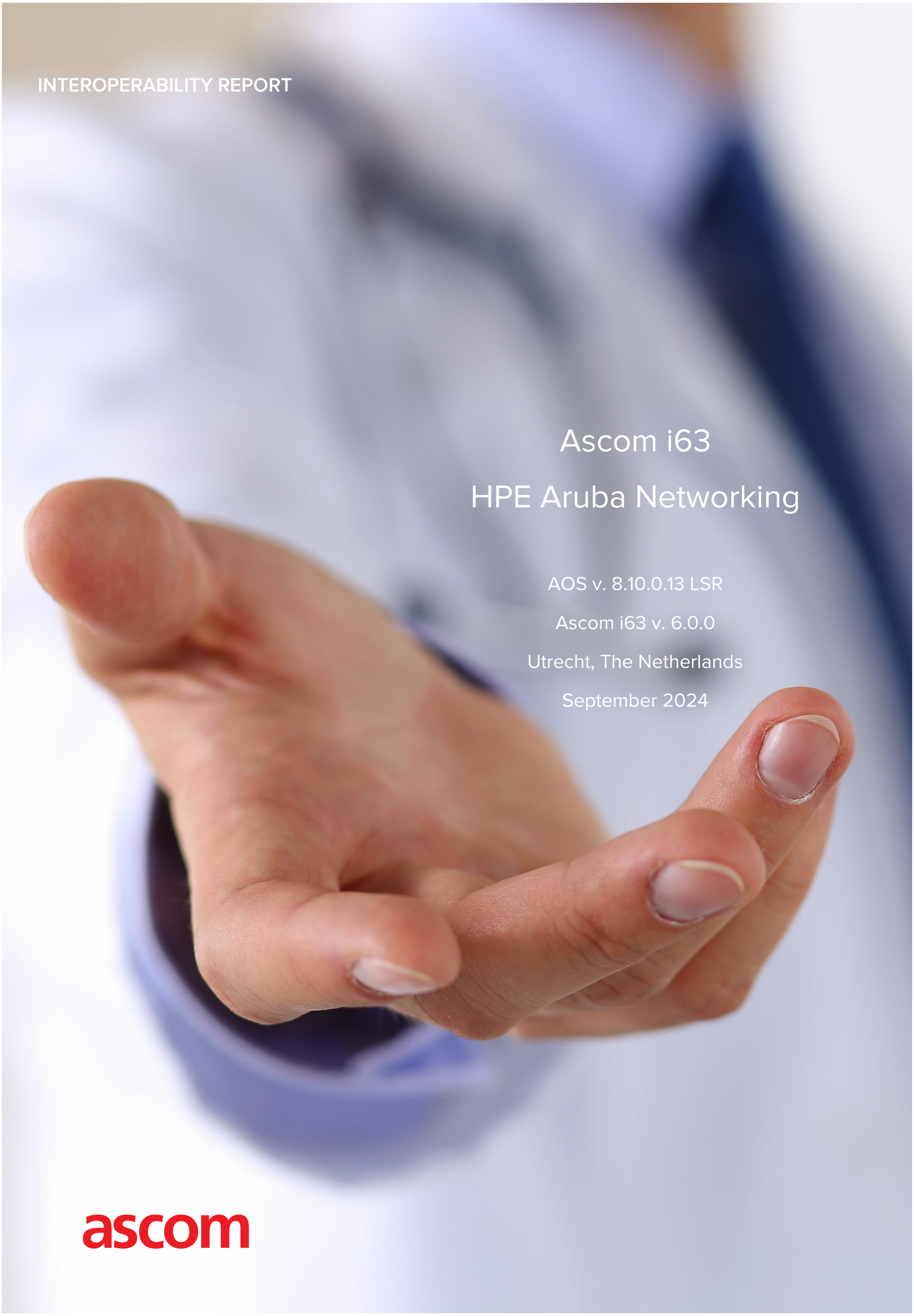


INTEROPERABILITY REPORT

Ascom i63

HPE Aruba Networking

AOS v. 8.10.0.13 LSR

Ascom i63 v. 6.0.0

Utrecht, The Netherlands

September 2024

Contents

Introduction

This document summarizes interoperability test results relating to the validation of Ascom's and the Partner's respective platforms. It also describes recommended steps and guidelines to configure these platforms and provides a point of contact for inquiries. The report should be used in conjunction with configuration guides from Ascom and the Partner.

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 HPE Aruba Networking

HPE Aruba Networking is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

To learn more, visit http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

Site Information

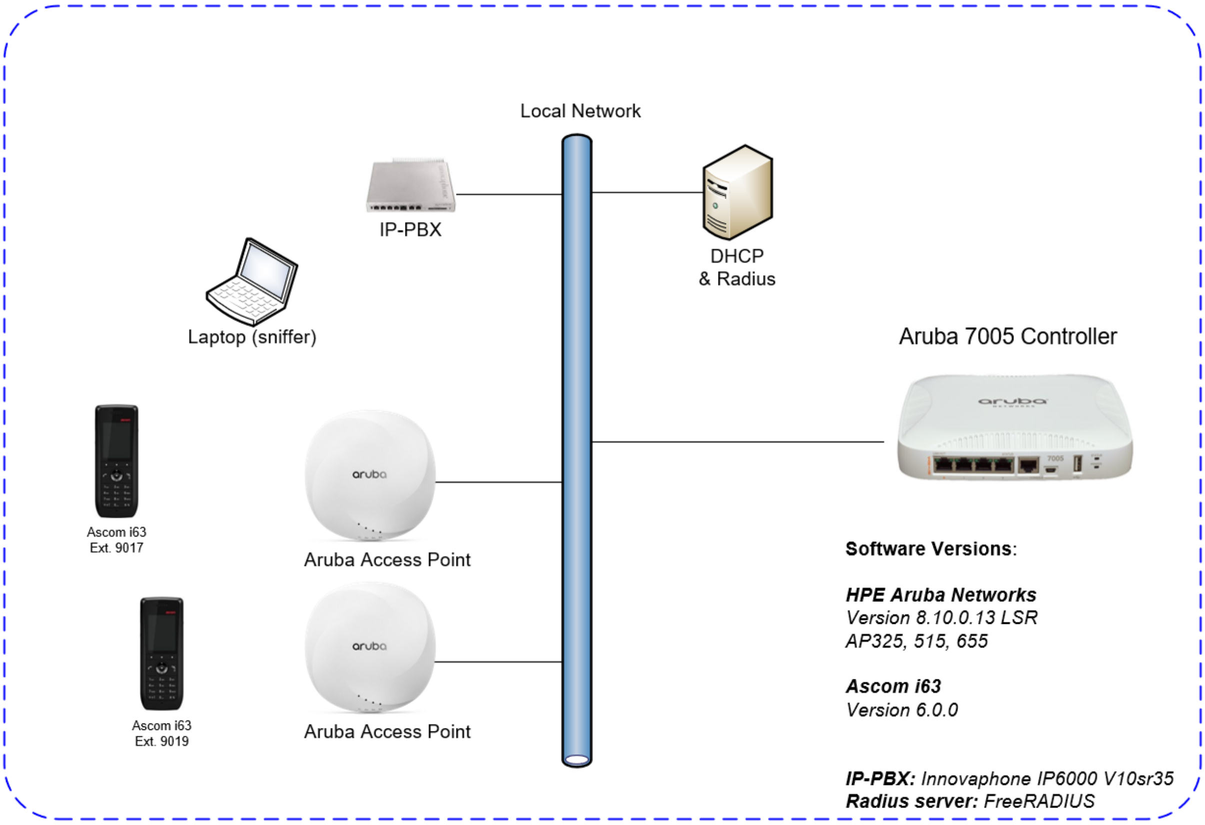
Test site

Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

Participants

Remco van den Pangaart, Ascom, The Netherlands

Test topology



Software Versions:

HPE Aruba Networks
Version 8.10.0.13 LSR
AP325, 515, 655

Ascom i63
Version 6.0.0

IP-PBX: *Innovaphone IP6000 V10sr35*
Radius server: *FreeRADIUS*

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 except for WPA3-SAE. Observed roaming times were typically around 25-50ms.

Using 802.11r/Fast Transition (FT) roaming is best common practice for VoWi-Fi deployments and therefore recommended and for WPA3 mandatory.

Compatibility information

One Access point model from every product generation has been selected AP-325, 515, and 655). By testing these access points, Ascom is considered to cover all access points listed below based on chipset compatibility.

Supported Partner Access Points with AOS version 8.10.0.13 LSR:

AP303, 304, 305, 314, 315, 324, 325, 334, 335, 344, 345

AP504, 505, 514, 515, 534, 535, 554, 555

AP635, 655

Supported Partner Controller Platforms with AOS version 8.10.0.13 LSR:

7000 Series Mobility Controllers

7200 Series Mobility Controllers

9000 Series Mobility Controllers

9200 Series Mobility Controllers

MC-VA-xxx Virtual Mobility Controllers

Interoperability Validation 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	N/T	Legacy PS, test case not relevant (UAPSD required)
802.11e U-APSD	OK	
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 33 ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 25 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 39 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 28 ms
Roaming, WPA3- SAE authentication, AES encryption	NOK	Typical roaming time 174 ms Strongly recommended to use 802.11r/FT
Roaming, WPA3-SAE authentication, AES encryption + FT	OK	Typical roaming time 31 ms
Roaming, WPA3-Enterprise + FT	OK	Typical roaming time 27 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/ax. Refer to Appendix B for detailed test results.

