INTEROPERABILITY REPORT

# Ascom i63

# HPE Aruba Networking Central

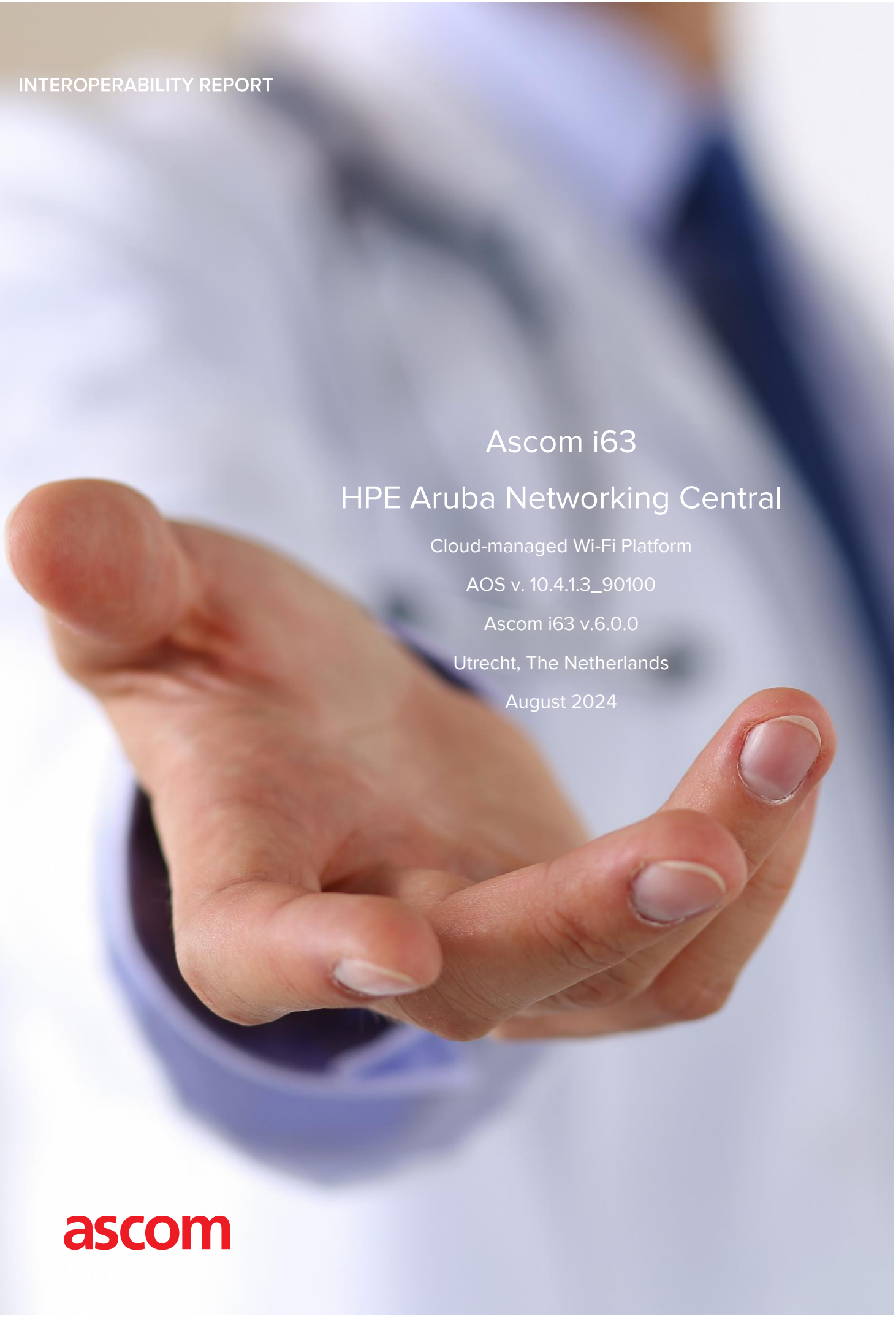
Cloud-managed Wi-Fi Platform

AOS v. 10.4.1.3_90100

Ascom i63 v.6.0.0

Utrecht, The Netherlands

