

INTEROPERABILITY REPORT

Ascom i63  
HPE Aruba Networking Central

Cloud-managed Wi-Fi Platform

AOS v. 10.4.1.3\_90100

Ascom i63 v.6.0.0

Utrecht, The Netherlands

August 2024

**ascom**

# Contents

<b>Introduction.....</b>	<b>3</b>
About Ascom.....	3
About HPE Aruba Networking .....	3
<b>Site Information.....</b>	<b>4</b>
Test site .....	4
Participants .....	4
Test topology.....	4
<b>Summary .....</b>	<b>5</b>
General conclusions .....	5
Compatibility information .....	5
Interoperability Validation Overview.....	6
Known limitations.....	7
<b>Appendix A: Validation Configurations .....</b>	<b>8</b>
Aruba Central, AOS 10.4.1.3 (build 90100).....	8
Ascom i63 Wi-Fi settings .....	14
<b>Appendix B: Detailed Validation Records .....</b>	<b>18</b>
<b>Document History .....</b>	<b>18</b>

# 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 HPE on Twitter and Facebook, and for the latest technical discussions on mobility and HPE Aruba Networking products visit Airheads Social at <http://community.arubanetworks.com>.

# Site Information

## Test site

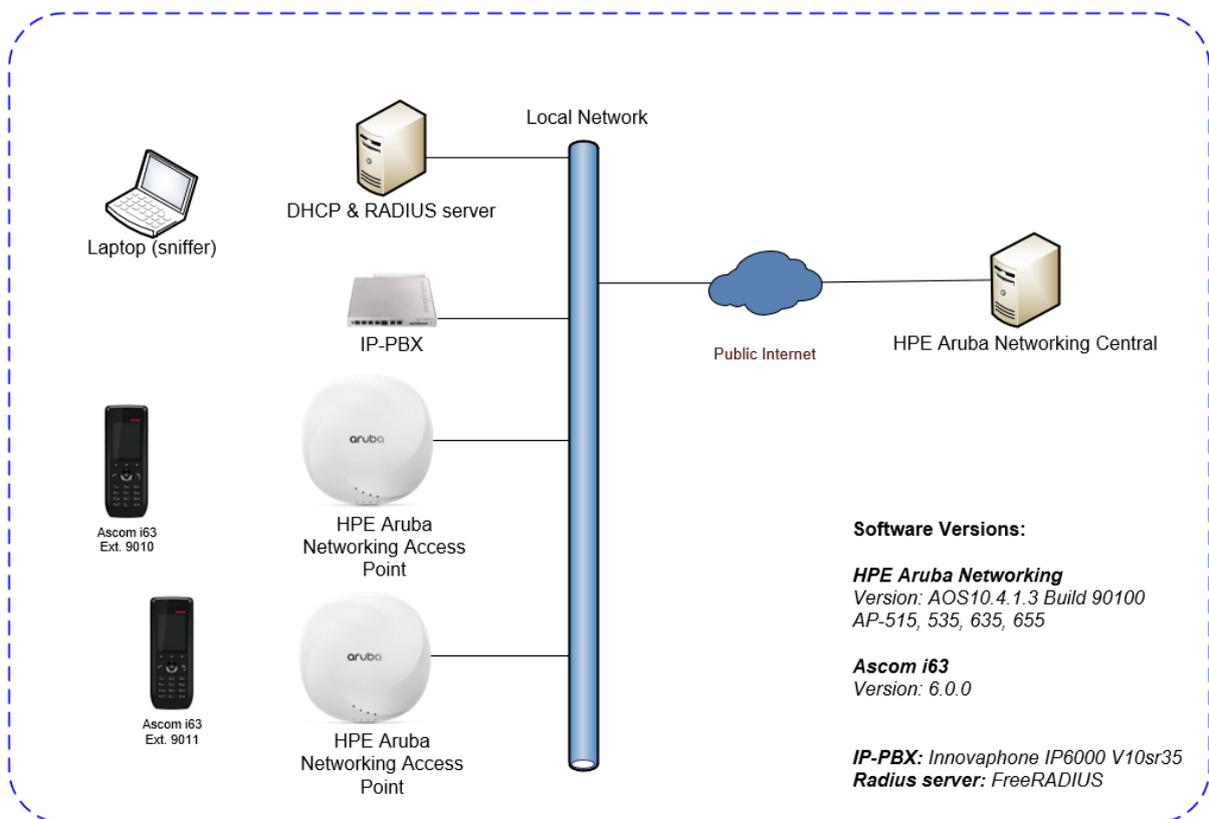
Ascom Nederland  
Orteliuslaan 982  
3528 BD Utrecht  
The Netherlands

