1X (FT and non-FT) were excellent and were in the range of 30 ms for all combinations. WPA3 roaming times were longer when using SAE and 802.1X without 802.11r/FT, averaging between 97 and 138 ms. However, enabling 802.11r/FT significantly improved performance, reducing roaming times to between 26 and 38 ms. As such, enabling 802.11r is recommended to optimize roaming efficiency in WPA3 environments

Compatibility information

To ensure representative coverage across product generations and groups, one access point model was selected from each category: **305, 410, 4000, and 5010**. By testing these models, we effectively cover the performance characteristics of all access point models listed below.

Supported Partner Access Points running version 10.8.3.0:

AP305c/305cx

AP410c

AP460c

AP510c/510cx

AP650/650x

AP4000

AP5010

Verification overview

WLAN Compatibility and Performance

High Level Functionality	Result	Comments
Association with WPA2-PSK / AES Encryption	OK	
Association with PEAP-MSCHAPv2 Auth, AES Encryption	OK	
Association with EAP-TLS authentication	OK	
Association with WPA3-Personal	OK	
Association with WPA3-Enterprise	OK	
Association, Multiple ESSIDs	OK	
Beacon Interval and DTIM Period	OK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	OK	
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 27ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 22ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 29ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 25ms
Roaming with WPA3-Personal	OK	Typical roaming time 97ms
Roaming with WPA3-Personal, 802.11r/FT	OK	Typical roaming time 26ms
Roaming with WPA3-Enterprise	OK	Typical roaming time 128ms
Roaming with WPA3-Enterprise, 802.11r/FT	OK	Typical roaming time 35ms
Channel usage controlled by 802.11k	OK	
Association with Protected Management Frames 802.11w	OK	

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

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

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

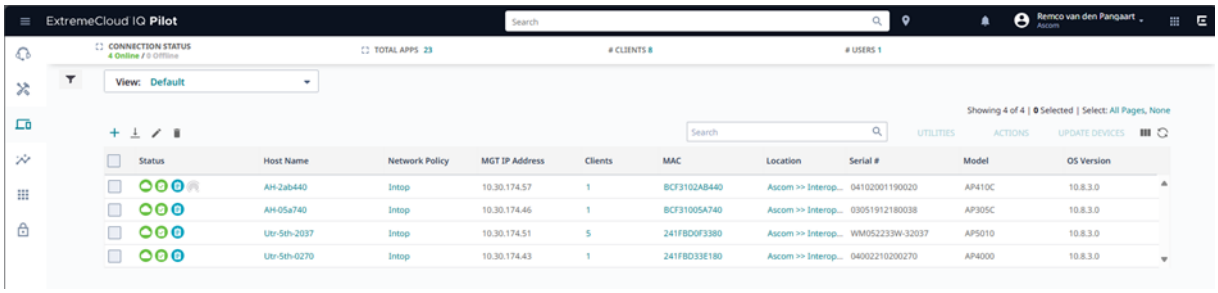
Appendix A: Verification Configurations

Extreme Networks Cloud and Access Points configurations.

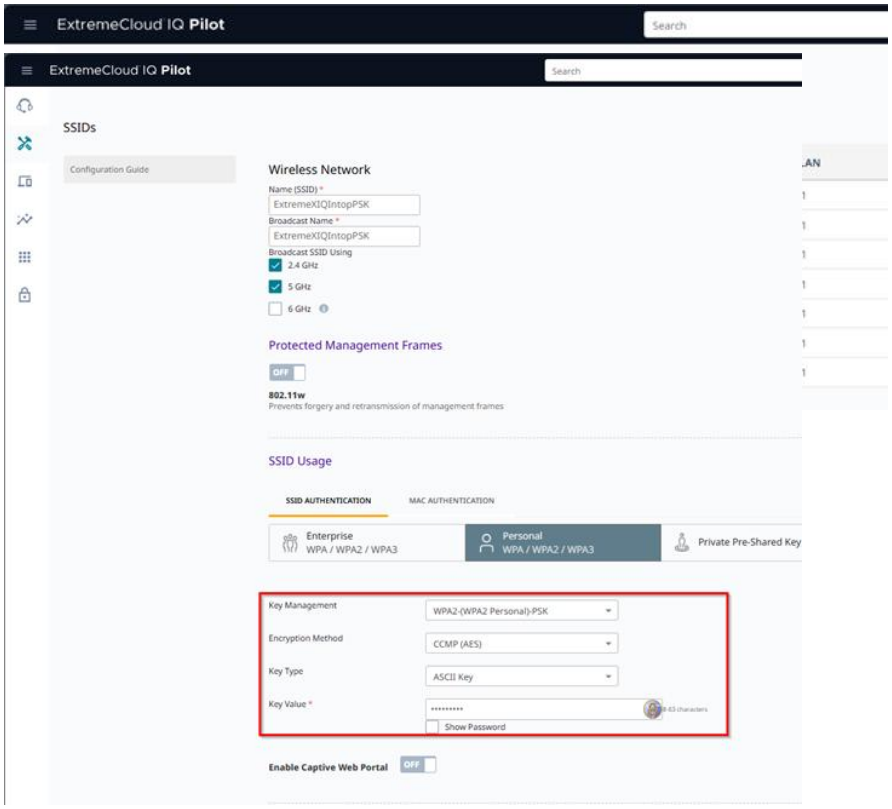
In the following chapter you will find screenshots and explanations of basic settings to get the Extreme Networks solution operational with Ascom i63. Please note that security settings were modified according to requirements in individual test cases.

ESS, Security settings.

Dashboard overview (Monitor) of active access points



List of all configured SSIDs

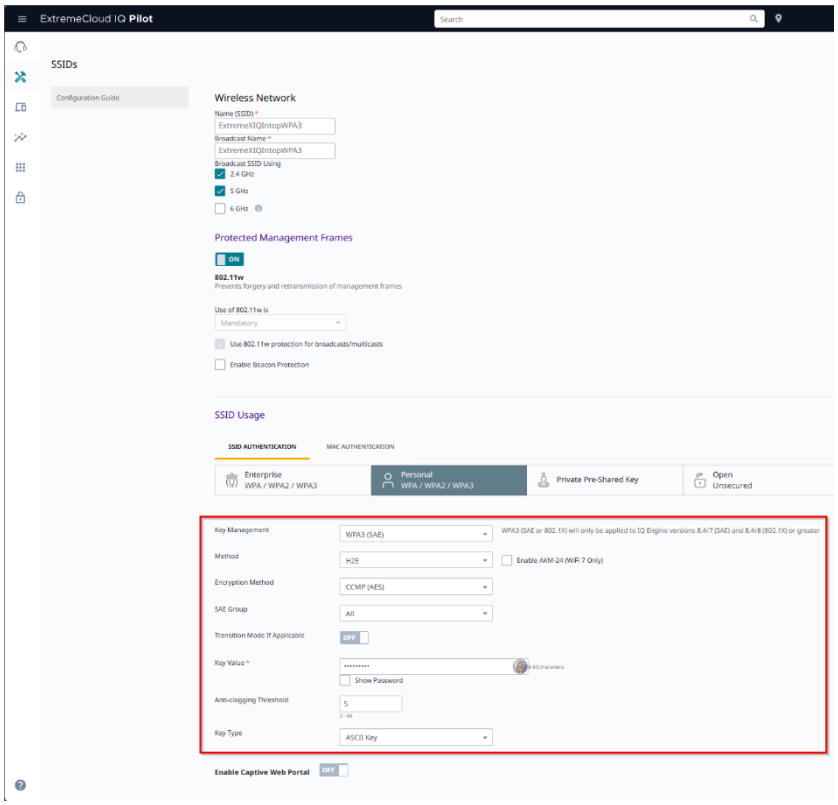


WPA2 PSK (Personal)

WPA2 PSK (Personal)

- Select WPA/WPA2/WPA3 (Personal)
- Select WPA2-(WPA2 Personal)-PSK as Key Management.
- Select CCMP (AES) as Encryption Method.
- Key can be entered in HEX or in ASCII format. Example shows a key entered in ASCII format.

