INTEROPERABILITY REPORT

Ascom i63

Huawei

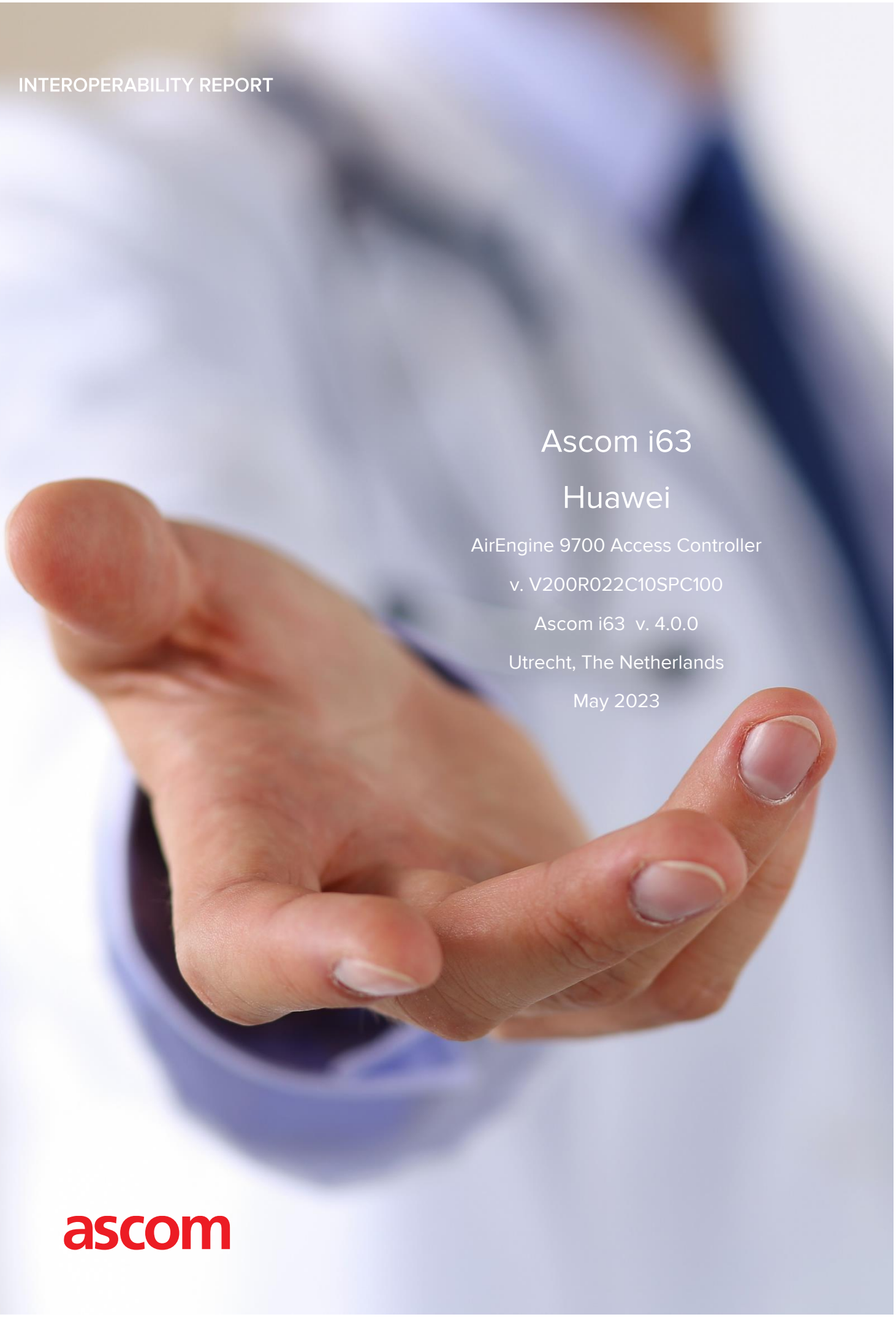
AirEngine 9700 Access Controller

v. V200R022C10SPC100

Ascom i63 v. 4.0.0

Utrecht, The Netherlands

May 2023



ascom

Contents

Introduction

This document describes a summary of the interoperability validation results of the Ascom and Huawei platform, furthermore it provides the necessary steps and guidelines to optimally configure the respective platforms. This report should be used in conjunction with configuration guides from both Huawei and Ascom.

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 Huawei

Founded in 1987, Huawei is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. We have 207,000 employees and operate in over 170 countries and regions, serving more than three billion people around the world. We are committed to bringing digital to every person, home and organization for a fully connected, intelligent world.

To learn more, visit Huawei at http://www.huawei.com. For real-time news updates follow Huawei on LinkedIn, Twitter and Facebook.