Known limitations.

Description and Consequence	Workaround	Ticket(s) raised
For the 802.11d “Country Information” element to be broadcasted on non DFS channels it is necessary to have 802.11k enabled. This is important for regions utilizing “world mode” regulatory domain.	Refer to configuration settings in this document.	-
The default 11k profile enables “Quiet IE” to be broadcasted. This causes the legacy Ascom device to function poorly with frequent disconnects.	If legacy Ascom devices, i62 and Myco 1 & 2 are used in the same WLAN system it is **mandatory** to disable “Advertise Quiet IE”. Refer to configuration settings in this document.	

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

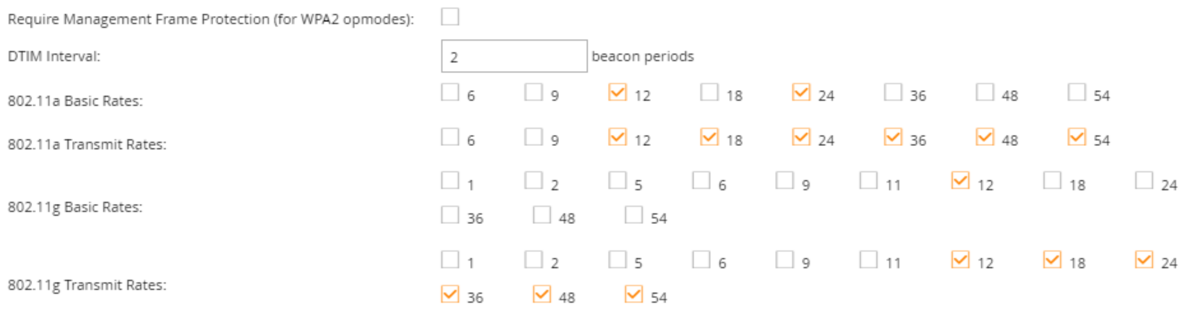
For detailed validation results, refer to Appendix B: Detailed Validation Records.

Appendix A: Validation Configurations

Aruba 7005 Mobility Controller, AOS 8.10.0.13 LSR

In the following chapter you will find screenshots and explanations of basic settings to get an HPE Aruba Networks 7005 Mobility Controller-based system to operate with an Ascom i63 handset. Please note that security settings were modified according to requirements in individual test cases.

General settings (Radio, WMM and QoS)



Require Management Frame Protection (for WPA2 opmodes): □

DTIM Interval: 2 beacon periods

802.11a Basic Rates: □ 6 □ 9 ☑ 12 □ 18 ☑ 24 □ 36 □ 48 □ 54

802.11a Transmit Rates: □ 6 □ 9 ☑ 12 ☑ 18 ☑ 24 ☑ 36 ☑ 48 ☑ 54

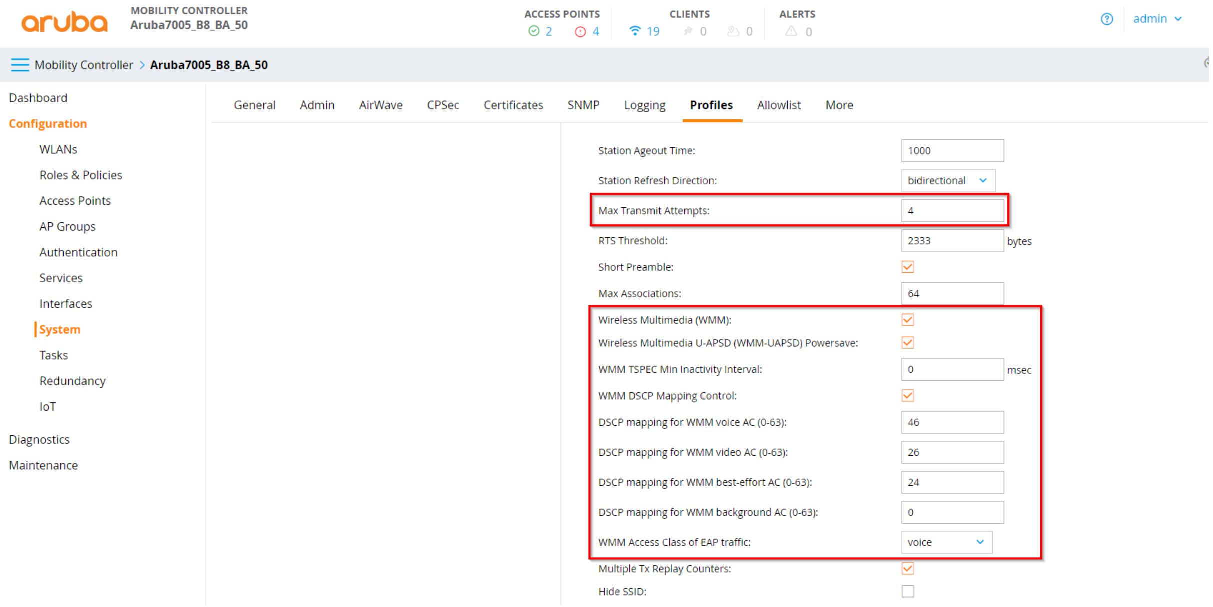
802.11g Basic Rates: □ 1 □ 2 □ 5 □ 6 □ 9 □ 11 ☑ 12 □ 18 □ 24 □ 36 □ 48 □ 54

802.11g Transmit Rates: □ 1 □ 2 □ 5 □ 6 □ 9 □ 11 ☑ 12 ☑ 18 ☑ 24 ☑ 36 ☑ 48 ☑ 54

Ascom recommends disabling the lower data rates and recommends that 12Mbps is set as lowest basic rate.

Ascom recommends a DTIM period of at least 2 but not higher than 5. A higher value will offer slightly better standby times.

Note: Not all Aruba Access point models support a DTIM period higher than 1.



Station Ageout Time: 1000

Station Refresh Direction: bidirectional

Max Transmit Attempts: 4

RTS Threshold: 2333 bytes

Short Preamble: ☑

Max Associations: 64

Wireless Multimedia (WMM): ☑

Wireless Multimedia U-APSD (WMM-UAPSD) Powersave: ☑

WMM TSPEC Min Inactivity Interval: 0 msec

WMM DSCP Mapping Control: ☑

DSCP mapping for WMM voice AC (0-63): 46

DSCP mapping for WMM video AC (0-63): 26

DSCP mapping for WMM best-effort AC (0-63): 24

DSCP mapping for WMM background AC (0-63): 0

WMM Access Class of EAP traffic: voice

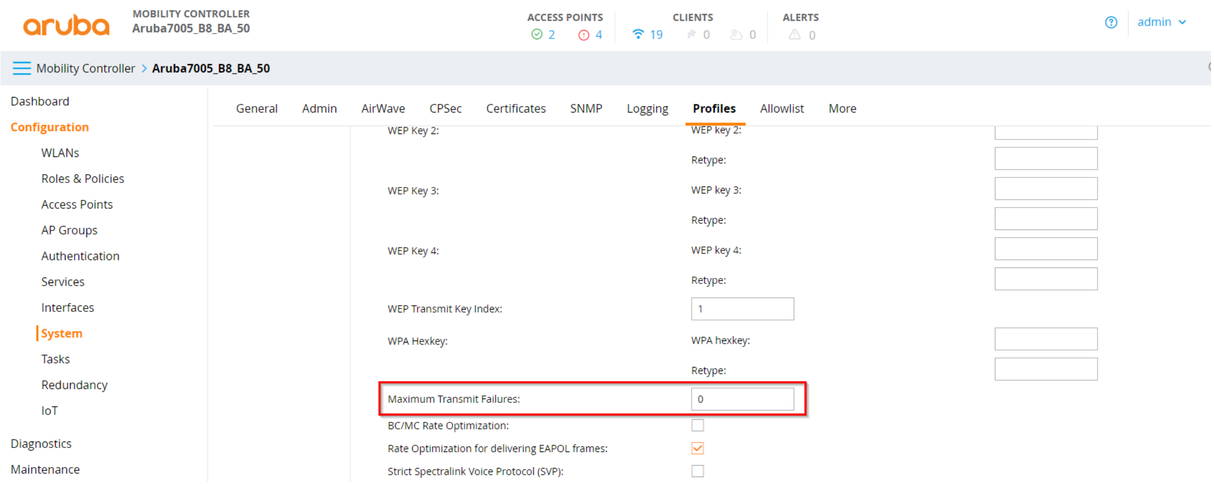
Multiple Tx Replay Counters: ☑

Hide SSID: □

Max Transmit Attempts is left at its default value 4.