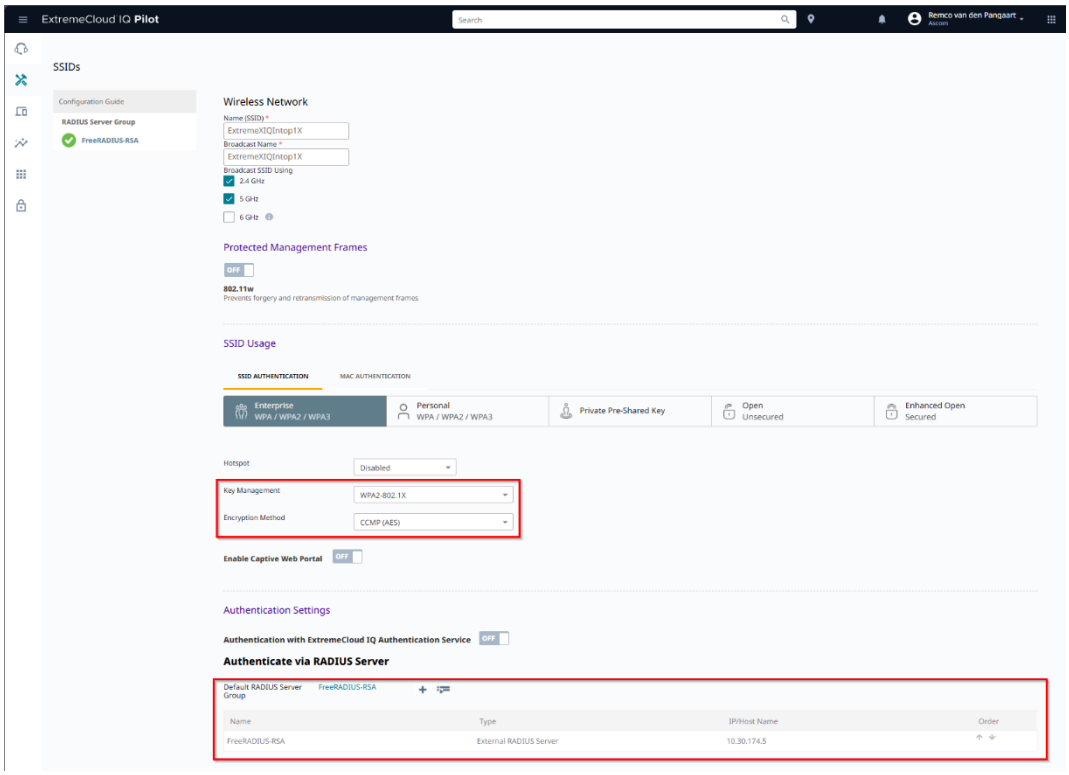
WPA3 SAE (Personal)



WPA3 SAE (Personal)

- Select WPA/WPA2/WPA3 (Personal)
- Select WPA3 (SAE) as Key Management.
- Select CCMP (AES) as Encryption Method.
- Key can be entered in HEX or in ASCII format. Example shows a key entered in ASCII format.

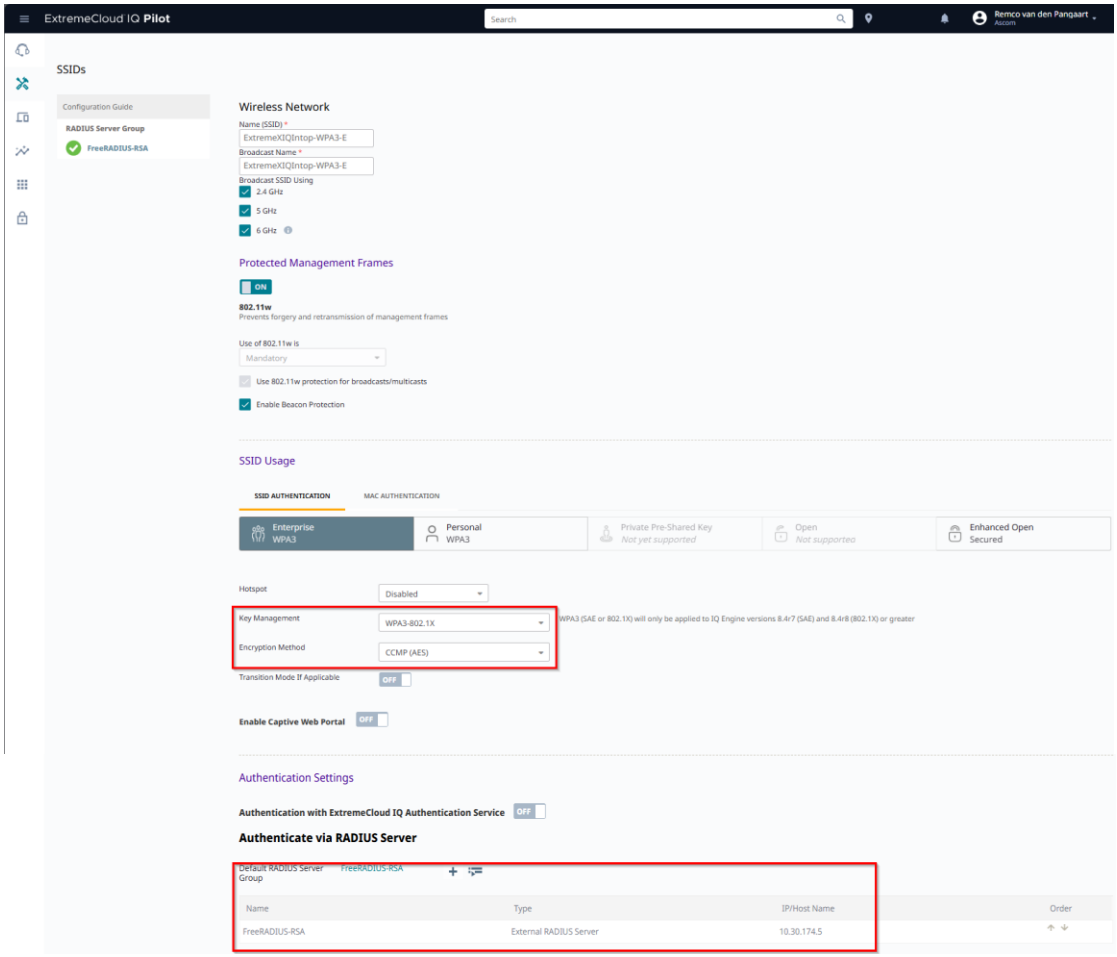
WPA2 802.1X (Enterprise)



WPA2 802.1X (Enterprise)

- Select WPA/WPA2 802.1X (Enterprise)
- Select WPA2-802.1X as Key Management
- Select CCMP as Encryption Method
- Select RADIUS server (defined in step 802.1X (Enterprise) – External Radius Server Configuration).