## Participants

Remco van den Pangaart, Ascom, The Netherlands

## Test topology

All test cases were completed using Ascom i63 version 6.0.0



# Summary

## General conclusions

This interoperability validation produced good results with regard to tested areas, such as authentication, stability, QoS and roaming. Roaming times were in general very good with all authentication methods. Observed times were typically around 26 - 50ms.

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

## Compatibility information

One Access Point model from every product generation has been selected: AP-515, AP-535, AP635 and AP-655. By testing these access points, Ascom is considered to have coverage of all Access Points listed below based on chipset compatibility.

In this configuration, HPE Aruba Networking Central, a cloud-managed Wi-Fi platform, is used to manage the Access Points.

## Supported Partner Access Points with AOS version 10.4.1.3\_90100:

AP-303, 304, 305, 314, 315, 324, 325, 334, 335, 344, 345

AP-504, 505, 514, 515, 534, 535, 554, 555

AP-635, 655

**Interoperability Validation Overview**  
**WLAN Compatibility and Performance**

High Level Functionality	Result	Comments
Association, WPA2-PSK / AES Encryption	OK	
Association, PEAP-MSCHAPv2 Auth, AES Encryption	OK	
Association with EAP-TLS authentication	OK	
Association with WPA3-SAE, Transition Mode	OK	
Association with WPA3-SAE authentication, AES encryption + FT	OK	
Association with WPA3-Enterprise + FT	OK	
Beacon Interval and DTIM Period	OK	
WMM Prioritization	OK	
WPA2-opportunistic/proactive Key Caching	OK	
802.11e U-APSD	OK	
CAC - TSPEC	OK	
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time: 36 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time: 34 ms
Roaming, WPA3-SAE authentication, AES encryption + FT	OK	Typical roaming time: 26 ms
Roaming, WPA3-Enterprise + FT	OK	Typical roaming time: 27 ms
Channel bonding 40/80/160MHz	OK	
Channel usage controlled by 802.11k	OK	
Network features controlled by 802.11v	N/T	Not supported by i63
Association with Protected Management Frames 802.11w	OK	
Association and roaming on 6 GHz	N/T	Not supported by 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
The handset is unable to connect with EAP-TLS using SHA1 certificate.	No workaround available	Ascom WH2-4310

For additional information regarding the known limitations please contact [interop@ascom.com](mailto:interop@ascom.com) or [support@ascom.com](mailto:support@ascom.com).

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

# Appendix A: Validation Configurations

## HPE Aruba Networking Central, AOS 10.4.1.3 (build 90100)

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

### WLAN, SSID and Security Settings

#### WLAN Overview

Name (Profile)	Security	Access Type	Traffic forwarding mode	Network Enabled
AOS10IntopPSK	wpa2-psk-aes	Unrestricted	Bridge	Yes
AOS10Intop1X	wpa2-aes	Unrestricted	Bridge	Yes
AOS10IntopWPA3	wpa3-sae-aes	Unrestricted	Bridge	Yes
AOS10IntopOpen	opensystem	Unrestricted	Bridge	No
AOS10IntopWPA3-1X	wpa3-aes-ccm-128	Unrestricted	Bridge	Yes

#### WPA2-Personal Overview (PSK)

See below for WPA2-Personal settings:

General		Security	
ESSID	AOS10IntopPSK	Security Level	Personal
Multicast Optimization	disabled	Auth Server 1	InternalServer
Band	2.4, 5	Key Management	WPA2-Personal
DTIM Interval	5 beacons	MAC Authentication	disabled
Primary Usage	employee	<b>VLANS</b>	
Inactivity Timeout	1000 secs	Traffic forwarding mode	Bridge
Dynamic Multicast OPT	disabled	Client VLAN Assignment	
Airtime	unlimited	VLAN	1
Hide SSID	disabled	<b>Access</b>	
Broadcast filtering	arp	ROLE ASSIGNMENTS FOR AUTHENTICATED USERS	disabled
Transmit Rates (legacy Only)		Enforce Mac Auth Only Role	disabled
	<b>2.4 GHz</b> Min: 12Mbps Max: 54Mbps	Assign Pre-Authentication Role	disabled
	<b>5 GHz</b> Min: 12Mbps Max: 54Mbps	Enforce Machine Authentication	disabled

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

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

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

## WPA3-Personal Overview (SAE)

See below for WPA3-Personal settings:

Category	Setting	Value
General	ESSID	AOS10IntopWPA3
	Multicast Optimization	disabled
	Band	all
	DTIM Interval	2 beacons
	Primary Usage	employee
	Inactivity Timeout	1000 secs
	Dynamic Multicast OPT	disabled
	Airtime	unlimited
	Hide SSID	disabled
	Broadcast filtering	arp
Transmit Rates (legacy Only)	2.4 GHz	Min: 12Mbps Max: 54Mbps
	5 GHz	Min: 12Mbps Max: 54Mbps
Security	Security Level	Personal
	Auth Server 1	InternalServer
	Key Management	WPA3-Personal
	MAC Authentication	disabled
VLANs	Traffic forwarding mode	Bridge
	Client VLAN Assignment	
Access	VLAN	1
	ROLE ASSIGNMENTS FOR AUTHENTICATED USERS	disabled
	Enforce Mac Auth Only Role	disabled
	Assign Pre-Authentication Role	disabled
	Enforce Machine Authentication	disabled

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

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

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

## WPA2-Enterprise Overview (802.1X Authentication)

See below for WPA2-Enterprise settings:

The screenshot shows the configuration page for AOS10-AP. The left sidebar contains a navigation menu with categories: Manage (Overview, Devices, Clients, Guests, Applications, Security), Analyze (Alerts & Events, Audit Trail, Tools, Reports), and Maintain (Firmware, Organization). The main content area is titled 'Network Summary' and is divided into two columns: 'General' and 'Security'. The 'General' column includes settings for ESSID (AOS10Intop1X), Multicast Optimization (disabled), Band (2.4, 5), DTIM Interval (5 beacons), Primary Usage (employee), Inactivity Timeout (1000 secs), Dynamic Multicast OPT (disabled), Airtime (unlimited), Hide SSID (disabled), Broadcast filtering (arp), and Transmit Rates (2.4 GHz and 5 GHz). The 'Security' column includes Security Level (Enterprise), Auth Server 1 (Freeradius), Key Management (WPA2-Enterprise), MAC Authentication (disabled), VLANs (Traffic forwarding mode: Bridge, Client VLAN Assignment: Static, VLAN: 1), and Access (ROLE ASSIGNMENTS FOR AUTHENTICATED USERS: disabled, Enforce Mac Auth Only Role: disabled, Assign Pre-Authentication Role: disabled, Enforce Machine Authentication: disabled).

Create a Primary RADIUS server by selecting the highlighted pen icon.

The screenshot shows the configuration page for AOS10-AP, specifically the 'Security' tab. The 'Security Level' is set to 'Enterprise'. The 'Key Management' is set to 'WPA2-Enterprise'. The 'Server Group' is set to 'Primary and backup only'. The 'Primary Server' is set to 'Freeradius', and a pen icon is highlighted next to it. The 'Secondary Server' is set to '--Select--'. There is an 'Advanced Settings' link below the server configuration.