Site Information

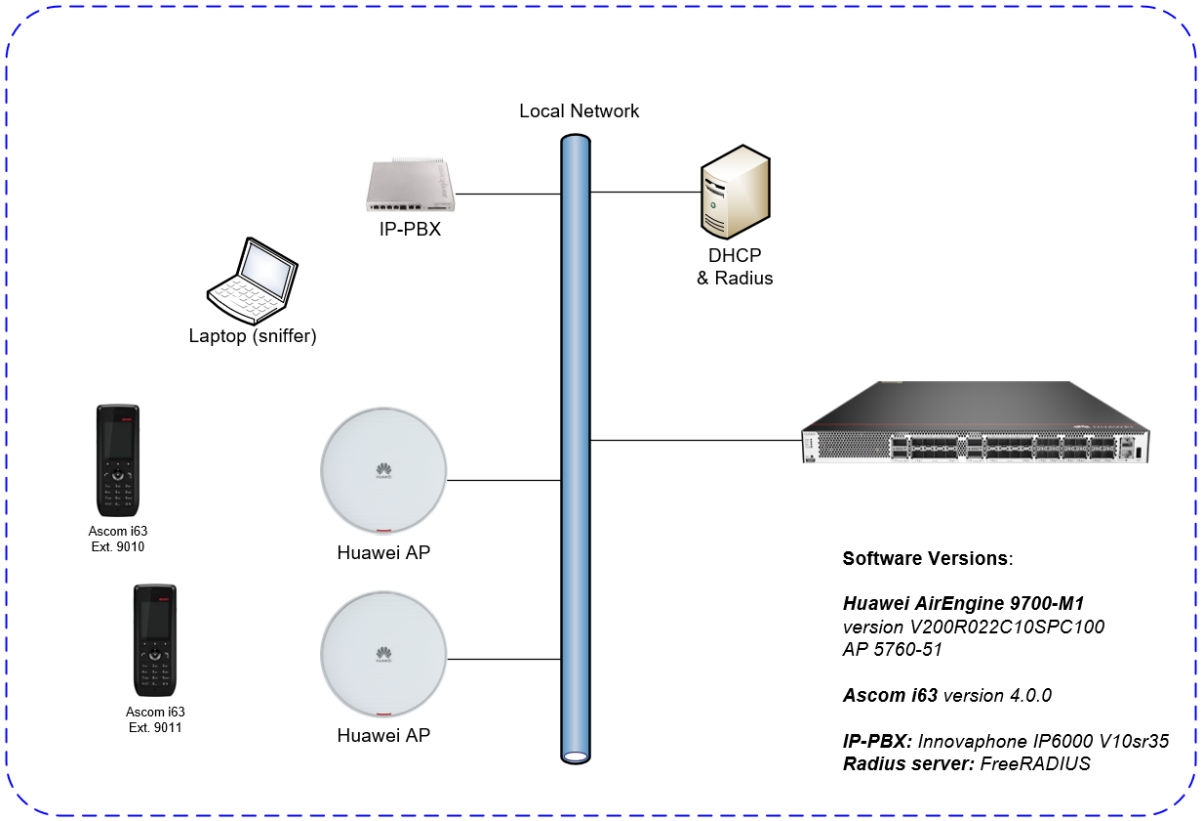
Test site

Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

Participants

Remco van den Pangaart, Ascom, The Netherlands

Test topology



Summary

General conclusions

This Ascom interoperability validation produced good results with regard to the tested areas of authentication, stability, roaming, QoS, and power save.
Roaming times were in general very good with all Authentication methods. Observed times were typically around 40-70ms. Using 11r/FT typically produced the best results and is therefore recommend.

Compatibility information

One Access point model from every product generation has been selected (AP 5760-51). By testing these access points, Ascom is considered to cover all access points listed below based on chipset compatibility.

Supported Partner Access Points with version V200R022C10SPC100:

AirEngine 5760-51
AirEngine 6760-X1
AirEngine 6760R-51
AirEngine 8760-X1-PRO
AirEngine 8760R-X1E
AirEngine 5760-22W
AirEngine 6760-X1E
AirEngine 6760R-51E
AirEngine 8760R-X1

Supported Partner Controller Platforms with version V200R022C10SPC100:

AirEngine 9700-M1 Access Controller
AC6508 Access Controller
AC6805 Access Controller
AC6800V Access Controller
iMaster NCE-Campus

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	N/T	Legacy PS, test case not relevant (U-APSD required)
802.11e U-APSD	OK	
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 46 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 40 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 46 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 44 ms
Channel usage controlled by 802.11k	OK	
Network features controlled by 802.11v	N/T	Not supported by Ascom i63

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

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.**

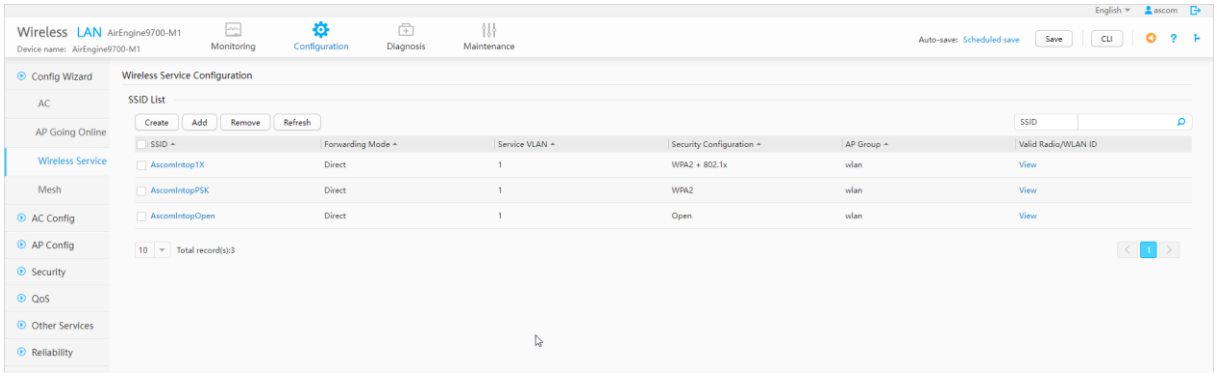
For detailed validation results, refer to Appendix B: Detailed Validation Records.

Appendix A: Validation Configurations

Huawei AirEngine 9700-M1 Access Controller, V200R022C00SPC100

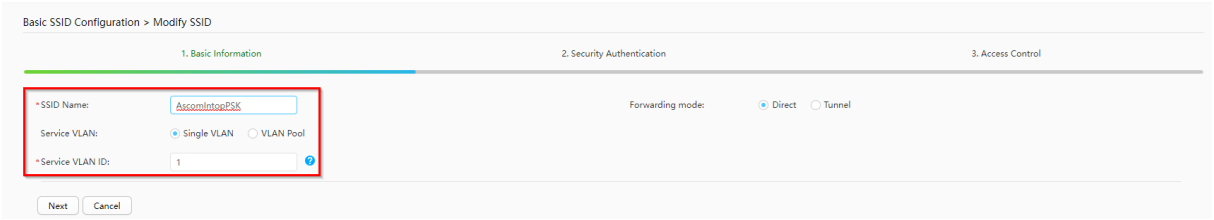
In the following chapter you will find screenshots and explanations of basic settings to get a Huawei AirEngine 9700-M1 Access Controller system to operate with an Ascom i63 handset. Please note that security settings were modified to meet requirements in individual test cases.