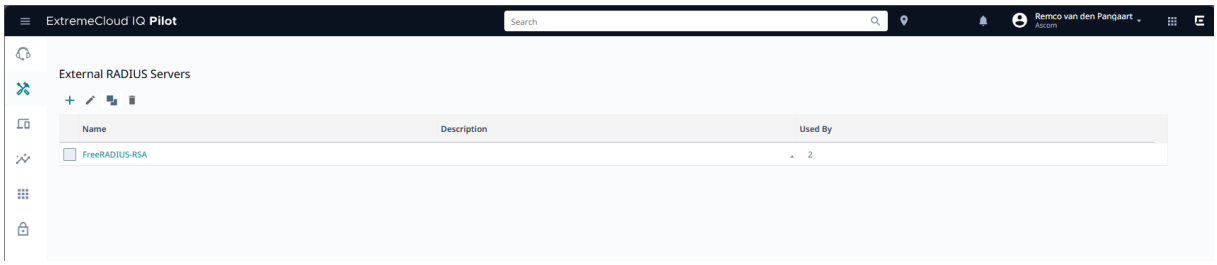
WPA3 802.1X (Enterprise)



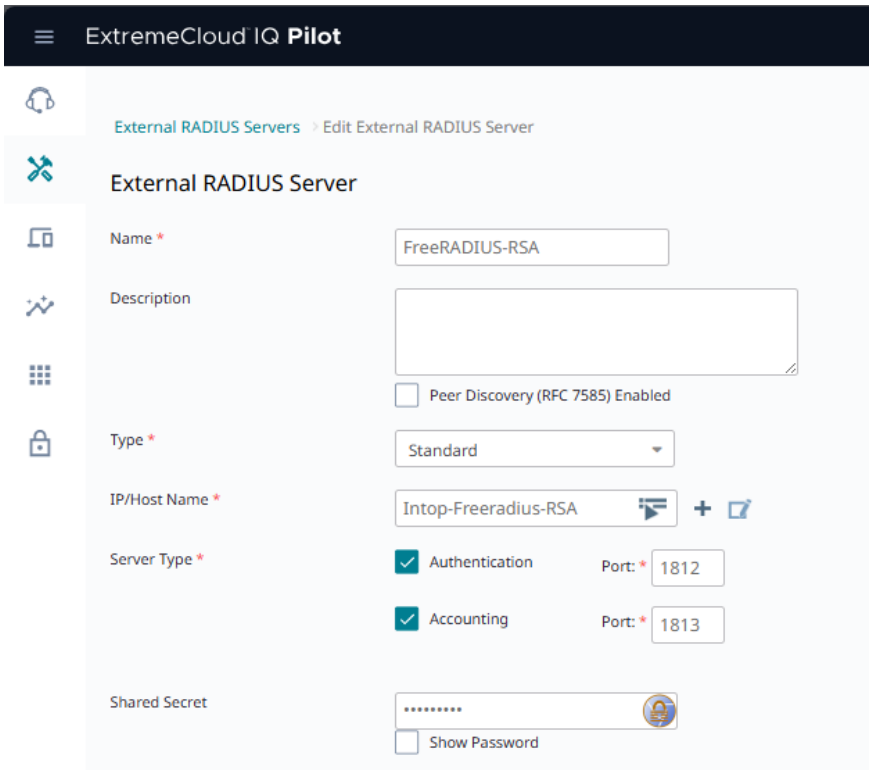
WPA3 802.1X (Enterprise)

- Select WPA / WPA2 / WPA3 (Enterprise).
- Select WPA3-802.1X as Key Management.
- Select CCMP (AES) as Encryption Method.
- Select RADIUS server (defined in step 802.1X (Enterprise) – External Radius Server Configuration).