Ensure that WMM and WMM Multimedia U-APSD are enabled. These parameters are mandatory for good performance.

To match the default values in the i63 ensure to use DSCP 46 for Voice and 26 for Video.



WEP Key 2: WEP key 2: / Retype:

WEP Key 3: WEP key 3: / Retype:

WEP Key 4: WEP key 4: / Retype:

WEP Transmit Key Index: 1

WPA Hexkey: WPA hexkey: / Retype:

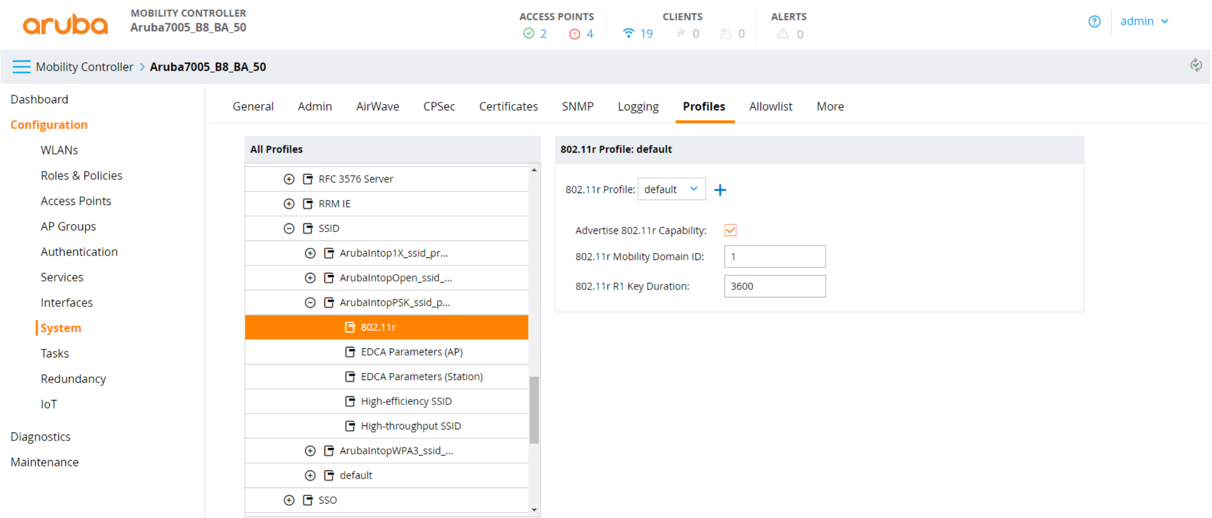
Maximum Transmit Failures: 0

BC/MC Rate Optimization: □

Rate Optimization for delivering EAPOL frames: ☑

Strict Spectralink Voice Protocol (SVP): □

Maximum Transmit Failures is set to its default 0, which means the function is disabled.



802.11r Profile: default

802.11r Profile: default

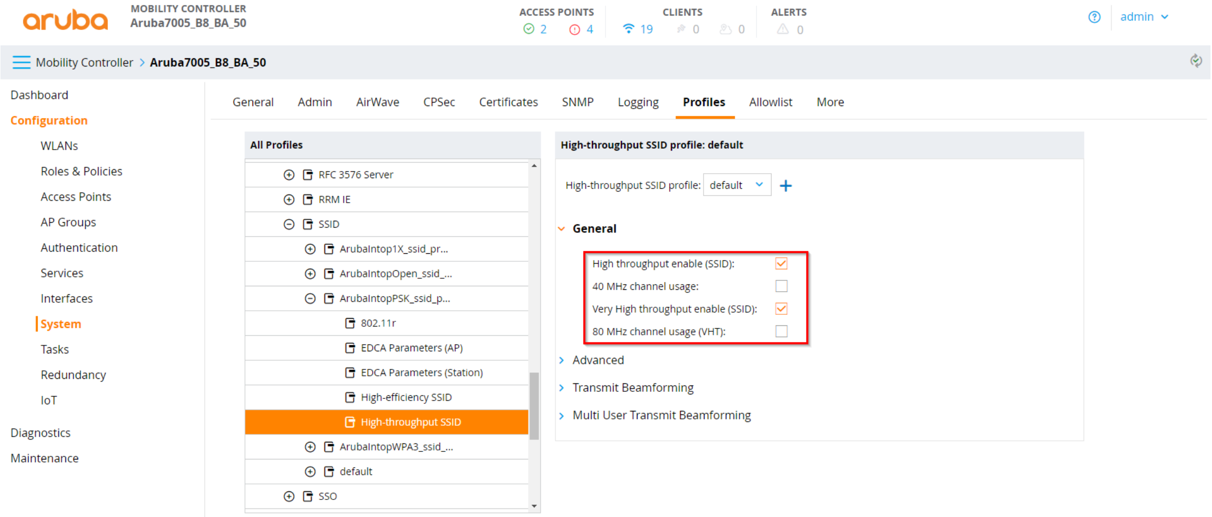
Advertise 802.11r Capability: ☑

802.11r Mobility Domain ID: 1

802.11r R1 Key Duration: 3600

It is highly recommended to use Fast Transition (802.11r).

For acceptable roaming times it is mandatory for WPA3.



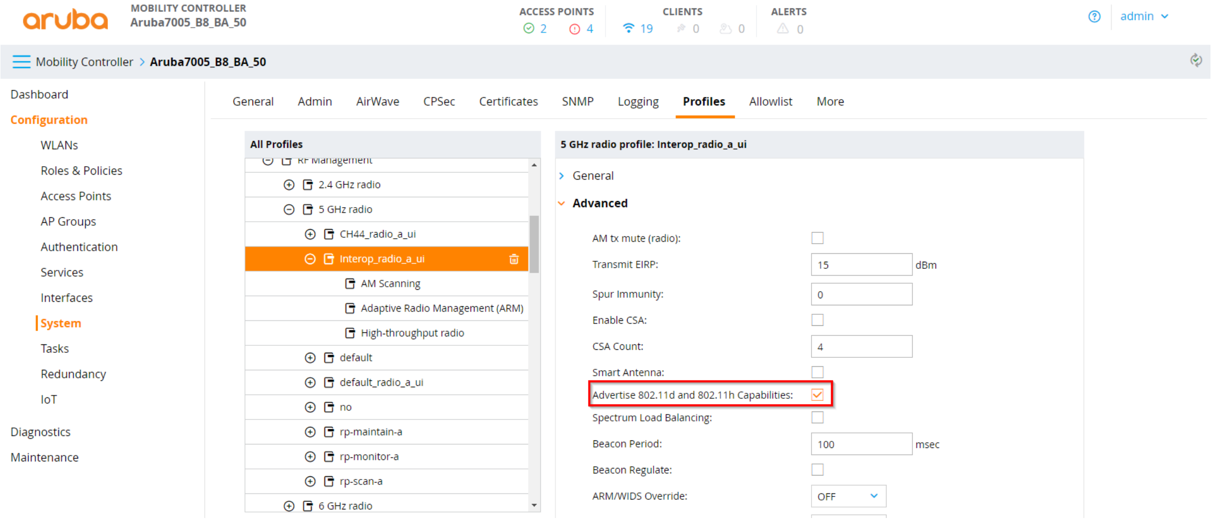
High-throughput SSID profile: default

High-throughput SSID profile: default

General

High throughput enable (SSID):	☑
40 MHz channel usage:	□
Very High throughput enable (SSID):	☑
80 MHz channel usage (VHT):	□

“High throughput enable” and “Very High throughput” enables 802.11n and 802.11ac capabilities are supported and recommended. Ascom recommends using 20 MHz channel width for voice deployments.



5 GHz radio profile: Interop_radio_a_ui

General

Advanced

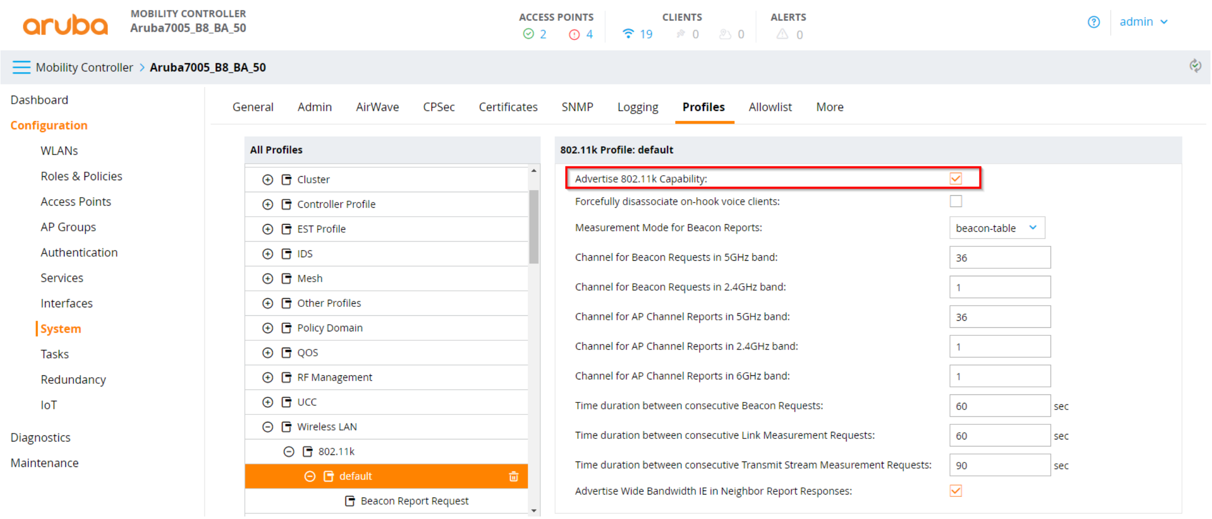
AM tx mute (radio):	□
Transmit EIRP:	15 dBm
Spur Immunity:	0
Enable CSA:	□
CSA Count:	4
Smart Antenna:	□
Advertise 802.11d and 802.11h Capabilities:	☑
Spectrum Load Balancing:	□
Beacon Period:	100 msec
Beacon Regulate:	□
ARM/WIDS Override:	OFF