General settings (SSID, Authentication)

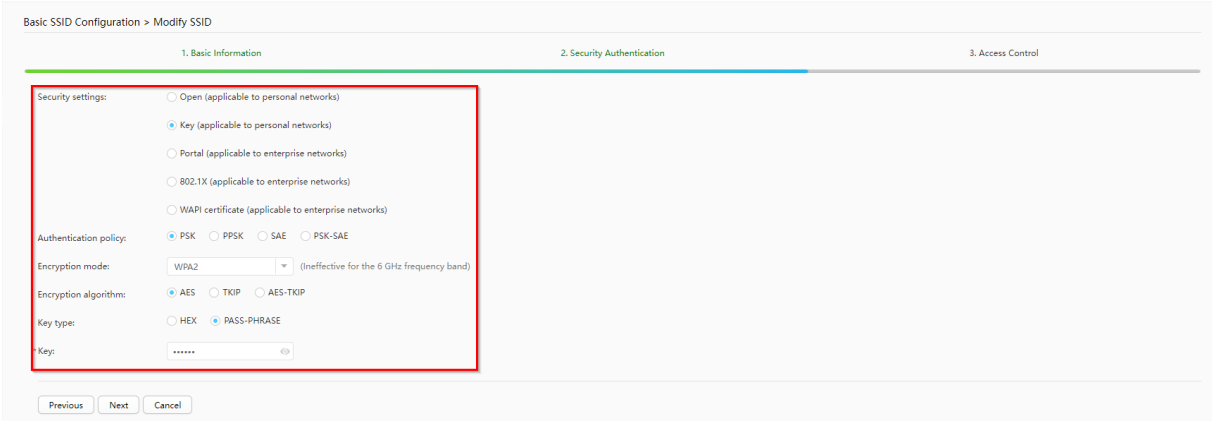


List of all configured SSIDs

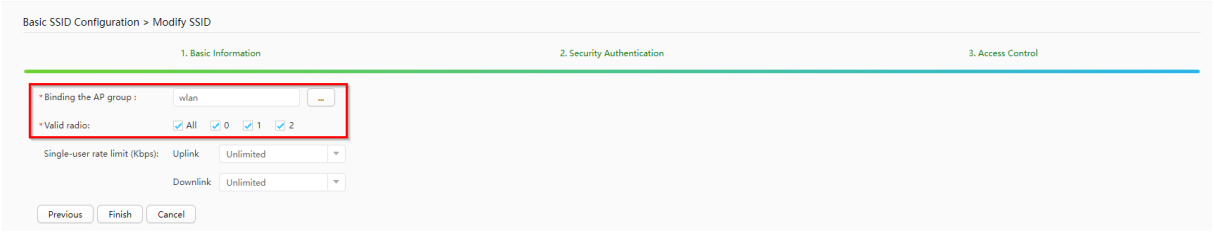
WPA2-PSK SSID Configuration (Personal)



- Define SSID Name.

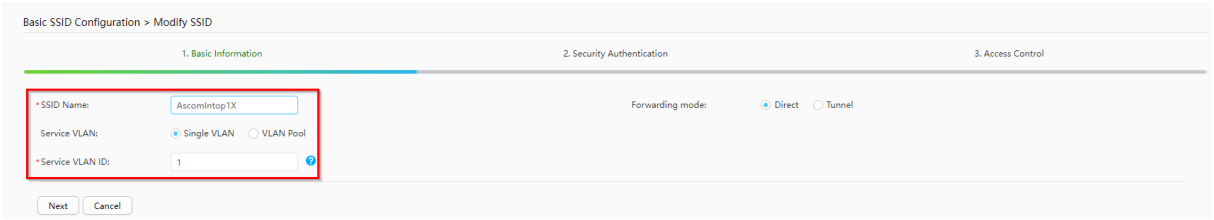


- Select “Key” for Security settings and “PSK” for Authentication policy.
- Select “WPA2” for Encryption mode.
- Key can be entered in HEX or in PASS-PHRASE (alphanumerical) format. Example shows a key entered in PASS-PHRASE format.

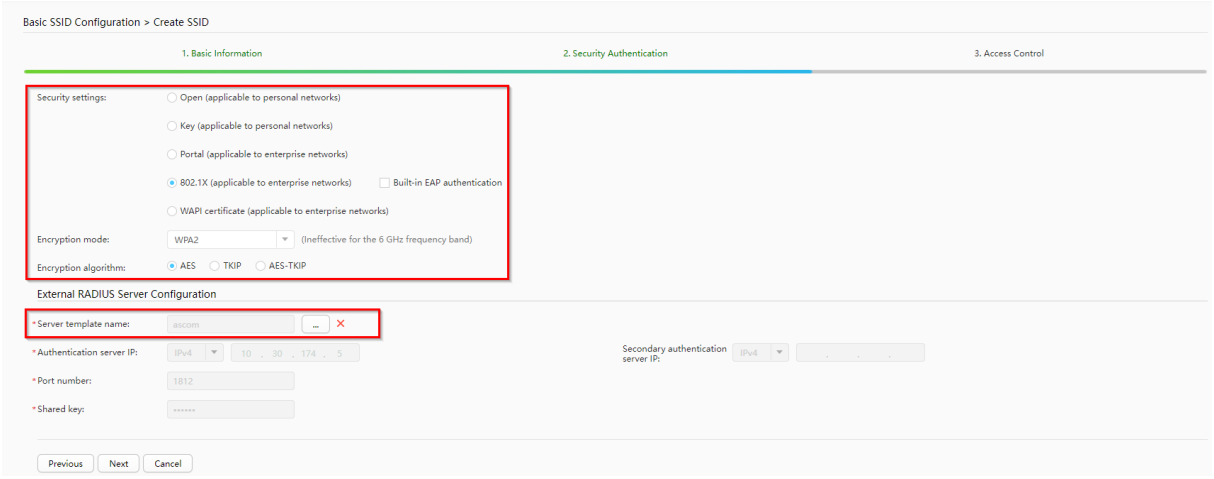


- Bind the created SSID to an AP group. Example shows binding to AP Group wlan.