August 2024



ascom

# Contents

# 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

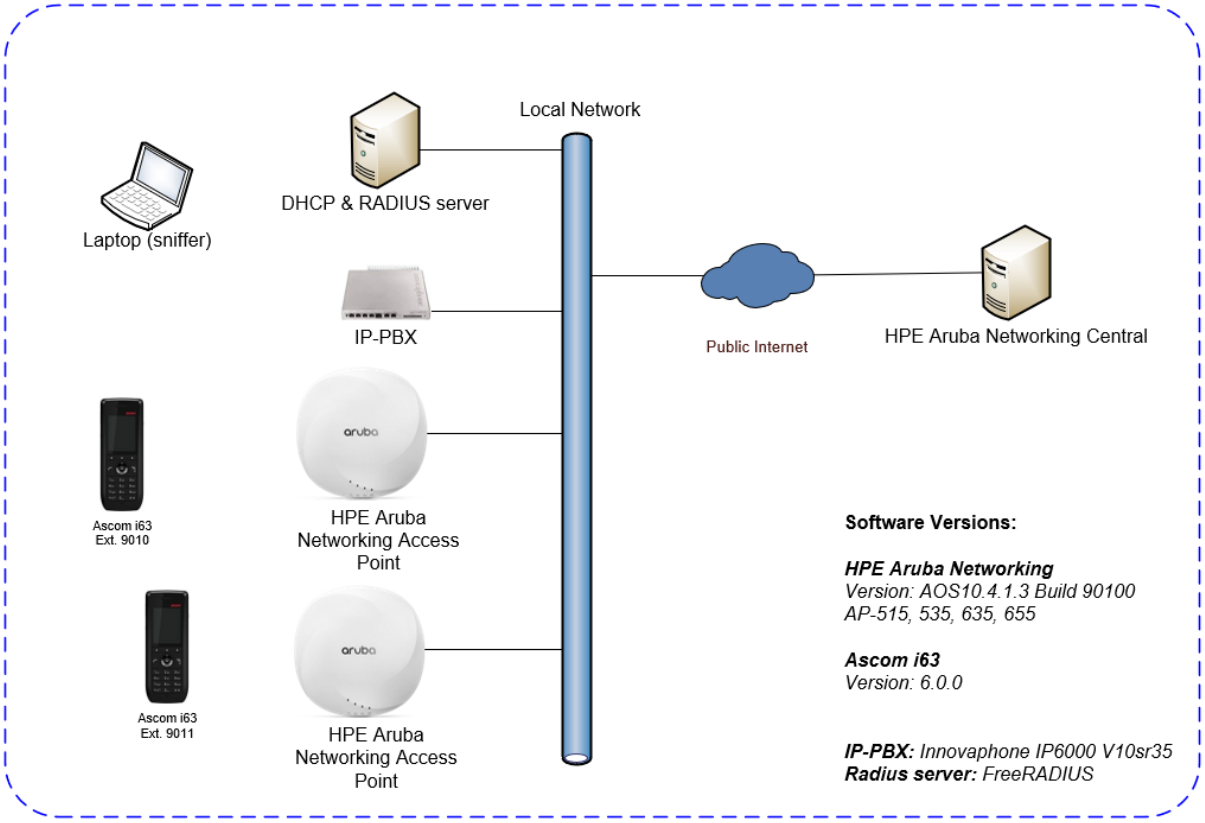
Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