For the 802.11d “Country Information” element to be broadcasted on non DFS channels it is necessary to have 802.11k enabled. This is important for regions utilizing “world mode” regulatory domain,

Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities. Recommended settings for 802.11b/g/n are to use only channel 1, 6 and 11. 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 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 VoWi-Fi deployments**



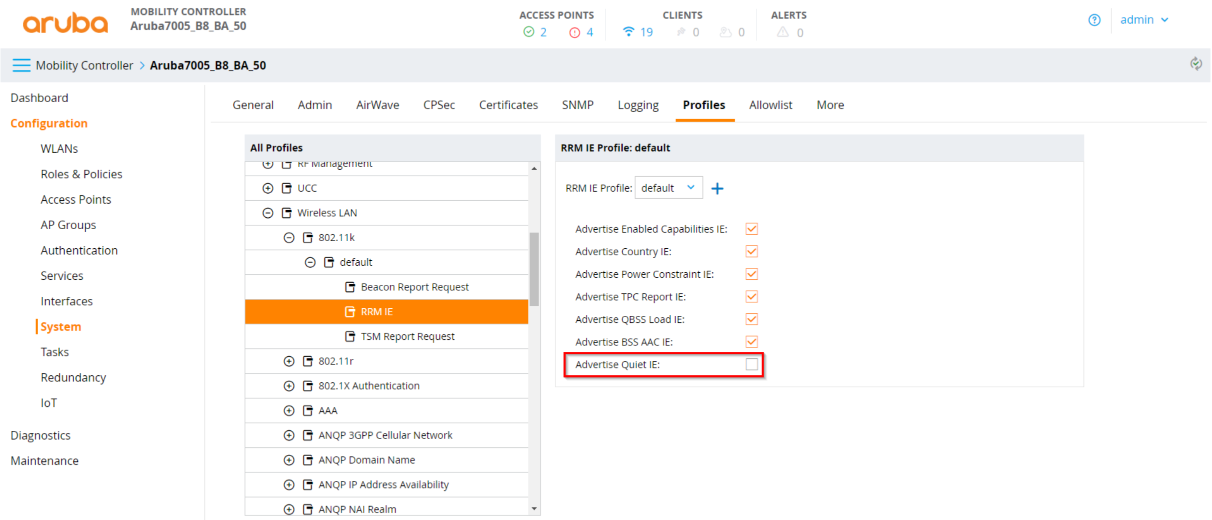
802.11k Profile: default

Advertise 802.11k Capability:	☑
Forcefully disassociate on-hook voice clients:	□
Measurement Mode for Beacon Reports:	beacon-table
Channel for Beacon Requests in 5GHz band:	36
Channel for Beacon Requests in 2.4GHz band:	1
Channel for AP Channel Reports in 5GHz band:	36
Channel for AP Channel Reports in 2.4GHz band:	1
Channel for AP Channel Reports in 6GHz band:	1
Time duration between consecutive Beacon Requests:	60 sec
Time duration between consecutive Link Measurement Requests:	60 sec
Time duration between consecutive Transmit Stream Measurement Requests:	90 sec
Advertise Wide Bandwidth IE in Neighbor Report Responses:	☑

Enable 802.11k.

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

For backwards compatibility with legacy Ascom handsets i62, Myco 1 and Myco 2 it is mandatory to disable “Advertise Quiet IE”.



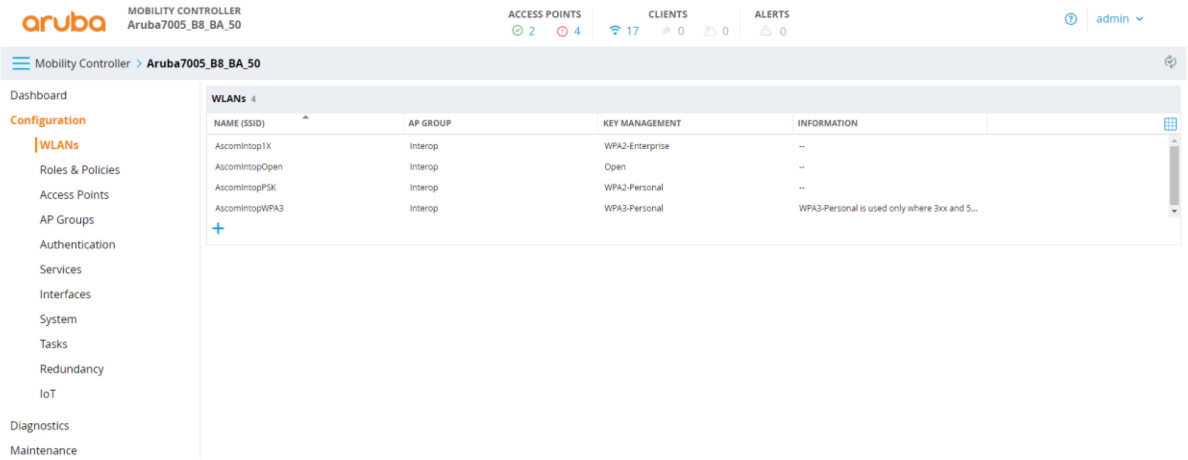
RRM IE Profile: default

RRM IE Profile: default

Advertise Enabled Capabilities IE:	☑
Advertise Country IE:	☑
Advertise Power Constraint IE:	☑
Advertise TPC Report IE:	☑
Advertise QBSS Load IE:	☑
Advertise BSS AAC IE:	☑
Advertise Quiet IE:	□

Disable “Advertise Quiet IE” and leave all other features enabled.

WLAN, Encryption and Authentication Settings

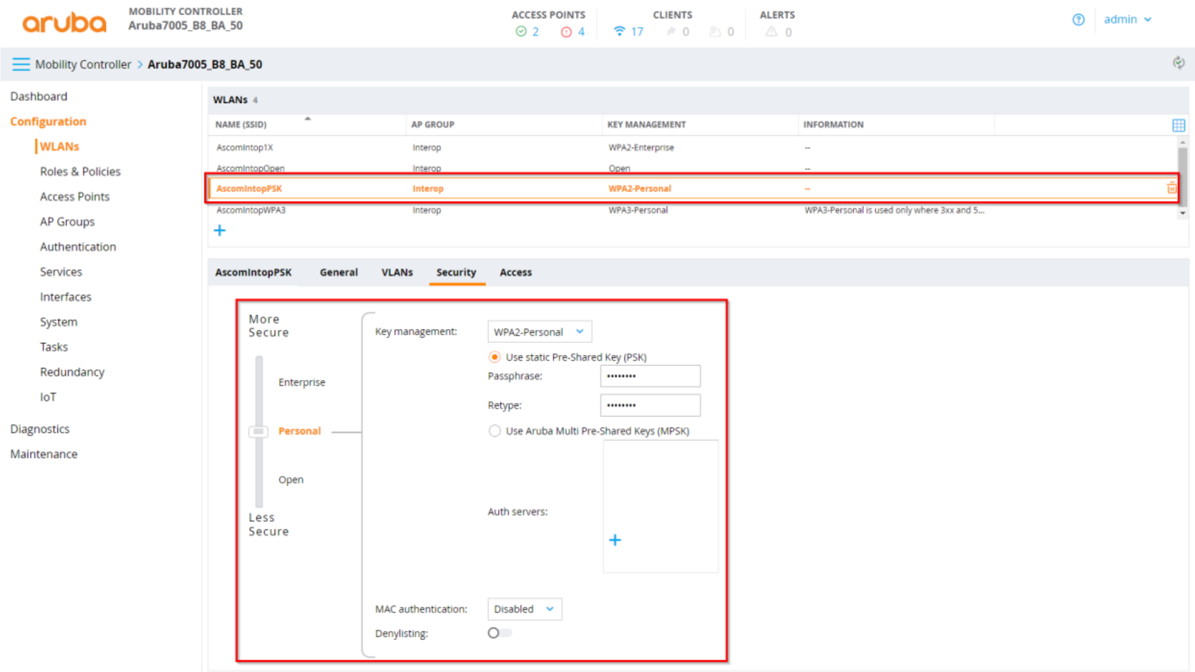


WLANs 4

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
AscomIntop1X	Interop	WPA2-Enterprise	--
AscomIntopOpen	Interop	Open	--
AscomIntopPSK	Interop	WPA2-Personal	--
AscomIntopWPA3	Interop	WPA3-Personal	WPA3-Personal is used only where 3xx and 5...