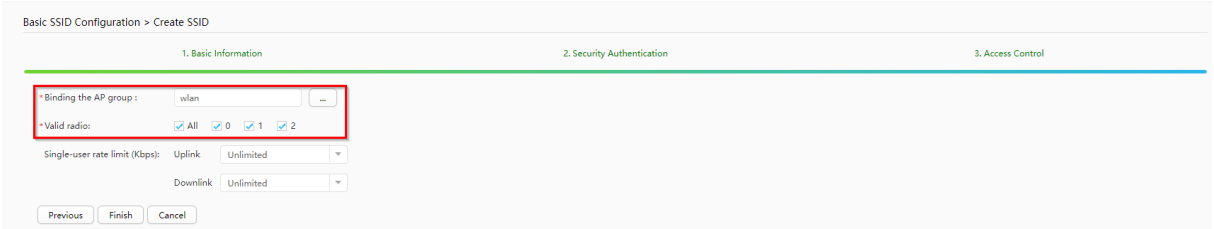
WPA2 802.1X SSID Configuration (Enterprise)



- Define SSID name.

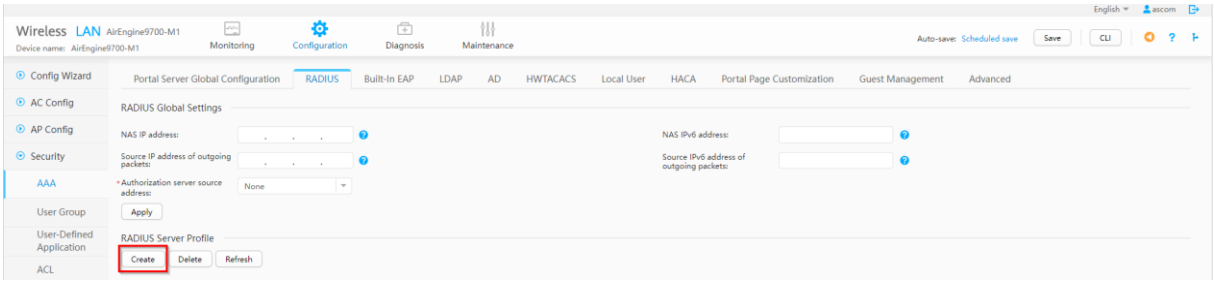


- Select 802.1X for Security settings.
- Select WPA2 Encryption mode and AES for Encryption algorithm.
- Select RADIUS server template (defined on the next page).

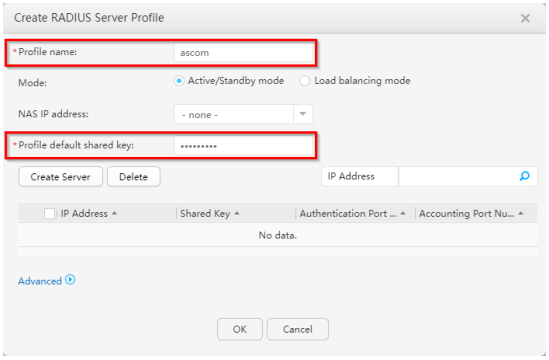


- Bind the created SSID to an AP group. Example shows binding to AP Group wlan.

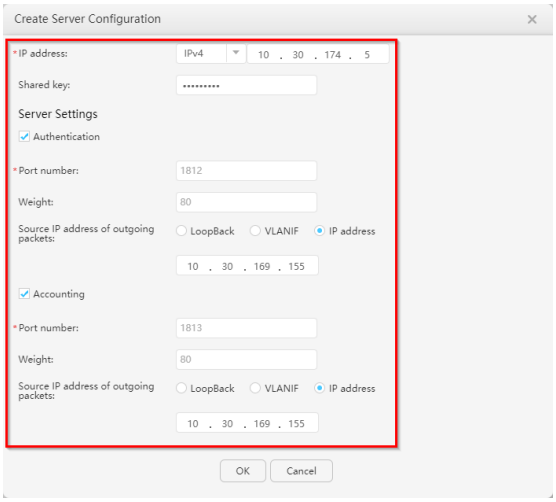
WPA2 802.1X (Enterprise) – RADIUS Server profile configuration



Create a new RADIUS Server Profile.

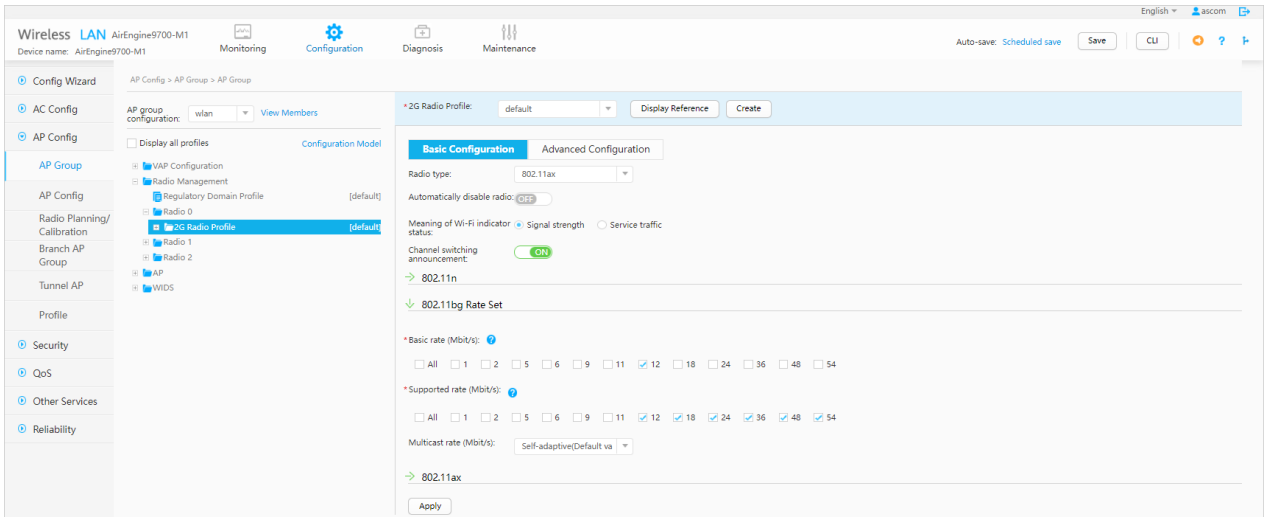


- Define a name for this RADIUS profile.
- Type in the “secret” that corresponds to the secret configured in the Radius server and click Create Server.