802.1X (Enterprise) – External Radius Server Configuration

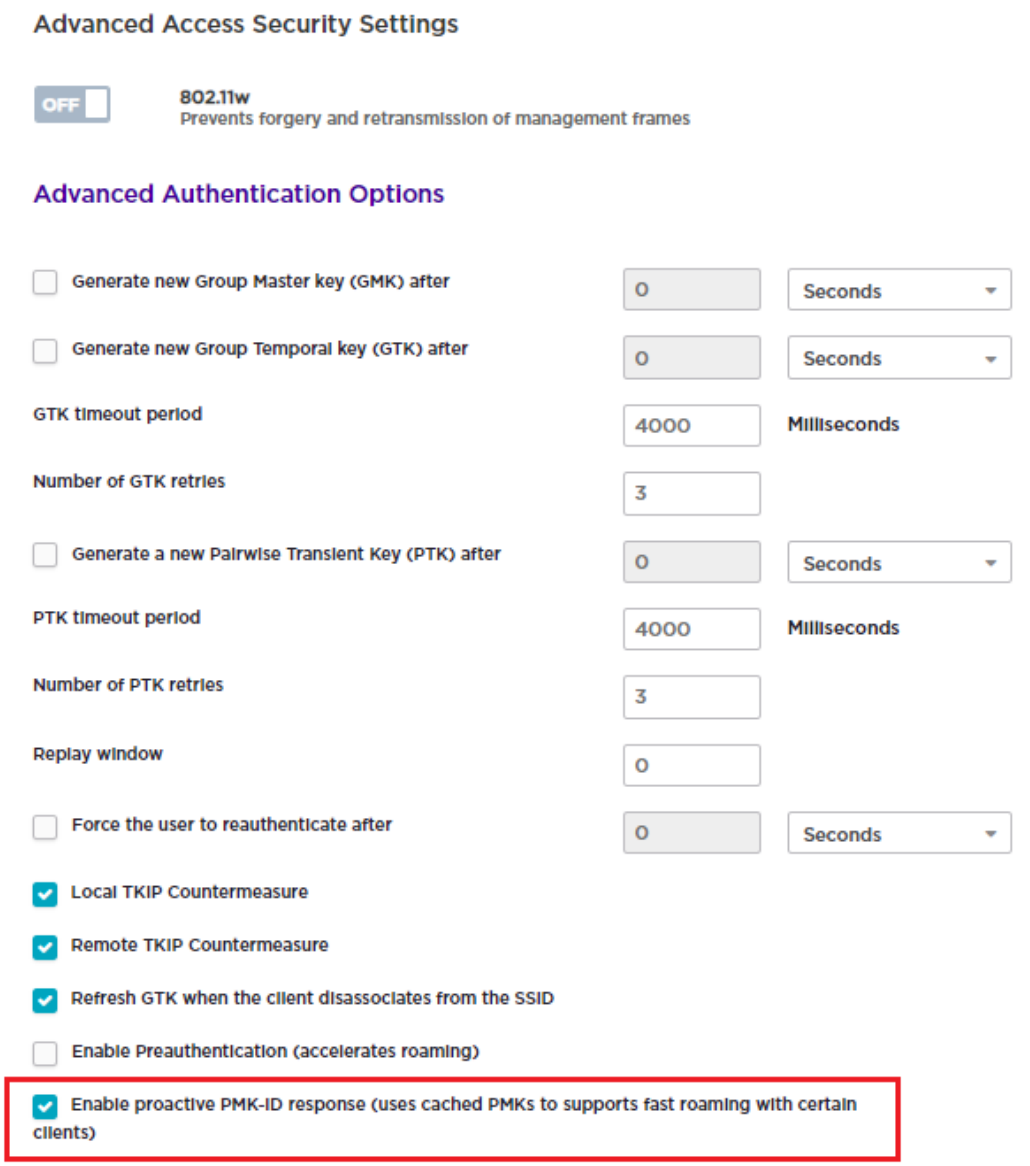


Overview of configured External Radius Servers.



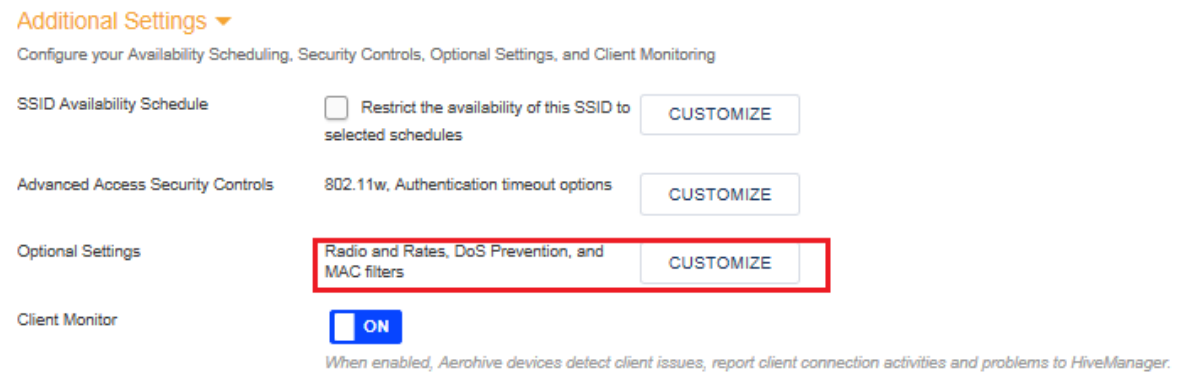
External Radius Server configuration

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



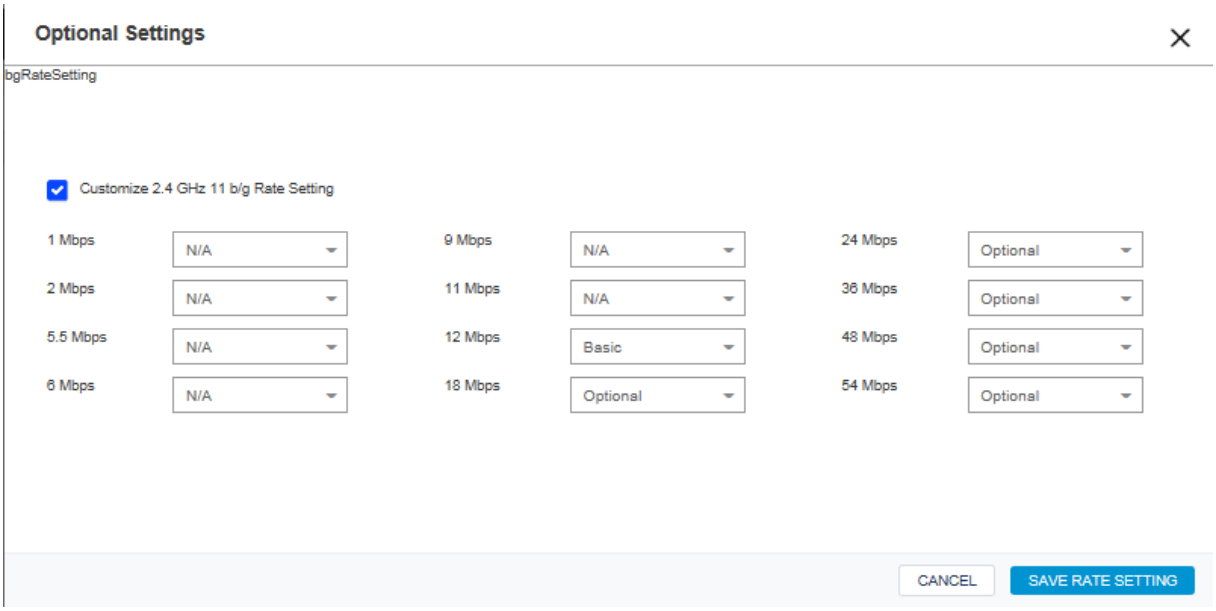
(Enterprise) - Additional settings - Advanced Access Security Controls

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



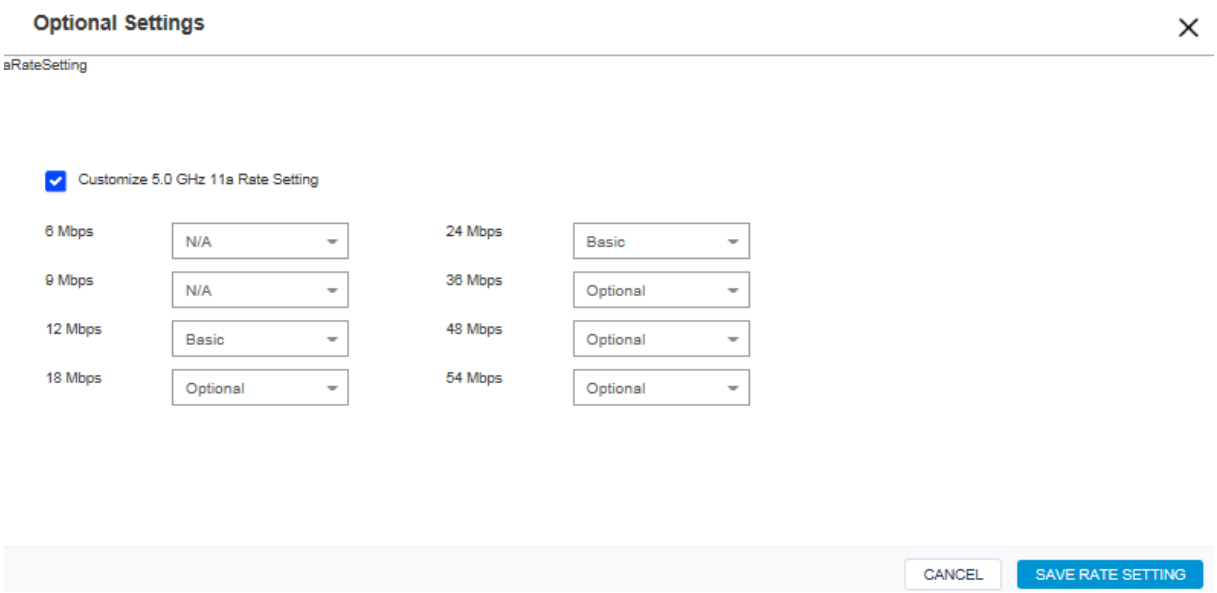
Data rate configuration. (Per SSID)