WLAN Overview

WPA2-Personal (PSK) Configuration



WLANs 4

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
AscomIntop1X	Interop	WPA2-Enterprise	--
AscomIntopOpen	Interop	Open	--
AscomIntopPSK	Interop	WPA2-Personal	--
AscomIntopWPA3	Interop	WPA3-Personal	WPA3-Personal is used only where 3xx and 5...

Key management: WPA2-Personal

● Use static Pre-Shared Key (PSK)

Passphrase: ••••••••

Retype: ••••••••

○ Use Aruba Multi Pre-Shared Keys (MPSK)

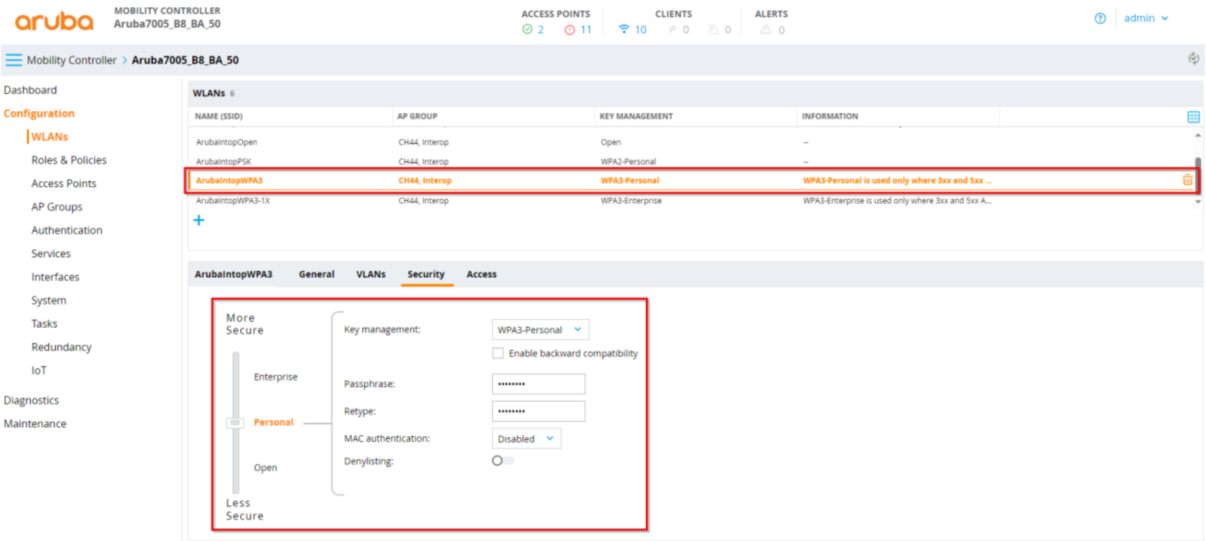
Auth servers:

MAC authentication: Disabled

Denylisting:

Set security to Personal, Key management to WPA2-Personal and enter a Passphrase.

WPA3-Personal (SAE) Configuration



WLANs 6

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
ArubaIntopOpen	CH44, Interop	Open	--
ArubaIntopPSK	CH44, Interop	WPA2-Personal	--
ArubaIntopWPA3	CH44, Interop	WPA3-Personal	WPA3-Personal is used only where 3xx and 5xx ...
ArubaIntopWPA3-1X	CH44, Interop	WPA3-Enterprise	WPA3-Enterprise is used only where 3xx and 5xx A...

Key management: WPA3-Personal

□ Enable backward compatibility

Passphrase: ••••••••

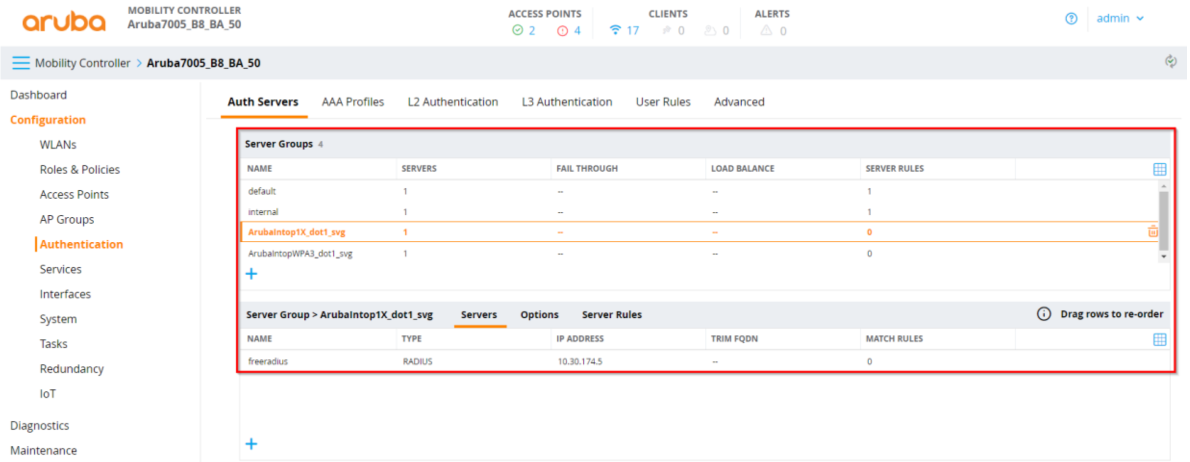
Retype: ••••••••

MAC authentication: Disabled

Denylisting: ○

Set security to Personal, Key management to WPA3-Personal and enter a Passphrase.

AAA Authentication profile Overview (802.1X Authentication)

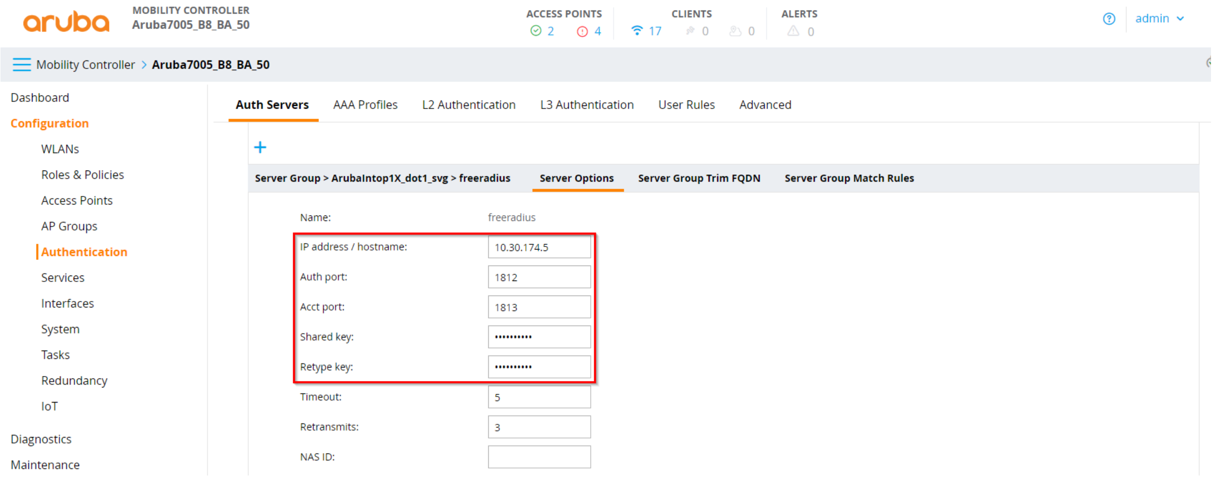


Server Groups 4

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
default	1	--	--	1
internal	1	--	--	1
ArubaIntop1X_dot1_svg	1	--	--	0
ArubaIntopWPA3_dot1_svg	1	--	--	0

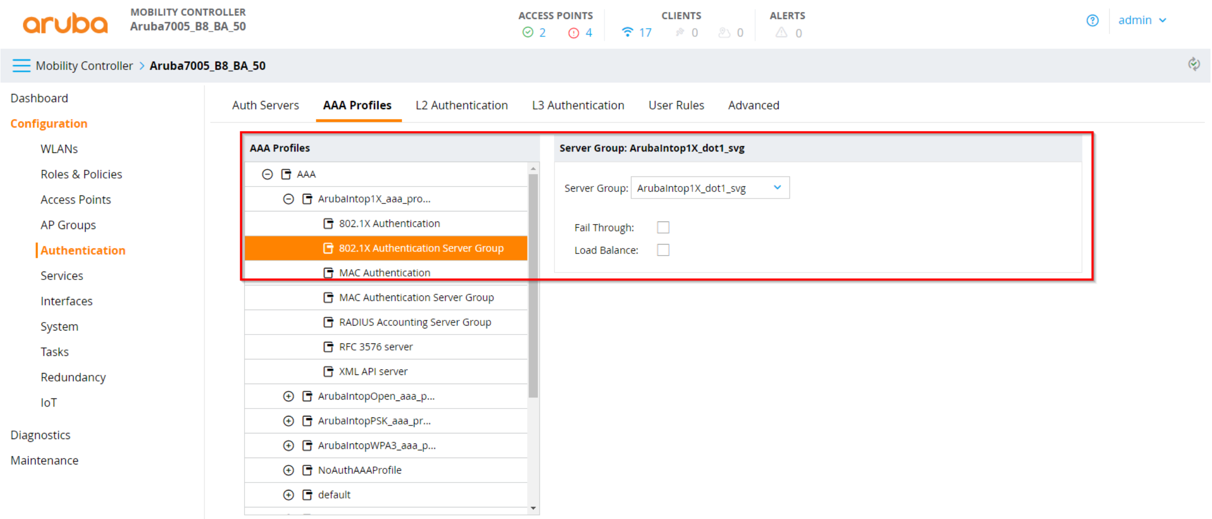
NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
freeradius	RADIUS	10.30.174.5	--	0

Create a Server group and add a server.