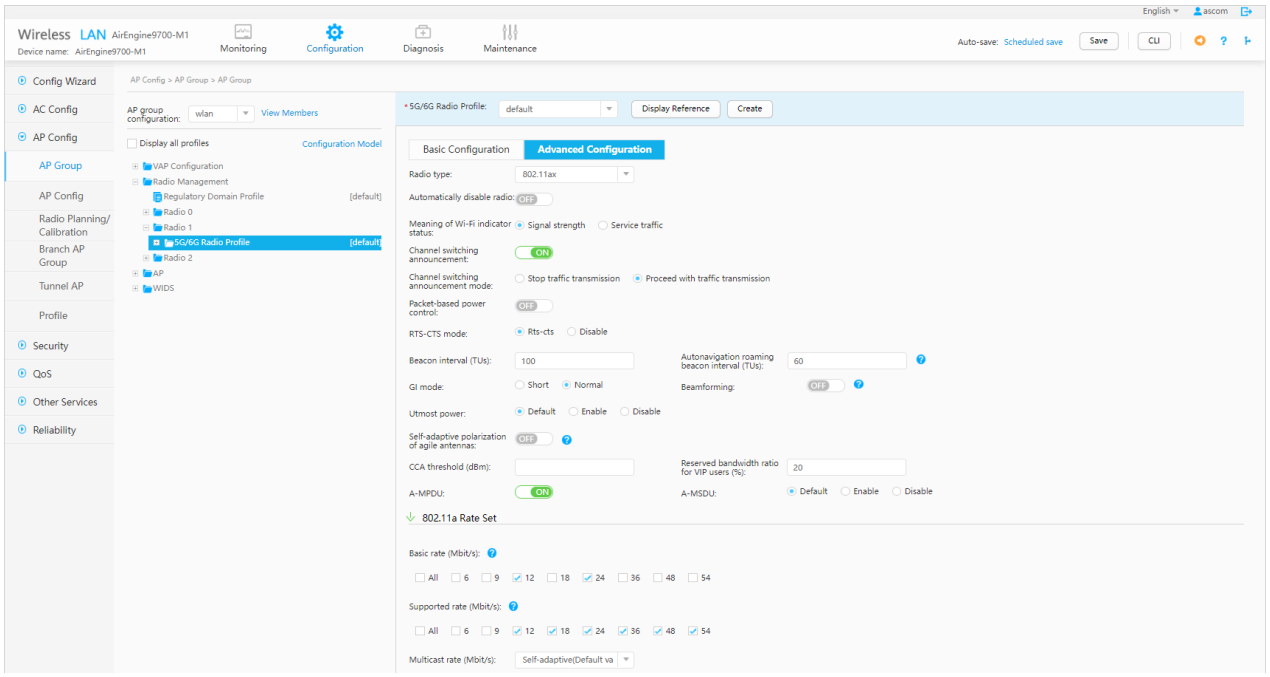


- Configure the IP Address to the Radius server.
- Select IP address for Source IP address of outgoing packets and enter IP address of the controller.

General settings (data rates, QoS, Radio)

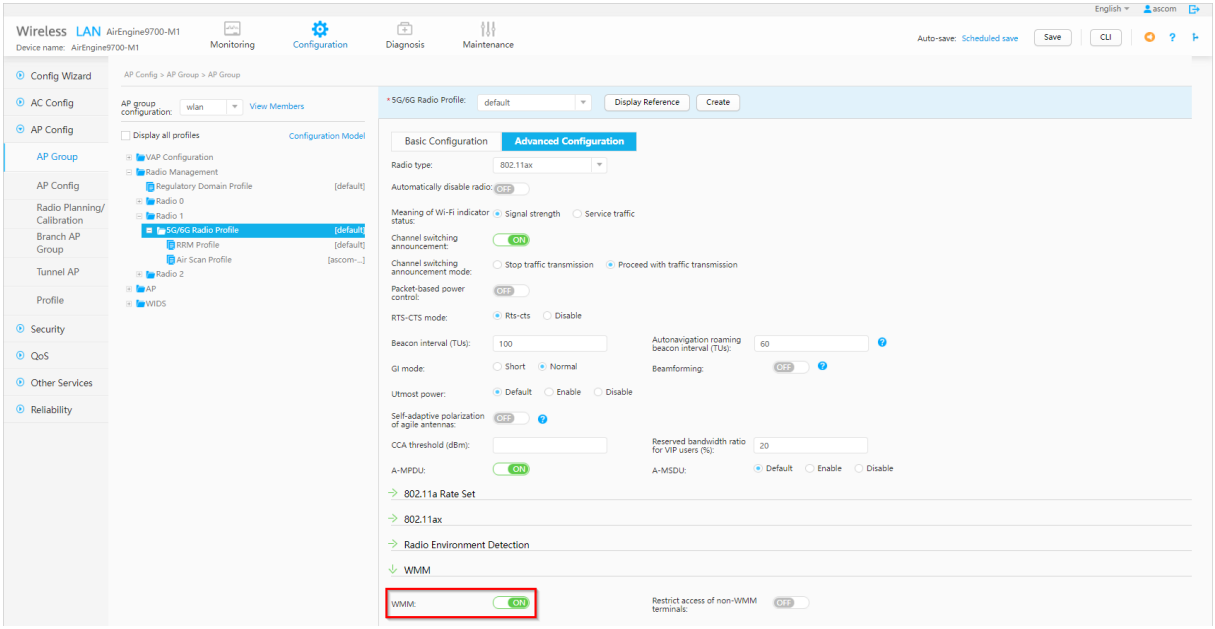


Data rate configuration 2.4GHz.