- Go to optional Settings



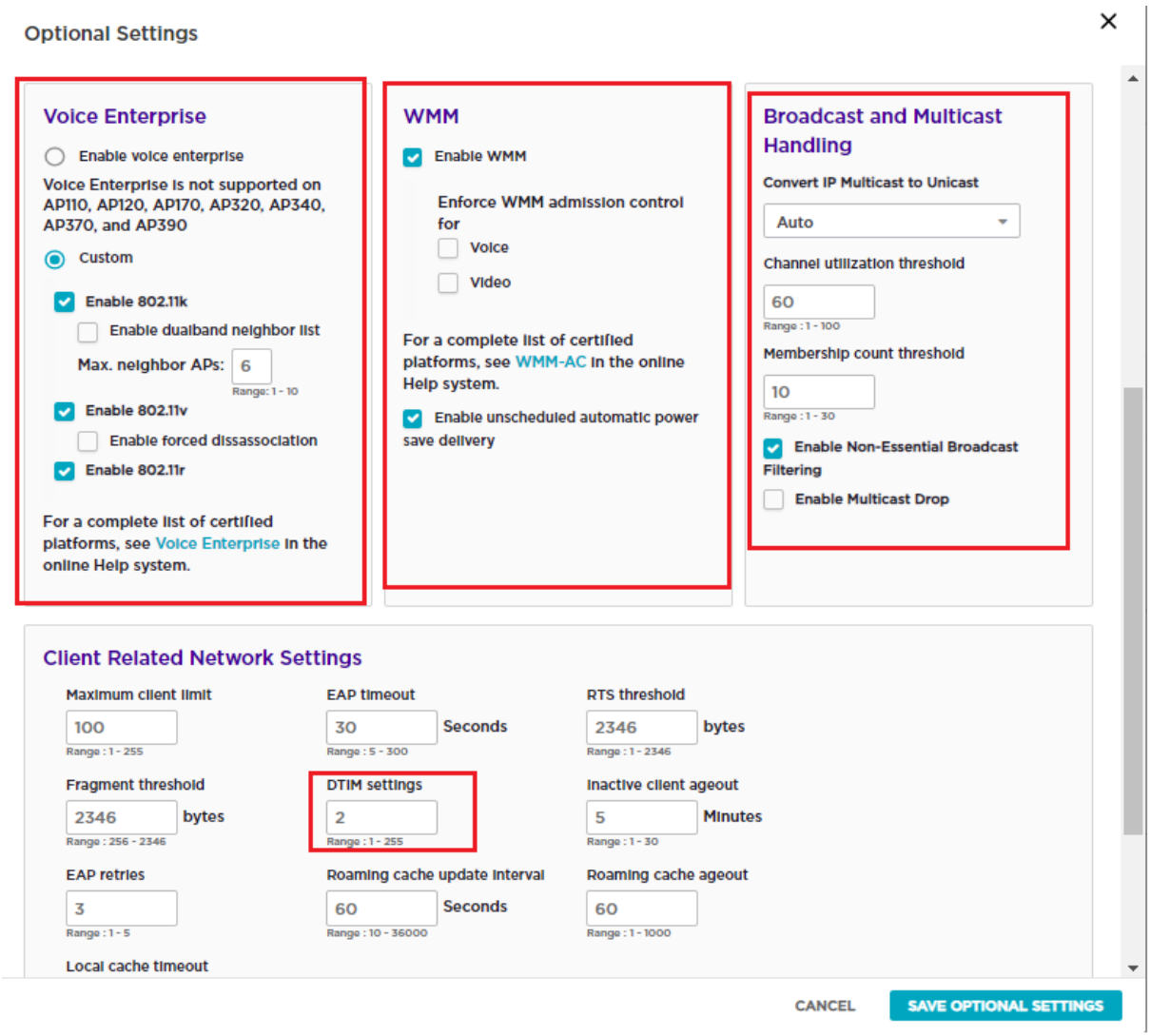
Data rate configuration.2.4GHz

- 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.



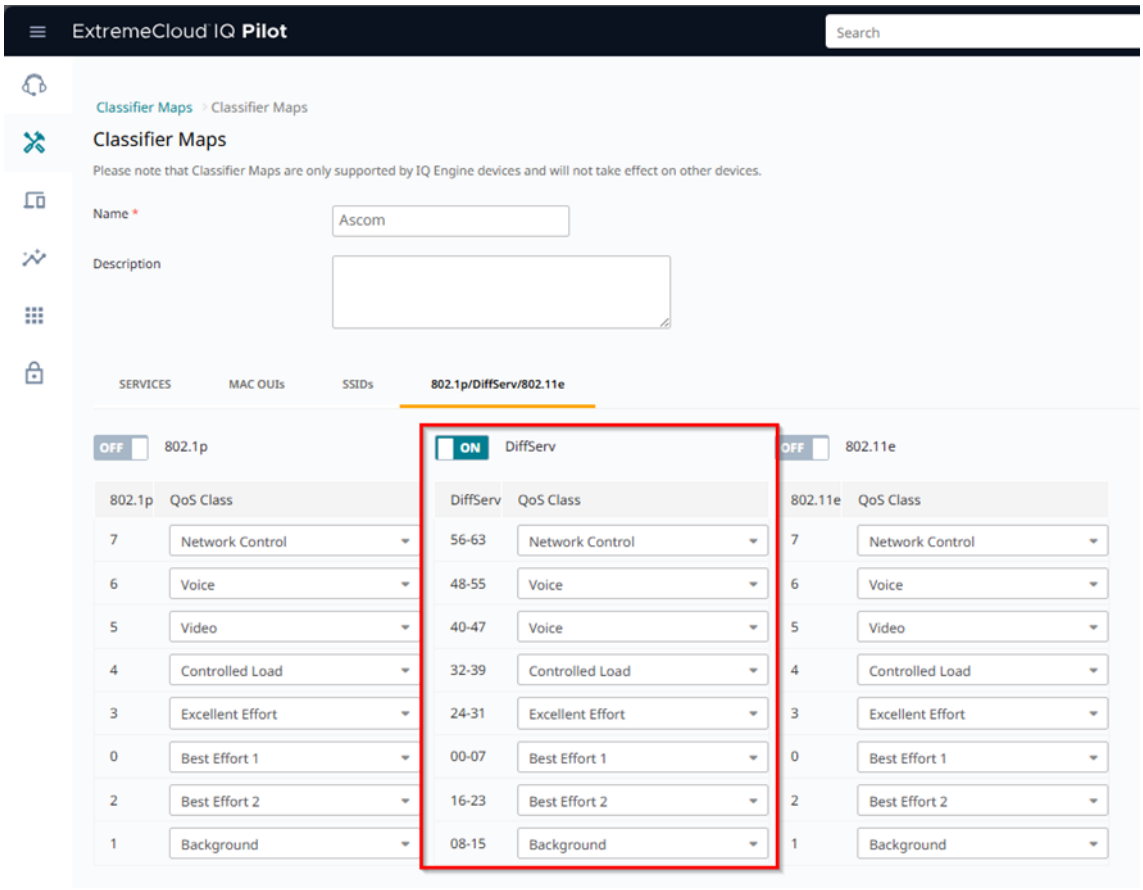
Optional SSID settings

- Enable 802.11k support.
- Enable 802.11v support. (802.11v is not really needed for i63, but still recommended if mixing with other Ascom products)
- Enable 802.11r support. (strongly recommended 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