Name:	freeradius
IP address / hostname:	10.30.174.5
Auth port:	1812
Acct port:	1813
Shared key:	••••••••••
Retype key:	••••••••••
Timeout:	5
Retransmits:	3
NAS ID:	

When configuring the authentication server, the IP address and Shared Key must correspond to the IP address and credentials used by the Radius server. The created Radius server needs to be added to the Server Group.



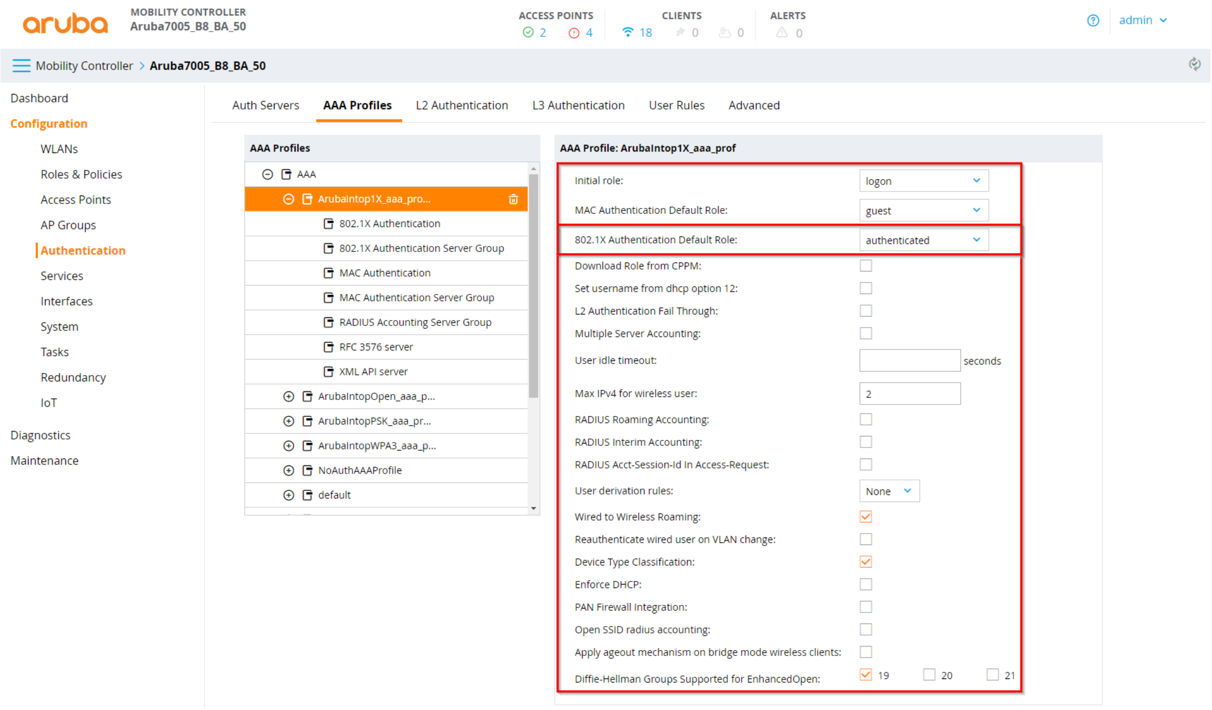
Server Group: ArubaIntop1X_dot1_svg

Server Group: ArubaIntop1X_dot1_svg

Fail Through: □

Load Balance: □

Select the Server Group just created.



AAA Profile: ArubaIntop1X_aaa_prof

Initial role: logon

MAC Authentication Default Role: guest

802.1X Authentication Default Role: authenticated

Download Role from CPPM: □

Set username from dhcp option 12: □

L2 Authentication Fail Through: □

Multiple Server Accounting: □

User idle timeout: seconds

Max IPv4 for wireless user: 2

RADIUS Roaming Accounting: □

RADIUS Interim Accounting: □

RADIUS Acct-Session-Id In Access-Request: □

User derivation rules: None

Wired to Wireless Roaming: ☑

Reauthenticate wired user on VLAN change: □

Device Type Classification: ☑

Enforce DHCP: □

PAN Firewall Integration: □

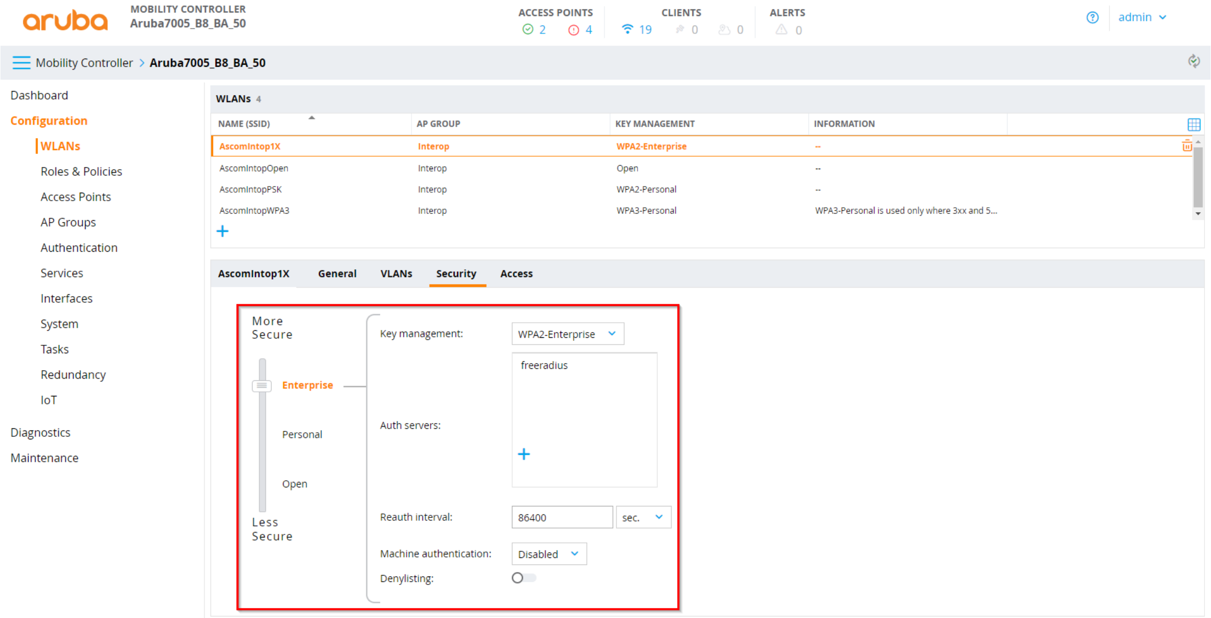
Open SSID radius accounting: □

Apply ageout mechanism on bridge mode wireless clients: □

Diffie-Hellman Groups Supported for EnhancedOpen: ☑ 19 □ 20 □ 21

Create an 802.1X Authentication Profile.
All settings Except the “802.1X Authentication Default Role” that is set to “authenticated” are left as default.

WPA2-Enterprise Overview (802.1X Authentication PEAP-MSCHAPv2)



WLANs 4

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
AscomIntop1X	Interop	WPA2-Enterprise	--
AscomIntopOpen	Interop	Open	--
AscomIntopPSK	Interop	WPA2-Personal	--
AscomIntopWPA3	Interop	WPA3-Personal	WPA3-Personal is used only where 3xx and 5...