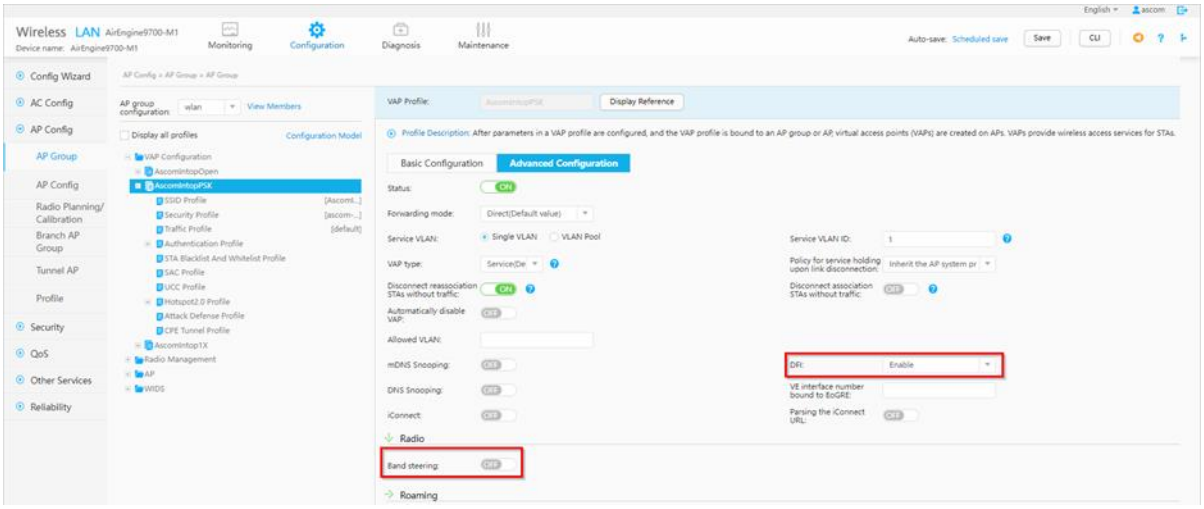


Data rate configuration 5GHz.

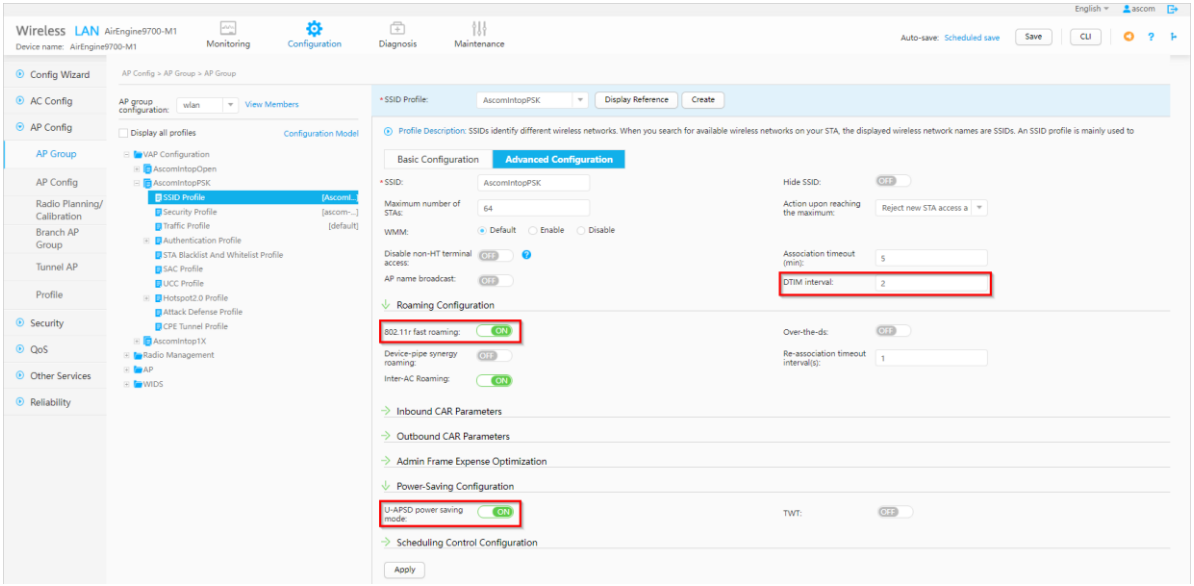
NOTE: The default data rate set will work just fine, however Ascom recommends disabling the lowest data rates and having 12Mbps is set as lowest data rate.



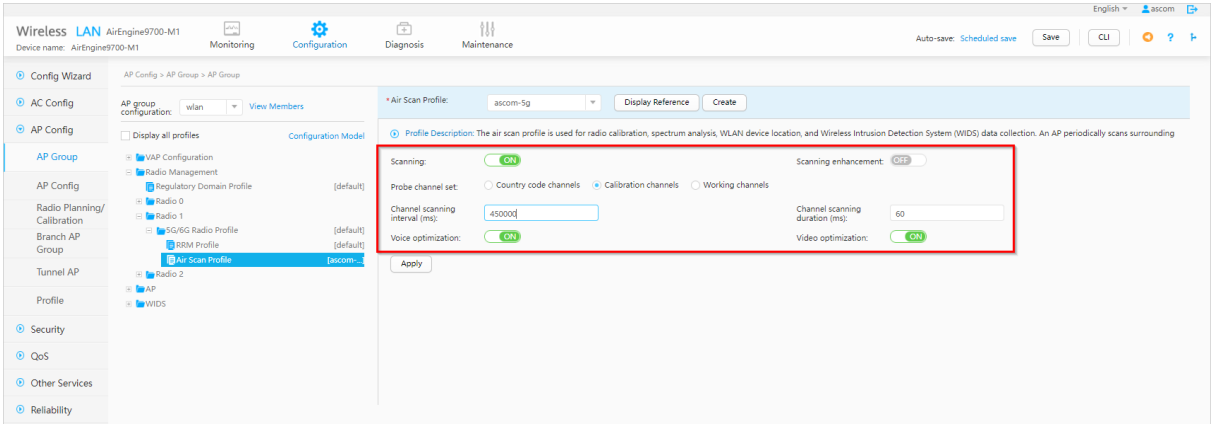
Ensure that WMM is switched on.