### 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

**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** or **support@ascom.com**.

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

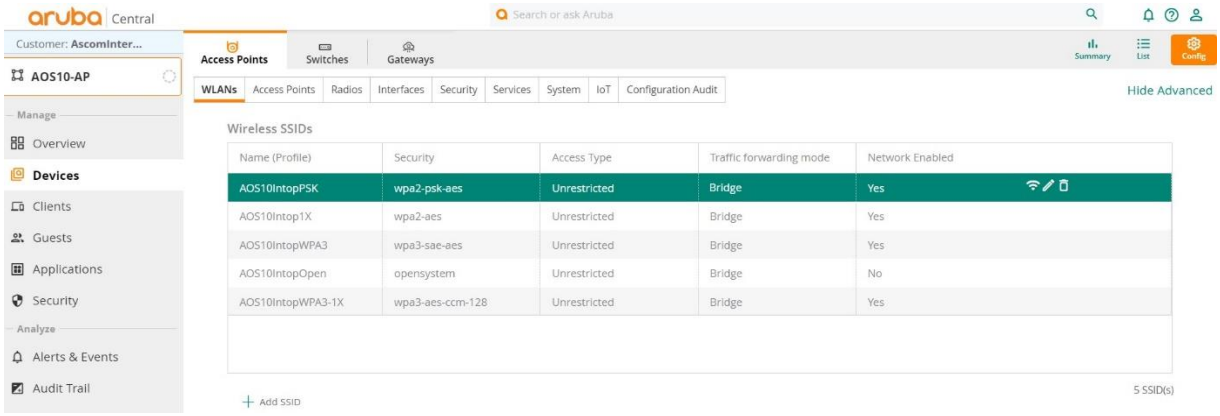
# Appendix A: Validation Configurations

### 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.

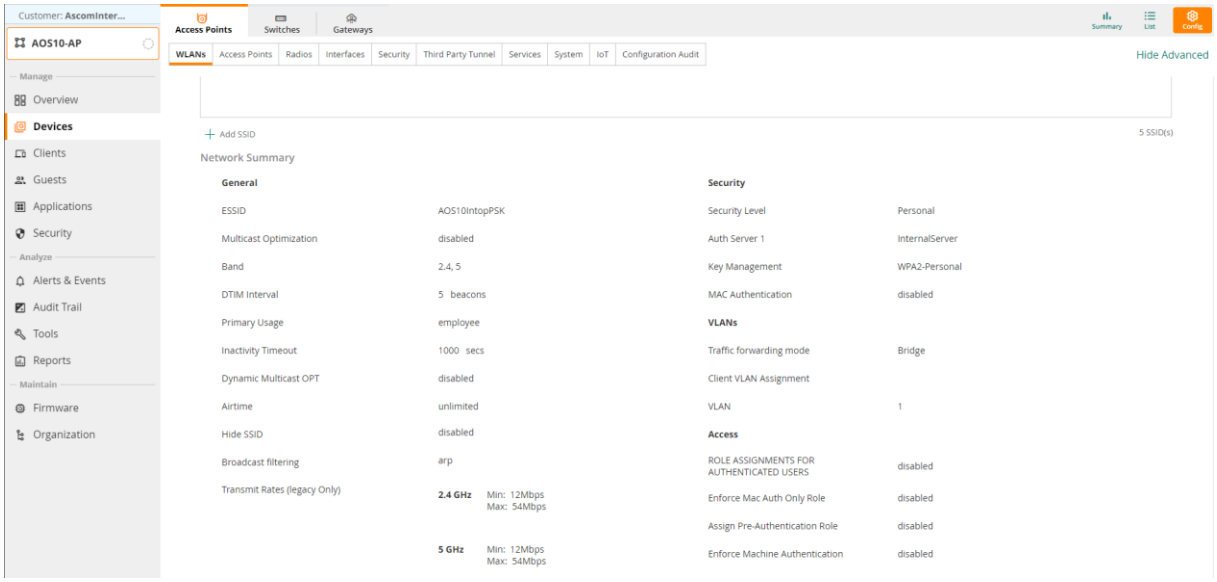
### WLAN, SSID and Security Settings

*WLAN Overview*




### WPA2-Personal Overview (PSK)

See below for WPA2-Personal settings:



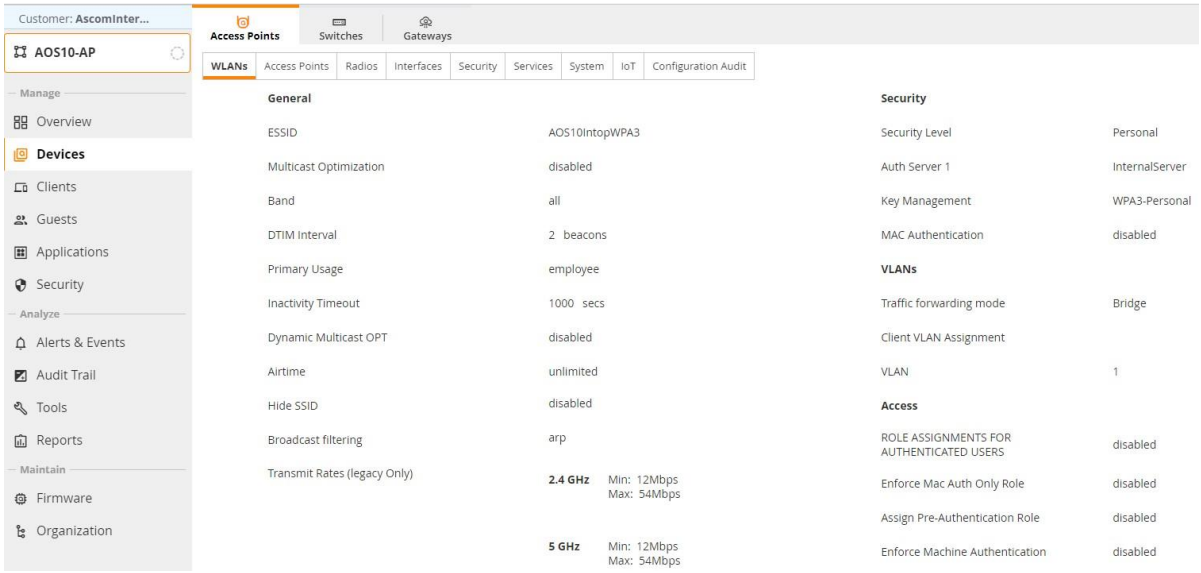

Ascom recommends a DTIM interval of at least 2 but not higher than 5. A higher value will offer slightly better standby times.

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:



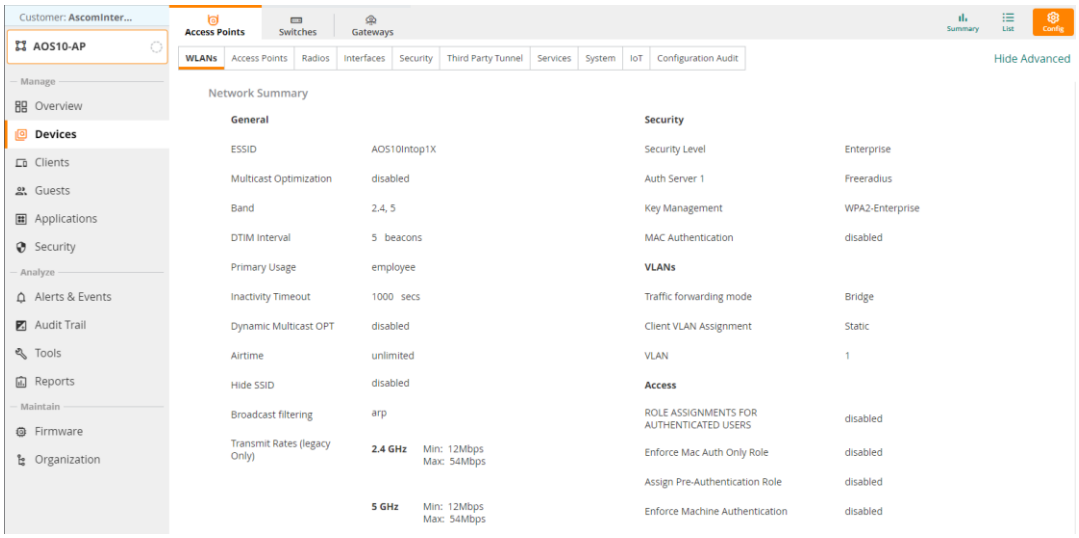

Ascom recommends a DTIM interval of at least 2 but not higher than 5. A higher value will offer slightly better standby times.

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

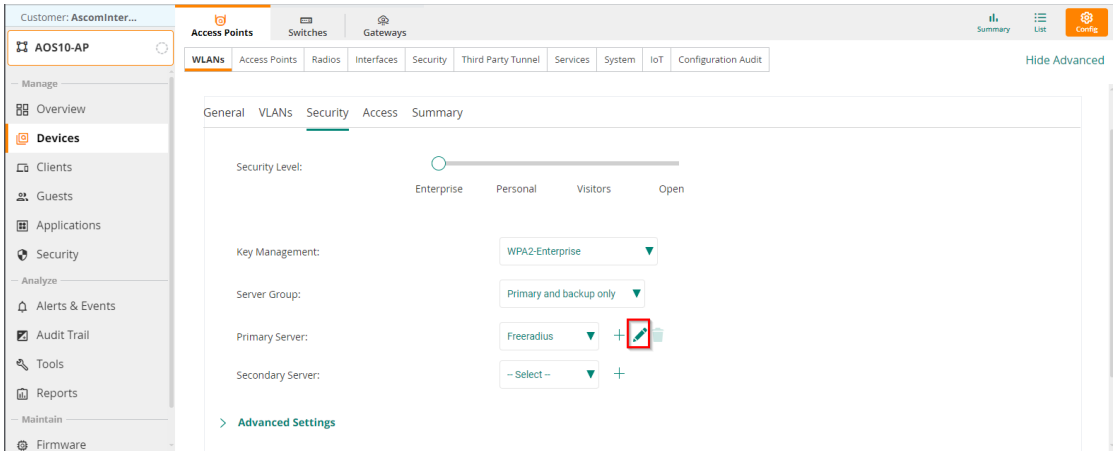
**Note: Not all HPE Aruba Networking Access point models support a DTIM period higher than 1.**