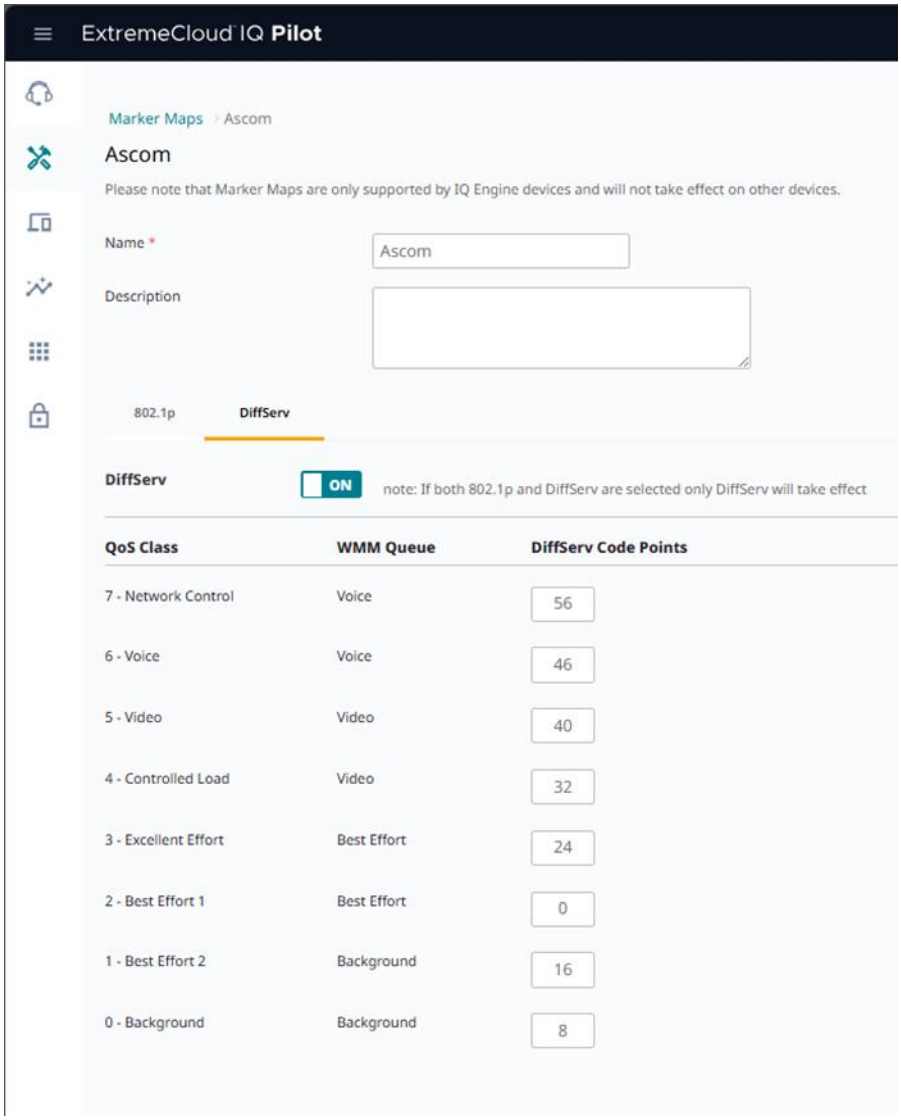
- Ascom recommends a DTIM period of at least 2 but no higher than 5.

Quality of Service (QoS)



Classifier Maps

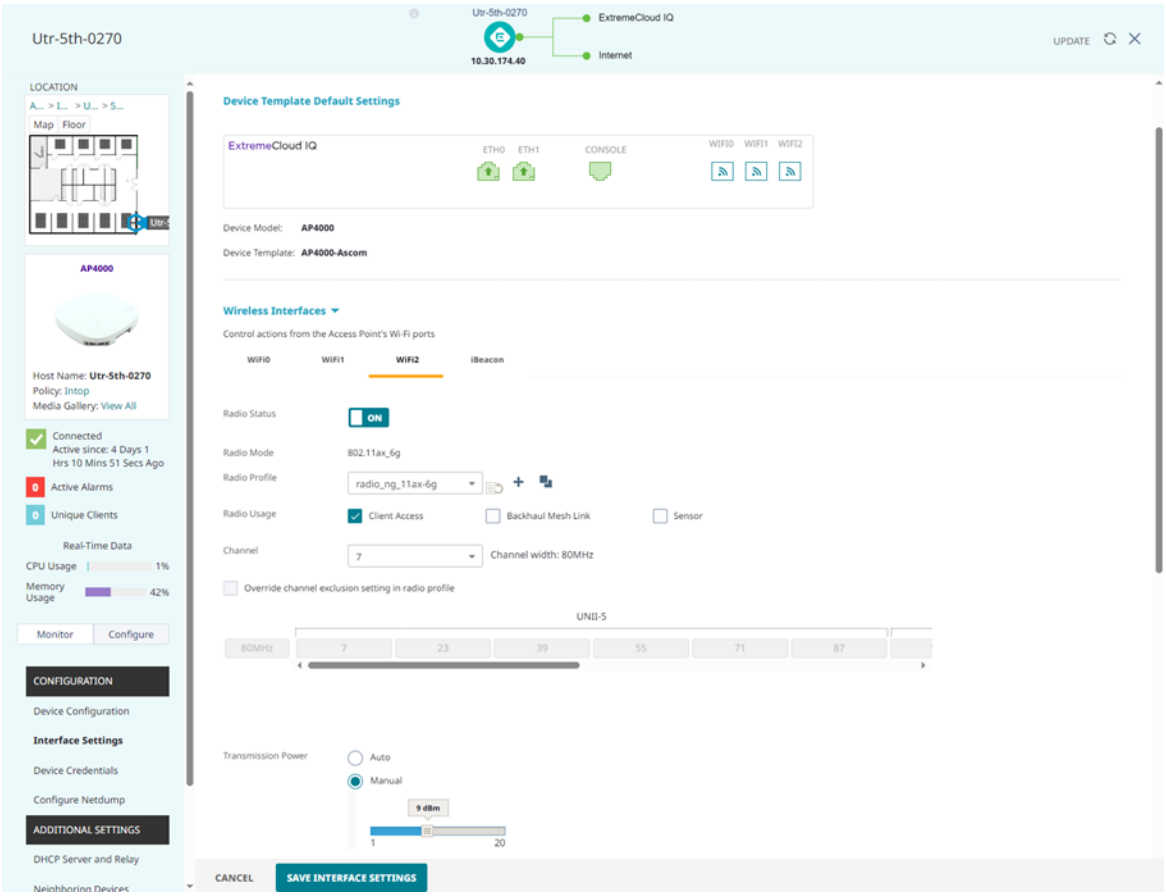
- Create classifier map according to the screenshot and enable DiffServ and 802.11e
- **Important. For DiffServ 40-47 select QoS Class: 6 – Voice.**