AscomIntop1X | General | VLANs | Security | Access

Key management: WPA2-Enterprise

Auth servers: freeradius

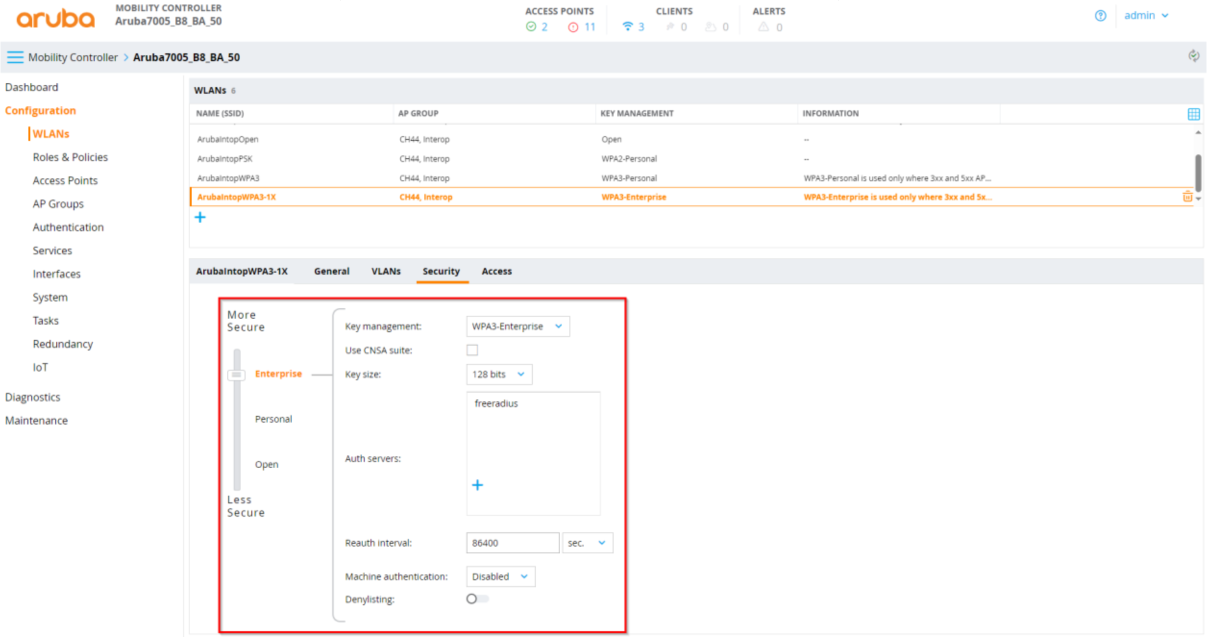
Reauth interval: 86400 sec.

Machine authentication: Disabled

Denylisting: ○

Set Security to “Enterprise”. Key management to WPA2-Enterprise and add the created Authentication server, Freeradius in this example.

WPA3-Enterprise Overview (802.1X Authentication PEAP-MSCHAPv2)



WLANs 6

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
ArubaIntopOpen	CH44, Interop	Open	--
ArubaIntopPSK	CH44, Interop	WPA2-Personal	--
ArubaIntopWPA3	CH44, Interop	WPA3-Personal	WPA3-Personal is used only where 3xx and 5xx AP...
ArubaIntopWPA3-1X	CH44, Interop	WPA3-Enterprise	WPA3-Enterprise is used only where 3xx and 5x...

ArubaIntopWPA3-1X | General | VLANs | Security | Access

Key management: WPA3-Enterprise

Use CNSA suite: □

Key size: 128 bits

Auth servers: freeradius

Reauth interval: 86400 sec.

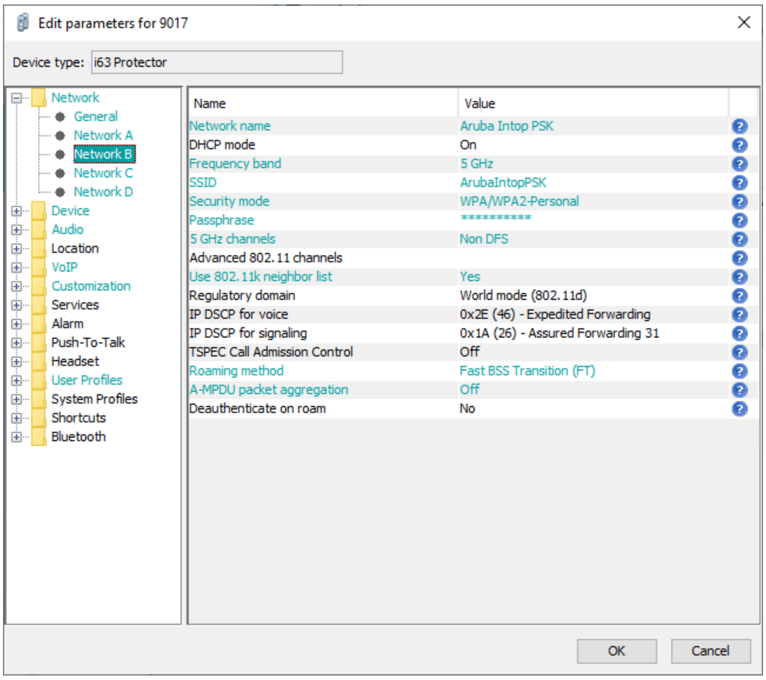
Machine authentication: Disabled

Denylisting: ○

Set Security to “Enterprise”. Key management to WPA3-Enterprise and add the created Authentication server, Freeradius in this example.

Ascom i63 Wi-Fi settings

WPA2-Personal (PSK) Network Settings



Device type: i63 Protector

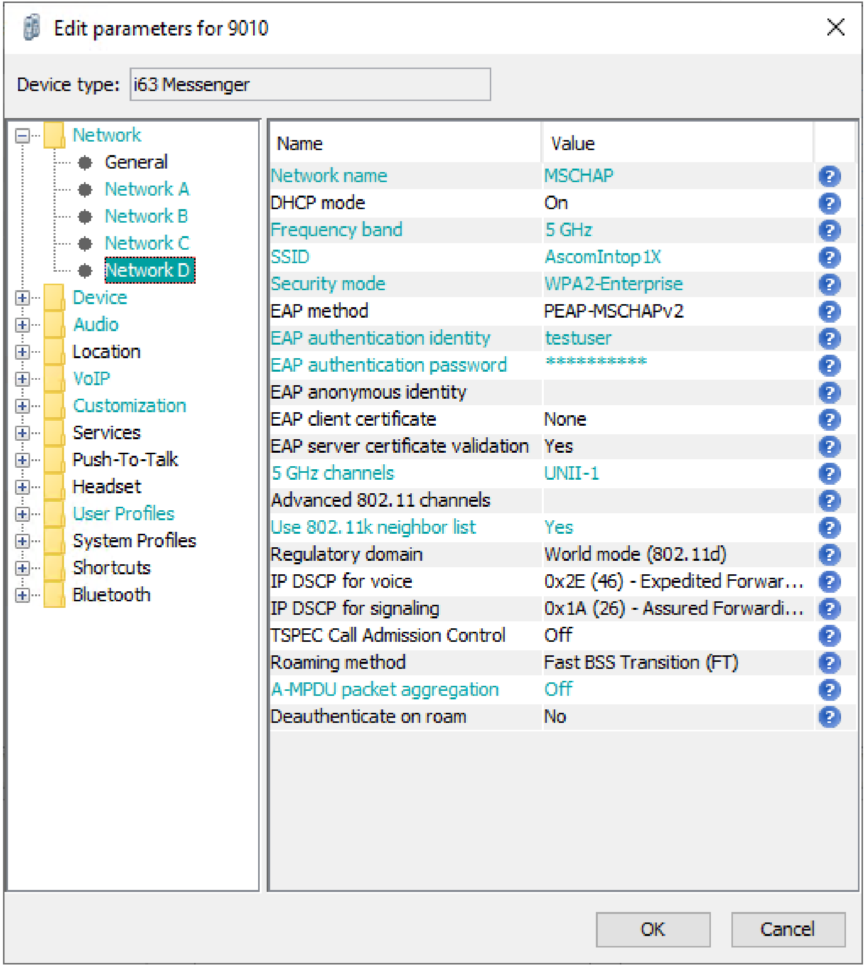
Name	Value
Network name	Aruba Intop PSK
DHCP mode	On
Frequency band	5 GHz
SSID	ArubaIntopPSK
Security mode	WPA/WPA2-Personal
Passphrase	**********
5 GHz channels	Non DFS
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
Roaming method	Fast BSS Transition (FT)
A-MPDU packet aggregation	Off
Deauthenticate on roam	No

Network settings for WPA2-Personal

- Select frequency band according to system setup (here 5GHz)
- Enter 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)
- Set A-MPDU packet aggregation to off. This is a compatibility setting to minimize network disconnects.