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 screenshot shows the 'Edit Server' dialog box. The 'Server Type' is set to 'RADIUS'. The 'Name' is 'Freeradius'. The 'IP Address/FQDN' is '10.30.174.5'. The 'Shared Key' and 'Retype Key' fields are highlighted with a red box. The 'NAS IP Address' is 'optional', 'NAS Identifier' is 'optional', 'Auth Port' is '1812', and 'Accounting Port' is '1813'. There are 'Cancel' and 'OK' buttons at the bottom right.

## WPA3-Enterprise Overview (802.1X Authentication)

See below for WPA3-Enterprise settings:

The screenshot shows the Aruba Central configuration interface for an AOS10-AP. The 'Security' tab is selected, displaying various security settings. The 'General' section includes fields for ESSID (AOS10IntopWPA3-1X), Multicast Optimization (disabled), Band (all), DTIM Interval (5 beacons), Primary Usage (employee), Inactivity Timeout (1000 secs), Dynamic Multicast OPT (disabled), Airtime (unlimited), Hide SSID (disabled), Broadcast filtering (none), and Transmit Rates (2.4 GHz and 5 GHz, both with Min: 12Mbps and Max: 54Mbps). The 'Security' section shows Security Level (Enterprise), Auth Server 1 (Freeradius), Key Management (WPA3-Enterprise(CCM 128)), and MAC Authentication (disabled). The 'VLANs' section shows Traffic forwarding mode (Bridge) and Client VLAN Assignment (VLAN 1). The 'Access' section shows Role Assignments for Authenticated Users (disabled), Enforce Mac Auth Only Role (disabled), Assign Pre-Authentication Role (disabled), and Enforce Machine Authentication (disabled).

Create a Primary RADIUS server by selecting the highlighted pen icon.

The screenshot shows the Aruba Central configuration interface for an AOS10-AP, specifically the 'Security' tab. The 'Security Level' is set to Enterprise. The 'Key Management' is set to WPA3-Enterprise(CCM 128). The 'Primary Server' dropdown is set to 'Freeradius', and a red box highlights the pen icon next to it, indicating where to click to edit the server configuration. The 'Secondary Server' is currently set to '--Select--'.

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 screenshot shows the 'Edit Server' dialog box in Aruba Central. The 'Server Type' is set to 'RADIUS'. The 'Name' field is 'Freeradius'. The 'IP Address/FQDN' field is '10.30.174.5'. The 'Shared Key' and 'Retype Key' fields are highlighted with red boxes, indicating they must be entered correctly. The 'NAS IP Address' is optional, and the 'Auth Port' is 1812. The 'Accounting Port' is 1813. The 'Dynamic Authorization' checkbox is unchecked. The 'Query Status of RADIUS Servers(RFC 5997)' checkbox is also unchecked.

## General settings (Radio, WMM and QoS)

Ensure that Client Match is enabled. This parameter activates 802.11v on the system.

The screenshot shows the Aruba Central configuration interface for Adaptive Radio Management (ARM). The left sidebar shows the navigation menu with 'Devices' selected. The main content area is titled 'Adaptive Radio Management(ARM)' and contains several sections: 'Client Control', 'Access Point Control', 'Channel Control', 'Error Rate', 'Radio', and 'External Antenna'. The 'Client Control' section is expanded, showing the following settings:

- Band Steering Mode: Prefer higher band
- Airtime Fairness Mode: Default Access
- ClientMatch:  (highlighted with a red box)
- ClientMatch Calculating Interval: 3 seconds
- ClientMatch Neighbor Matching: 60 %
- ClientMatch Threshold: 5
- ClientMatch Key: (empty text field)
- Spectrum Load Balancing Mode: Channel

Refer to the WMM multimedia settings below:

The screenshot shows the Aruba Central configuration interface for WiFi Multimedia settings. The left sidebar shows the navigation menu with 'Devices' selected. The main content area is titled 'WiFi Multimedia' and contains the following settings:

	Share	DSCP Mapping
Background WiFi Multimedia Share:	0 %	0
Best Effort WiFi Multimedia Share:	0 %	24
Video WiFi Multimedia Share:	0 %	26
Voice WiFi Multimedia Share:	0 %	46

Below the table, the following settings are visible:

- Traffic Specification(TSPEC):
- TSPEC Bandwidth: 2000 kbps
- Spectrallink Voice Protocol (SVP):
- WiFi Multimedia Power Save (U-APSD):

To match default DSCP markings used by the i63, ensure that Voice is mapped to DSCP 46 and Video to DSCP 26 in the WLAN infrastructure.