Marker Maps

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

Radio Configuration



Configuration of access points

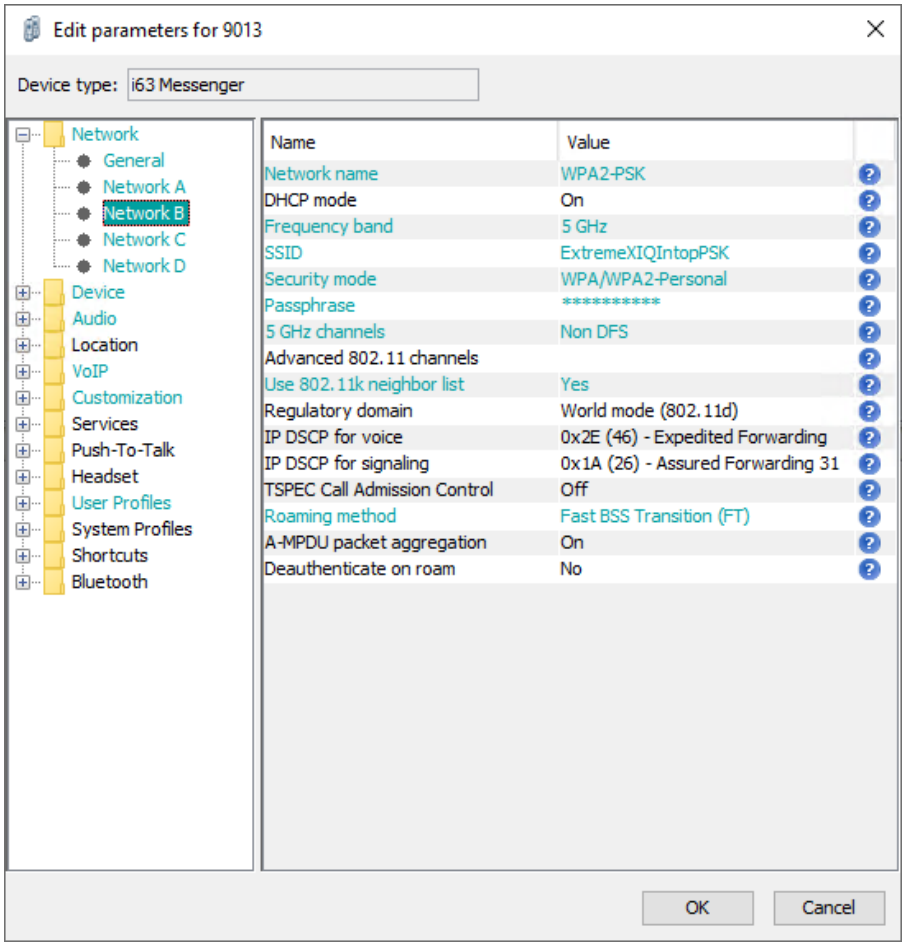
- Radio profiles used are the default (Default radio profiles **radio_ng_11ax-2g** for WiFi0, **radio_ng_11ax-5g for** WiFi1 and **radio_ng_11ax-6g** for WiFi2 interface).
- In the example channel and Transmission power has been set manually for each access point (for testing).

General guidelines when deploying Ascom 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 channels enabled can be allowed. Ascom does not recommend exceeding these limits unless 802.11k is in use.**
2. **Ascom support and can coexist in 40/80/160MHz channel bonding environments. The recommendation is, however, to avoid 80/160MHz channel bonding, as it severely reduces the number of available non-overlapping channels.**
3. **Make sure that all non-DFS channels 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 VoWI-FI deployments.**

   *) Dynamic Frequency Selection (radar detection)

WPA2-Personal (PSK)

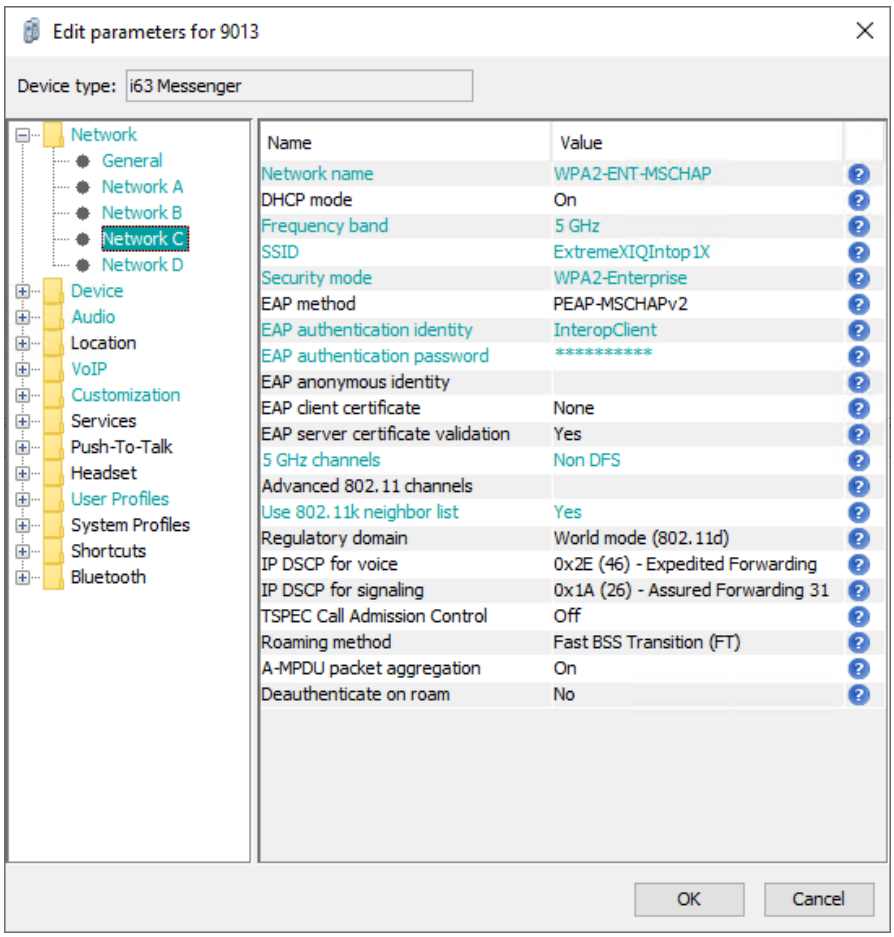


Network settings for WPA2-PSK

- Select frequency band according to system setup (here 5Ghz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA/WPA2-Personal.
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list
- Set Roaming method to Fast BSS Transition (FT).