### WAP2-Enterprise Overview (802.1X Authentication)

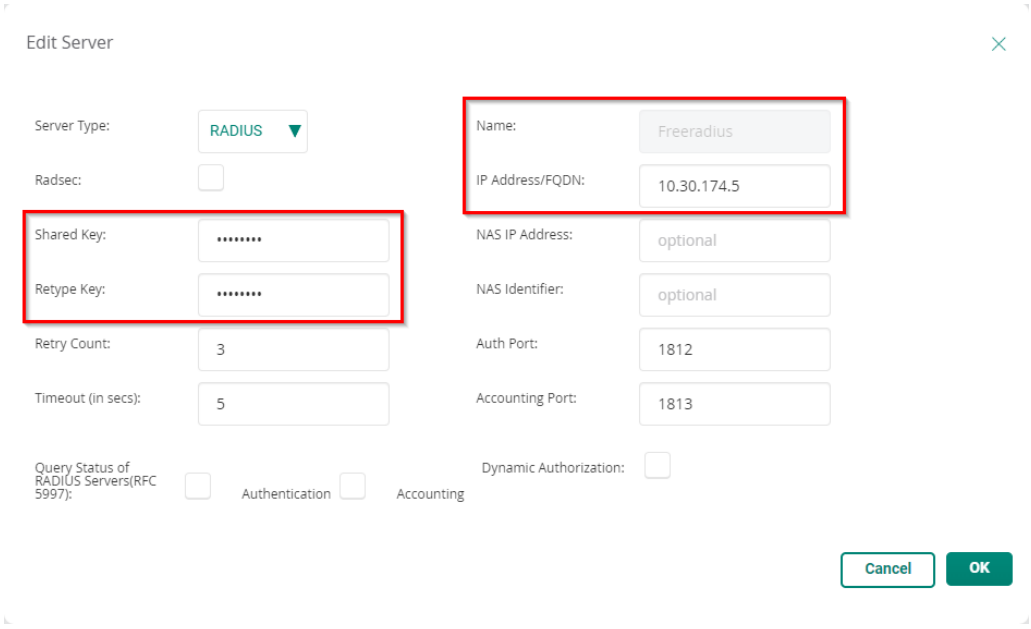
See below for WPA2-Enterprise settings:




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

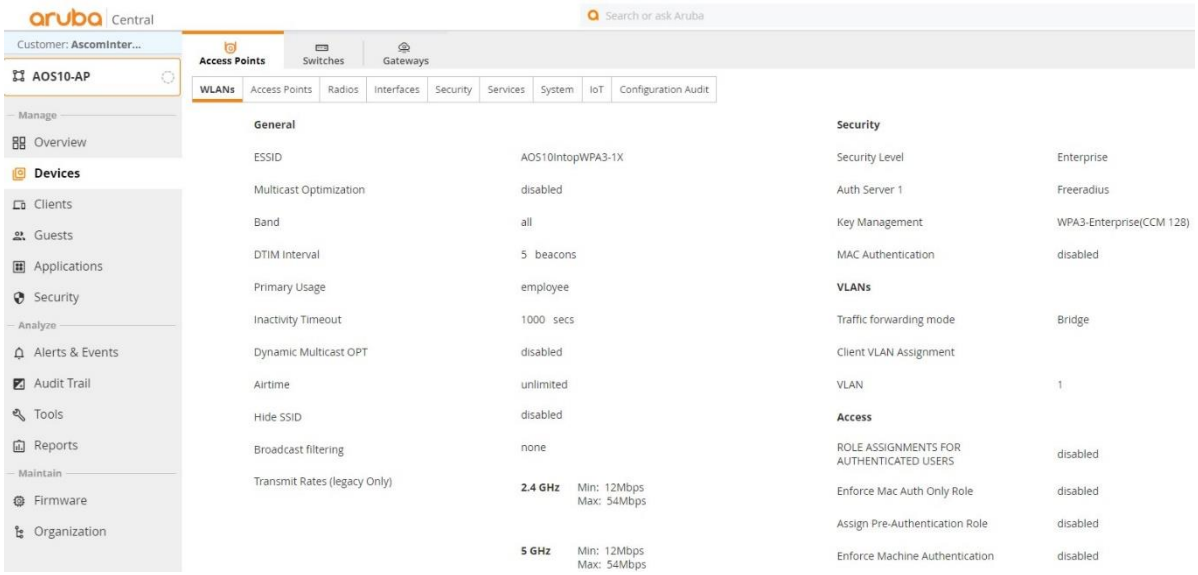



When configuring the authentication server, the IP address and Shared Key must correspond to the IP address and credentials used by the Radius server.