Guidelines for Fast Roaming (FT) are shown below:

The screenshot shows the Aruba Central configuration interface for a customer named 'AscomInter...'. The device selected is 'AOS10-AP'. The configuration page is for 'Access Points' and is currently on the 'WLANs' tab. The 'Fast Roaming' section is expanded and highlighted with a red box. Within this section, the following settings are highlighted with red boxes:

- 802.11r: Enabled (toggle switch is on)
- MDID: 1
- 802.11k: Enabled (toggle switch is on)
- RRM Quiet IE: Enabled (toggle switch is on)

For the best roaming performance, it is strongly recommended to use Fast Transition (802.11r).

Make sure that 802.11k and RRM Quiet IE are enabled for optimal Radio Resource Management (RRM).

**Note: When backwards compatibility is required for Ascom i62 and Myco 1 & 2, switch off “RRM Quiet IE”.**

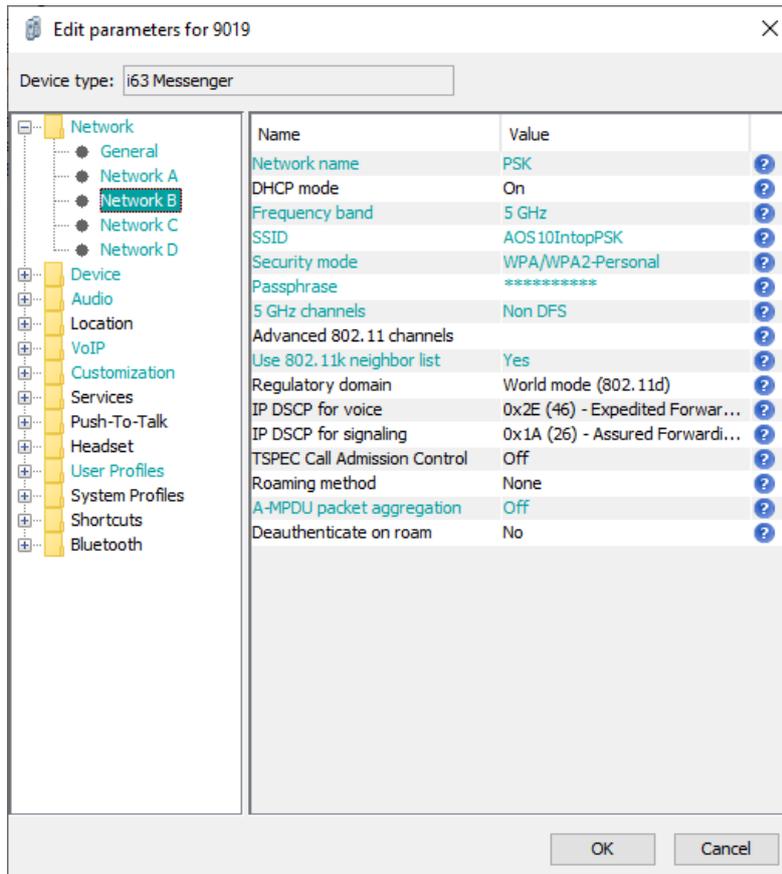
The Ascom i62 and Myco 1 & 2 do not support 11k and 11v, but normally operate without issues on an SSID where these settings are enabled (assuming i62 version 6.0.0 or later).