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

WPA2-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



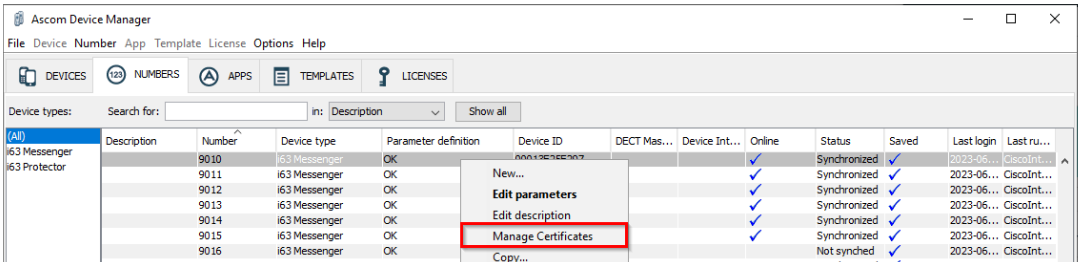
Device type: i63 Messenger

Name	Value
Network name	MSCHAP
DHCP mode	On
Frequency band	5 GHz
SSID	AscomIntop1X
Security mode	WPA2-Enterprise
EAP method	PEAP-MSCHAPv2
EAP authentication identity	testuser
EAP authentication password	**********
EAP anonymous identity	
EAP client certificate	None
EAP server certificate validation	Yes
5 GHz channels	UNII-1
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwar…
IP DSCP for signaling	0x1A (26) - Assured Forwardi…
TSPEC Call Admission Control	Off
Roaming method	Fast BSS Transition (FT)
A-MPDU packet aggregation	Off
Deauthenticate on roam	No

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

- Select frequency band according to system setup (here 5GHz)
- Enter the configured SSID
- Select Security mode WPA2-Enterprise
- Enter 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.
- Set A-MPDU packet aggregation to off. This is a compatibility setting to minimize network disconnects.

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

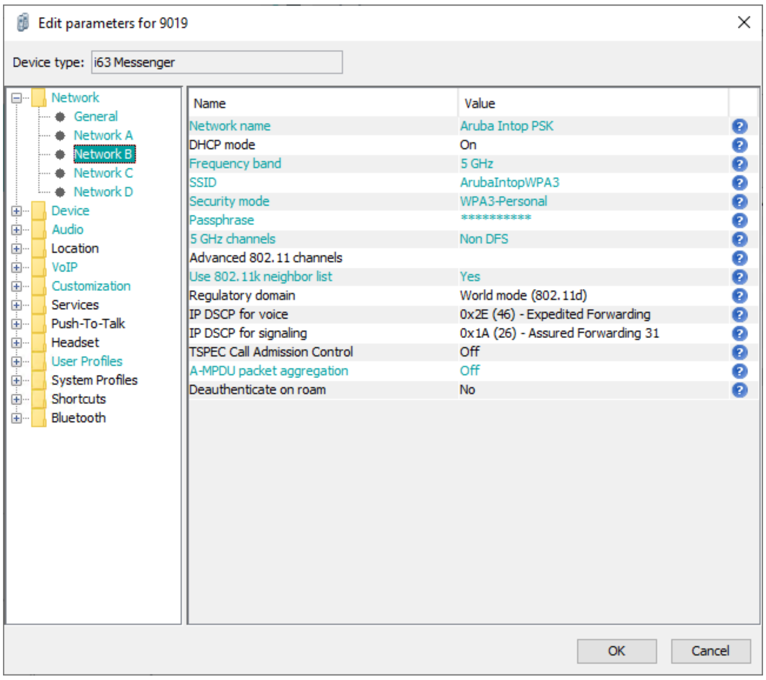


Description	Number	Device type	Parameter definition	Device ID	DECT Mas…	Device Int…	Online	Status	Saved	Last login	Last ru…
	9010	i63 Messenger	OK	[illegible]			✓	Synchronized	✓	2023-06…	CiscoInt…
	9011	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9012	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9013	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9014	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9015	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9016	i63 Messenger	OK					Not synched	✓	2023-06…	CiscoInt…

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

Note that for EAP-TLS both a CA and a client certificate are needed.

WPA3-Personal (SAE) Network Settings



Device type: i63 Messenger

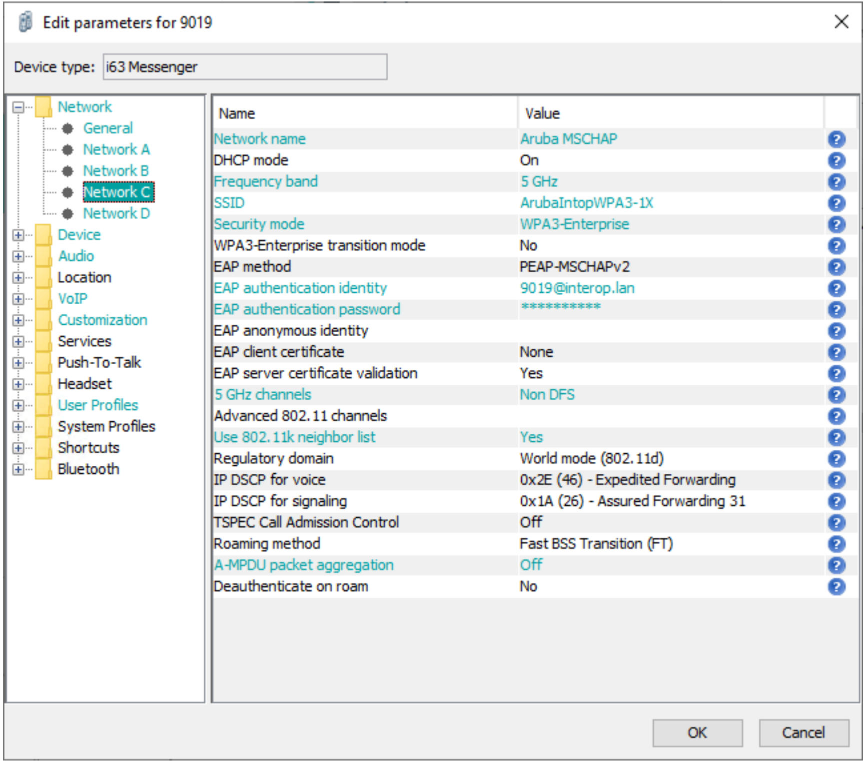
Name	Value
Network name	Aruba Intop PSK
DHCP mode	On
Frequency band	5 GHz
SSID	ArubaIntopWPA3
Security mode	WPA3-Personal
Passphrase	**********
5 GHz channels	Non DFS
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
A-MPDU packet aggregation	Off
Deauthenticate on roam	No

Network settings for WPA3-Personal

- Select frequency band according to system setup (here 5GHz)
- Enter name of SSID configured in the WLAN system
- Select Security mode WPA3-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 A-MPDU packet aggregation to off. This is a compatibility setting to minimize network disconnects.

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

WPA3-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



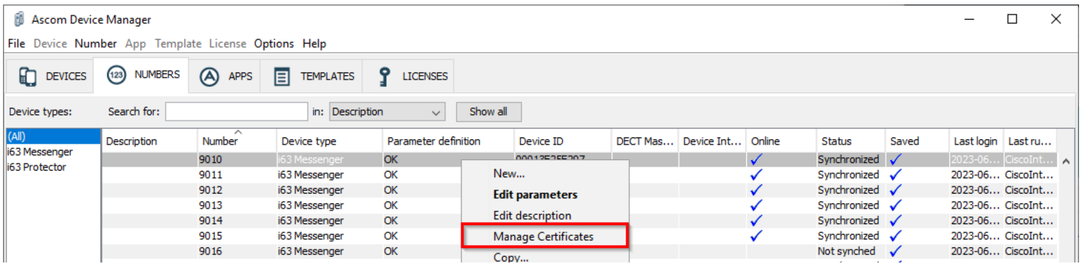
Device type: i63 Messenger

Name	Value
Network name	Aruba MSCHAP
DHCP mode	On
Frequency band	5 GHz
SSID	ArubaIntopWPA3-1X
Security mode	WPA3-Enterprise
WPA3-Enterprise transition mode	No
EAP method	PEAP-MSCHAPv2
EAP authentication identity	9019@interop.lan
EAP authentication password	**********
EAP anonymous identity	
EAP client certificate	None
EAP server certificate validation	Yes
5 GHz channels	Non DFS
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	World mode (802.11d)
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
Roaming method	Fast BSS Transition (FT)
A-MPDU packet aggregation	Off
Deauthenticate on roam	No

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

- Select frequency band according to system setup (here 5GHz)
- Enter the configured SSID
- Select Security mode WPA3-Enterprise
- Enter 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.
- Set A-MPDU packet aggregation to off. This is a compatibility setting to minimize network disconnects.

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



Description	Number	Device type	Parameter definition	Device ID	DECT Mas…	Device Int…	Online	Status	Saved	Last login	Last ru…
	9010	i63 Messenger	OK	[illegible]			✓	Synchronized	✓	2023-06…	CiscoInt…
	9011	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9012	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9013	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9014	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9015	i63 Messenger	OK				✓	Synchronized	✓	2023-06…	CiscoInt…
	9016	i63 Messenger	OK					Not synched	✓	2023-06…	CiscoInt…

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

Note that both a CA and a client certificate are needed for EAP-TLS.

Appendix B: Detailed Validation Records

Pass	23
Fail	1
Comments	3
Not verified	5
Total	32

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

Document History

Rev	Date	Author	Description
D1	September 09 2024	NLRPa	Draft. AOS 8.10.0.13 LSR
D2	September 17 2024	NLRPa	Added WPA3