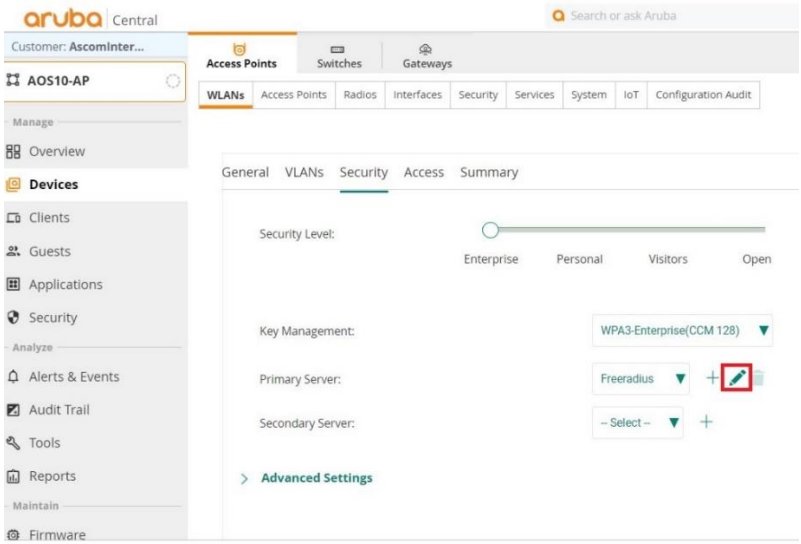


## WPA3-Enterprise Overview (802.1X Authentication)

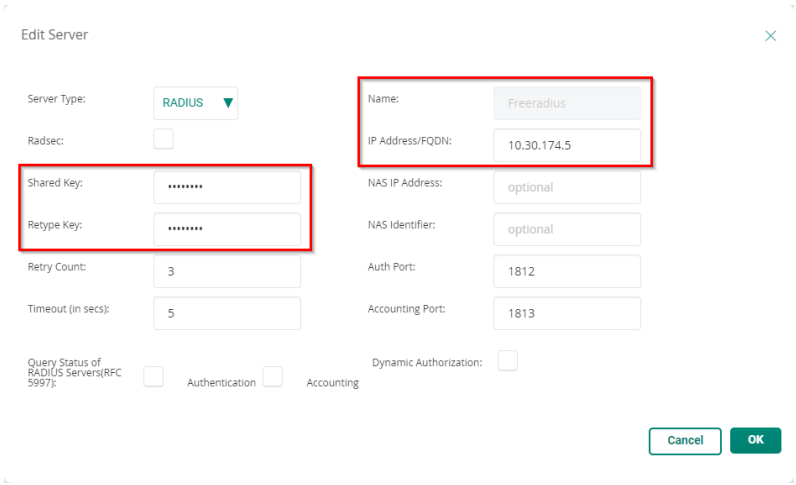
See below for WPA3-Enterprise settings:




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

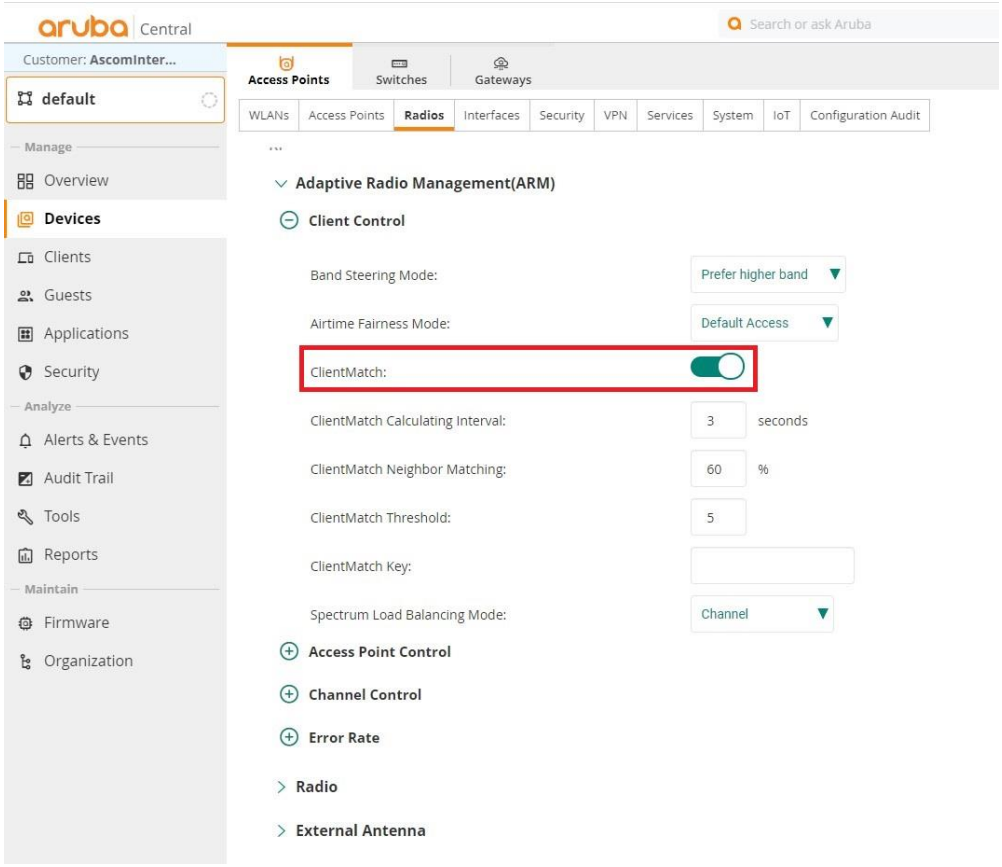



When configuring the authentication server, the IP address and Shared Key must correspond to the IP address and credentials used by the Radius server.