A Beacon Interval of 100ms and advertising 802.11d/h capabilities are best common practices. The recommended channel planning in 802.11b/g/n environments is to use channels 1, 6 and 11. For 802.11a/n/ac/ax, 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 Reports, enabling more than eight channels will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of nine enabled channels can be allowed. Ascom does not recommend exceeding these limits unless 802.11k is in use.**
- 2. Ascom supports and can coexist in 40/80/160MHz channel bonding environments. The recommendation is, however, to avoid 80/160 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**

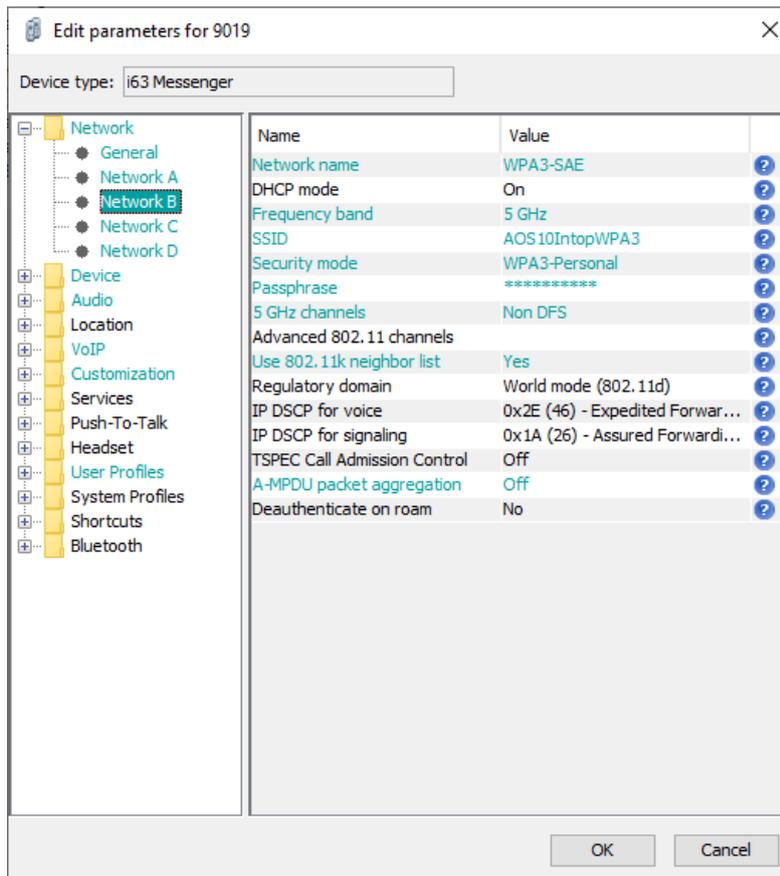
### WPA2-Personal (PSK) Network Settings



Network settings for WPA2-PSK

- Select frequency band according to system setup (here 5GHz)
- 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 A-MPDU packet aggregation to off. This is a compatibility setting to minimize network disconnects
- Note: The FCC does not allow 802.11d to determine the regulatory domain. Consequently, devices deployed in the USA must have the “Regulatory Domain” set to “FCC”.

## WPA3-Personal (SAE) Network Settings



Network settings for WPA3-SAE

- Select frequency band according to system setup (here 5GHz)
- 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: The FCC does not allow 802.11d to determine the regulatory domain. Consequently, devices deployed in the USA must have the "Regulatory Domain" set to "FCC".

## WPA2-Enterprise (PEAP-MSCHAPv2) Network Settings

Network settings for WPA2-Enterprise 1X authentication (PEAP-MSCHAPv2)