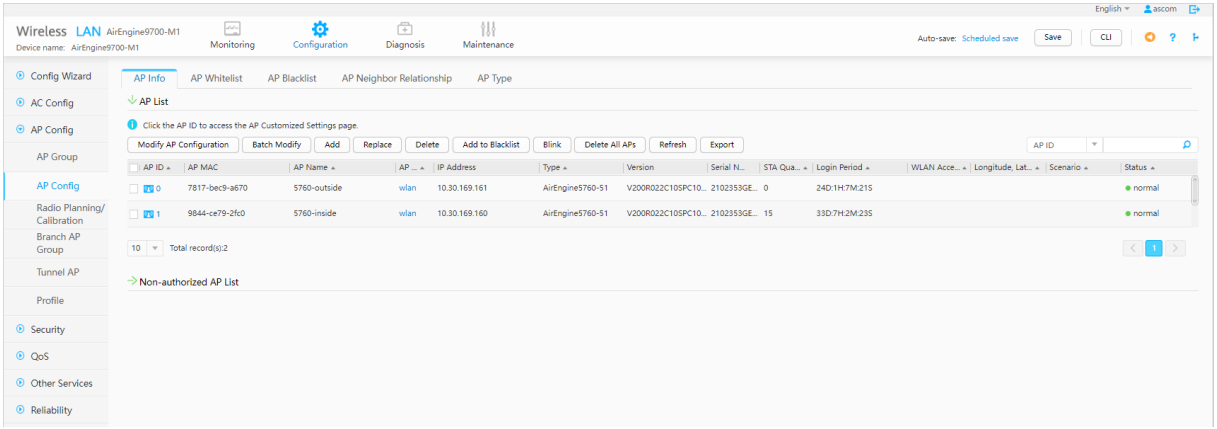
- Ensure Dynamic Flow Inspection (DFI) is set to Enable to match the default values in the i63.
- Disable Band steering.



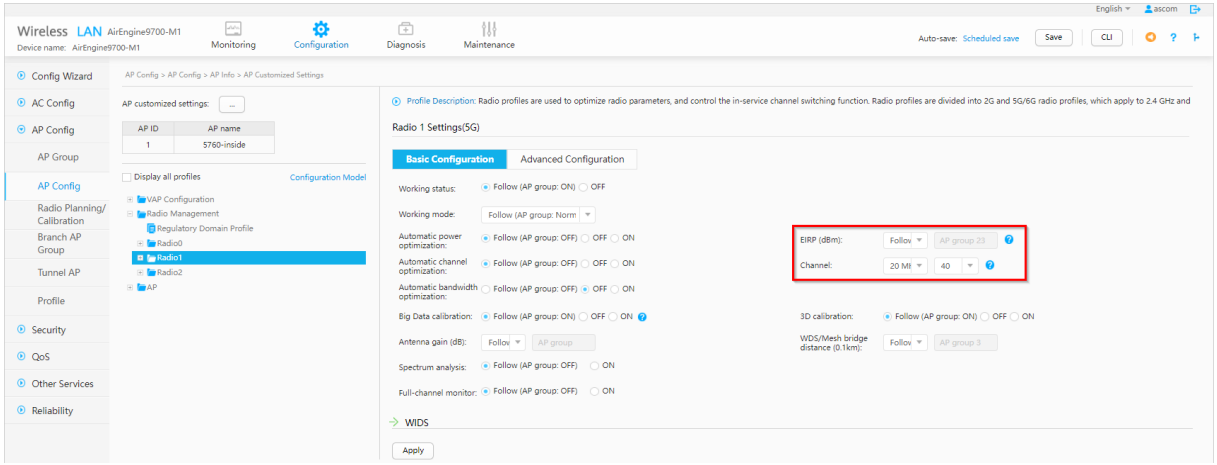
- Ascom recommends a DTIM period of at least 2 but not higher than 5.
- It is strongly recommended to use 802.11r Fast Roaming for enhanced roaming performance.
- Enable U-APSD.



To enable 802.11K (neighbor reports) it is necessary to enable Scanning in Air Scan Profile (this is a per radio setting).



Access point overview.



Specific radio configuration.

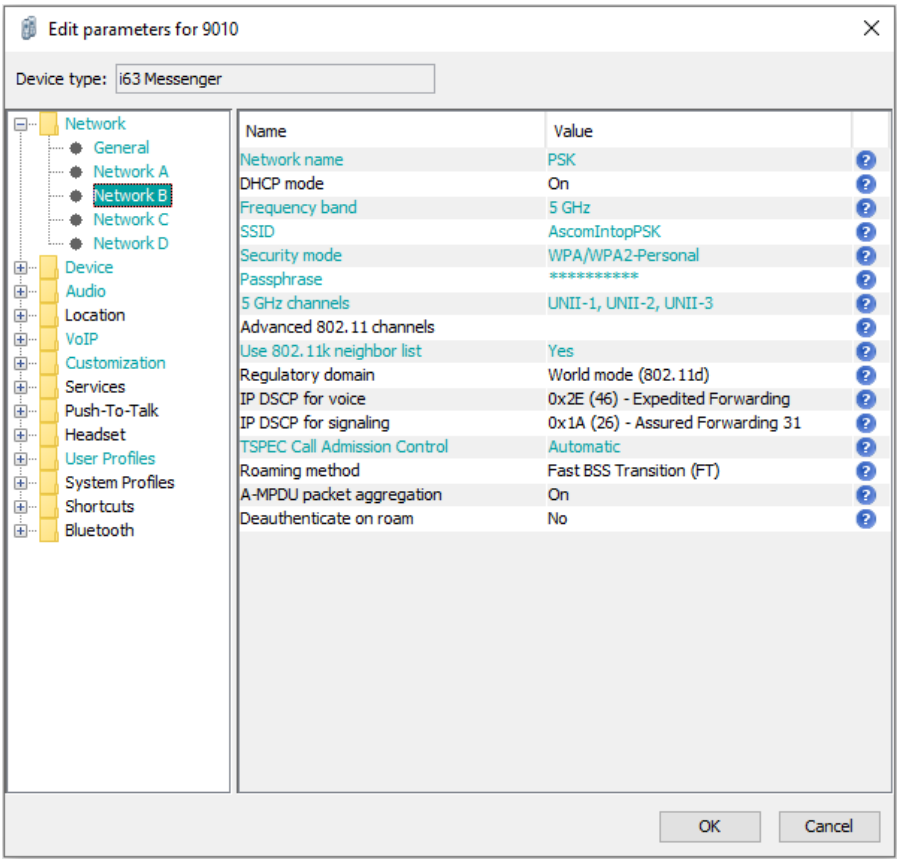
Note that Tx power level and channel was manually set for test purposes. A typical setup will rely on the Global setting for channel and power configuration.