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

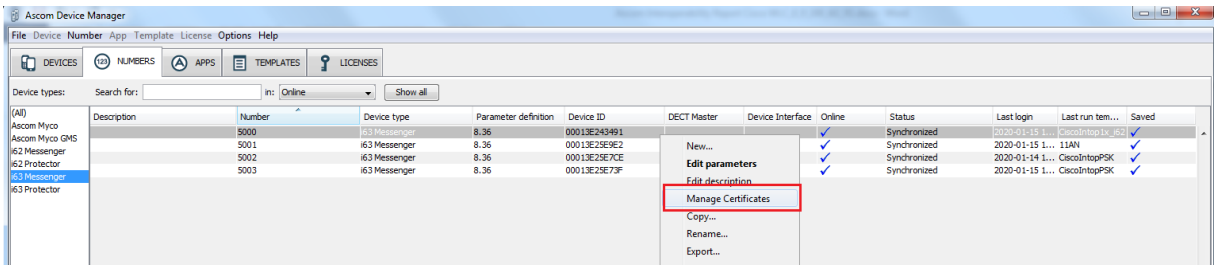
WPA2-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



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

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA2-Enterprise.
- Enter the EAP authentication identity and password.
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

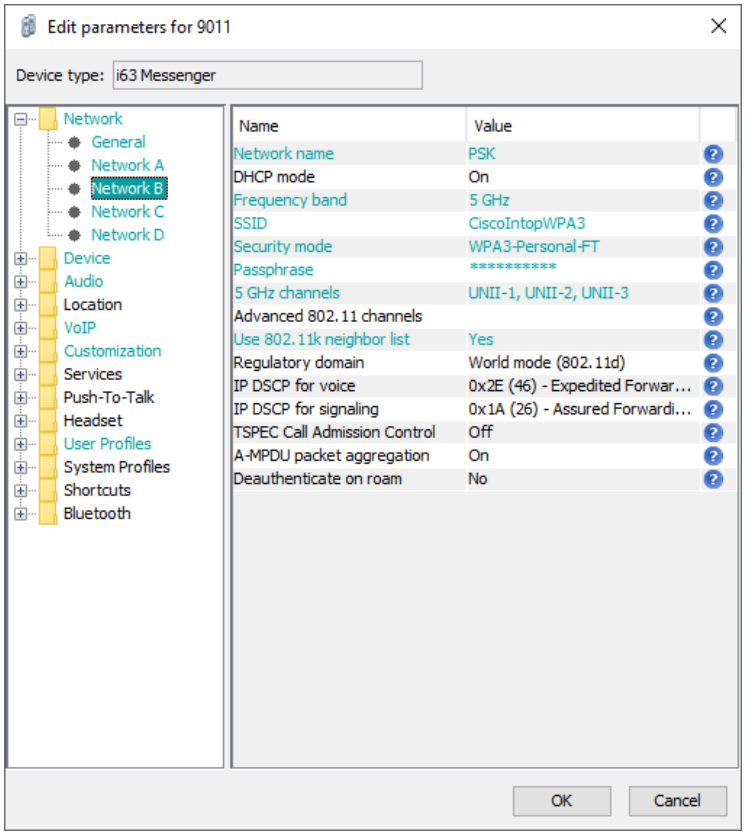
Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to “USA”.



802.1X Authentication requires a trusted certificate to be uploaded to the phone by “right clicking” - > Manage certificates.

Note that both Trusted Root and Application certificates are required when using EAP-TLS authentication.

WPA3-Personal (SAE)

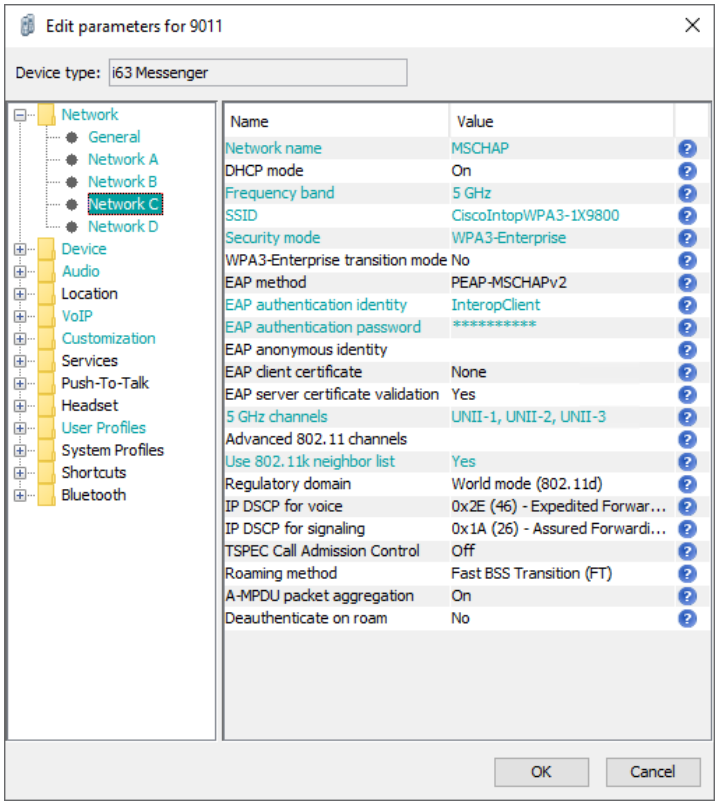


Network settings for WPA3-Personal

- Select frequency band according to system setup (here 5Ghz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA3-Personal-FT.
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

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

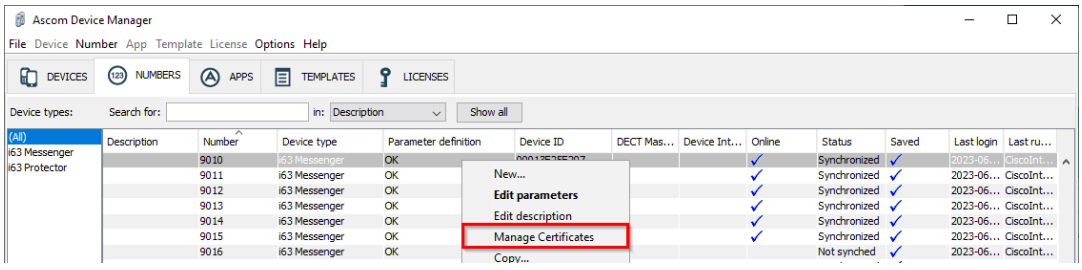
WPA3-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



Network settings for WPA3-Enterprise .1X authentication (PEAP-MSCHAPv2)

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA3-Enterprise.
- Enter the EAP authentication identity and password.
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

NOTE: The FCC no longer allows 802.11d to determine the regulatory domain. Accordingly, devices deployed in the United States must have the “Regulatory domain” set to “USA”.



802.1X Authentication requires a trusted certificate to be uploaded to the phone by “right clicking” - > Manage certificates.

Note that both Trusted Root and Application certificates are required when using EAP-TLS authentication.

Appendix B: Interoperability Verification Records

	2.4Ghz	5Ghz
Pass	23	25
Fail	0	0
Comments	4	2
Not verified	6	6
Total	33	33

Refer to the attached file for detailed verification results.

Document History

Rev	Date	Author	Description
D1	27-Aug-2025	NLRPA	Draft
D2		NLRPA	Minor corrections After internal review