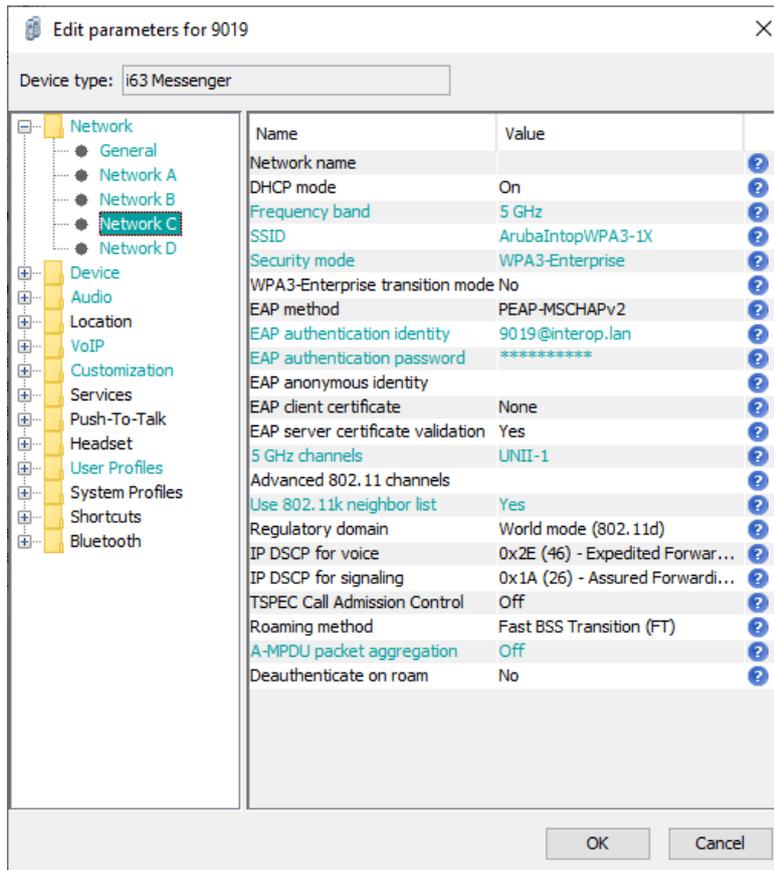
- Select frequency band according to system setup (here 5GHz)
- Select Security mode WPA2-Enterprise
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list.
- Set A-MPDU packet aggregation to off. This is a compatibility setting to minimize network disconnects
- Note: The FCC does not allow 802.11d to determine the regulatory domain. Consequently, devices deployed in the USA must have the “Regulatory Domain” set to “FCC”.

Device types:	Description	Number	Device type	Parameter definition	Device ID	DECT Mas...	Device Int...	Online	Status	Saved	Last login	Last ru...
(All)												
i63 Messenger		9010	i63 Messenger	OK				✓	Synchronized	✓	2023-06...	CiscoInt...
i63 Protector		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.

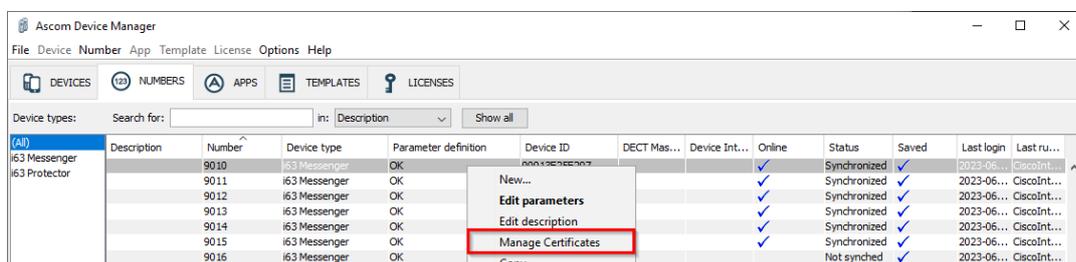
Note that both a CA and a client certificate are needed for TLS.

## WPA3-Enterprise (PEAP-MSCHAPv2) Network Settings



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

- Select frequency band according to system setup (here 5GHz)
- Select Security mode WPA3-Enterprise
- 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: The FCC does not allow 802.11d to determine the regulatory domain. Consequently, devices deployed in the USA must have the "Regulatory Domain" set to "FCC".



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 TLS.

# Appendix B: Detailed Validation Records

Pass	18
Fail	0
Comments	0
Not verified	8
<b>Total</b>	<b>26</b>

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

## Document History

Rev	Date	Author	Description
PA1	August 12, 2024	NLRPa,	Draft HPE Aruba Networking Central AOS 10.4.1.3 (build 90100).
PA2	August 14, 2024	NLRPa	Screenshots added, update Appendix B.
PA3	August 26, 2024	NLRPa	Minor corrections after review.