Ascom recommends only using channel 1, 6 and 11 for 802.11b/g/n. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines below.

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 these limits unless 802.11k is in use.**
2. **Ascom does support and can coexist in 80MHz channel bonding environments. The recommendation 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 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.**

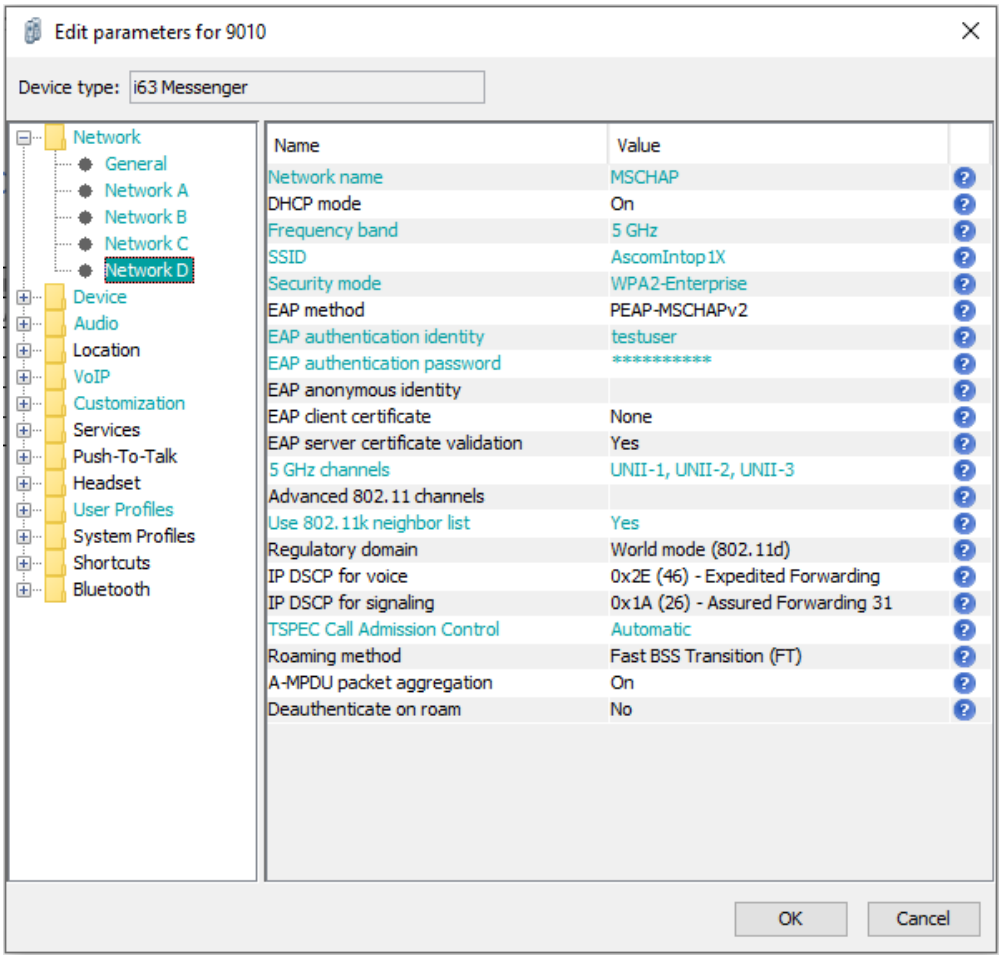
Ascom i63 Network settings



Network settings for WPA2 – PSK.

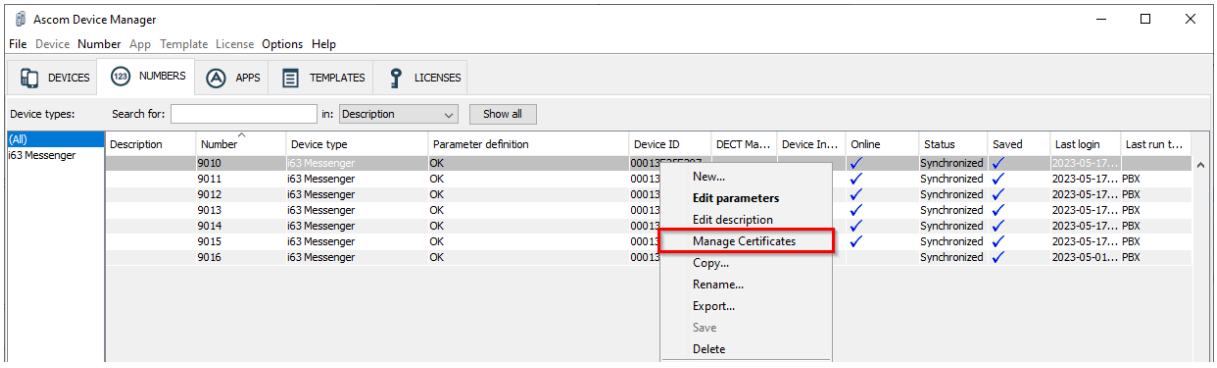
- Make sure that the enabled channels in the i63 handset match the channel plan used in the system.
- 802.11k neighbor list will improve roaming performance especially when the number of channels in the system exceeds the 9 non-DFS channels.

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



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

- Make sure that the enabled channels in the i63 handset match the channel plan used in the system.
- 802.11k neighbor list will improve roaming performance especially when the number of channels in the system exceeds the 9 non-DFS channels.



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

Note that for TLS both the root and client certificate need to be uploaded to the phone.

Appendix B: Detailed Validation Records

Pass	20
Fail	0
Comments	7
Not verified	3
Total	30

Contact your Ascom supplier for additional information about interoperability and test results.

Document History

Rev	Date	Author	Description
D1	2023-05-10	NLRPa	Draft version for internal review.
P1	2023-06-07	NLRPa	Minor changes after peer review.