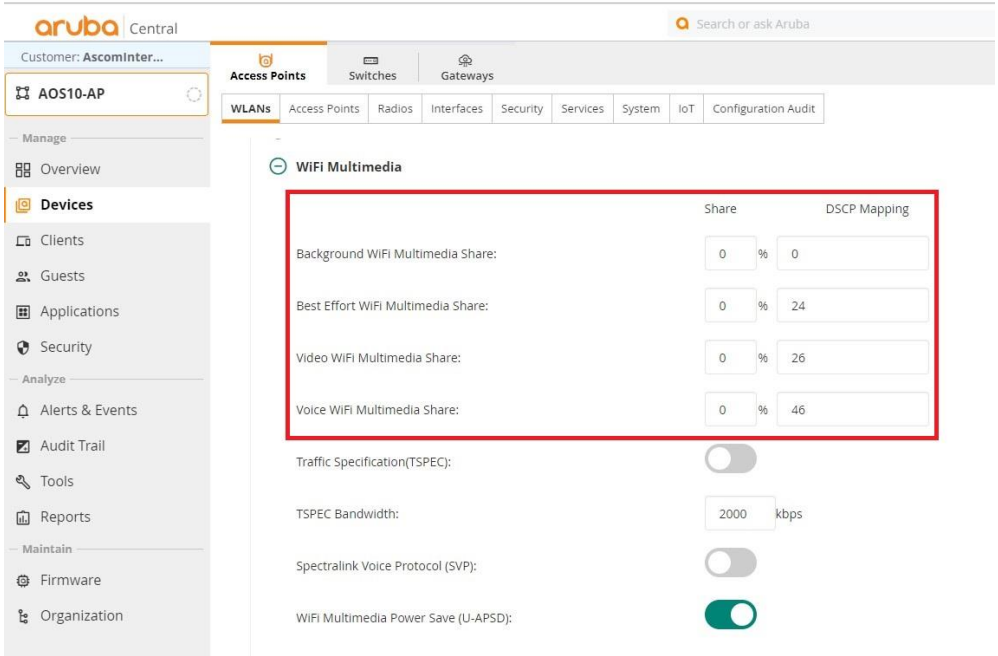


### General settings (Radio, WMM and QoS)

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

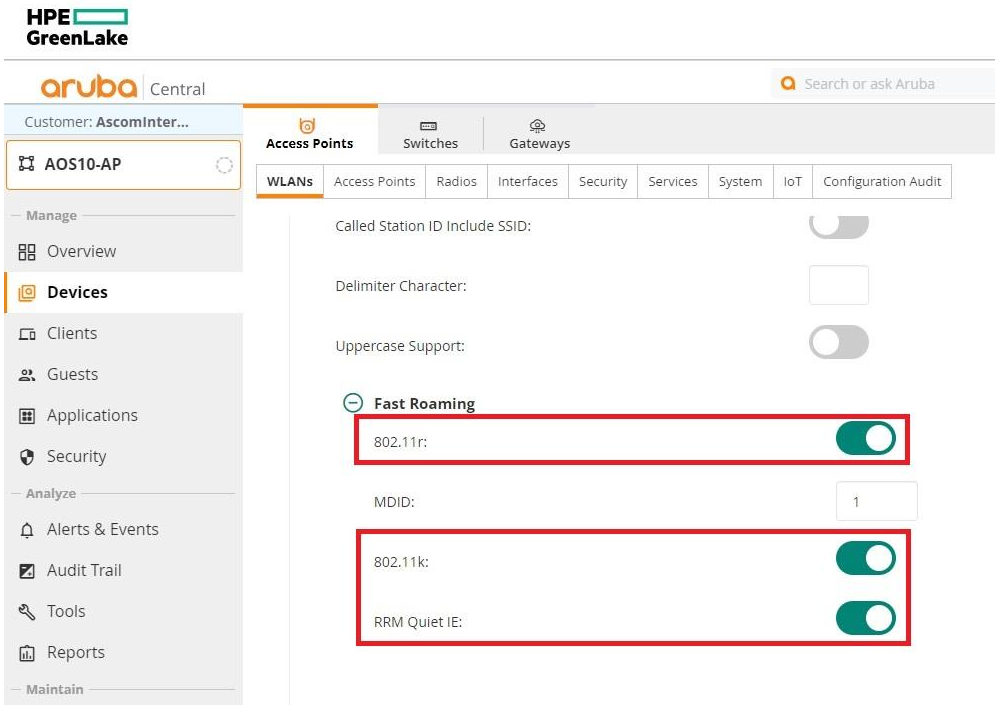



Refer to the WMM multimedia settings below:




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:




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 "RMM Quiet IE".**

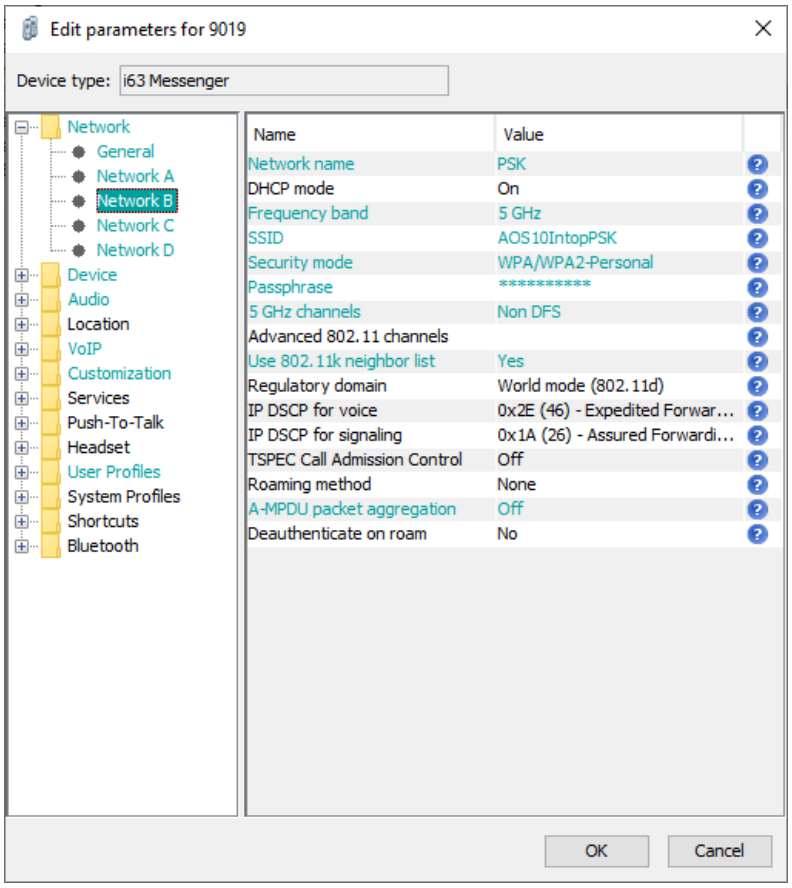
The Ascom i62 and Myco 1 & 2 do not support 11k and 11v, but normally operate without issues on an SSID where these settings are enabled (assuming i62 version 6.0.0 or later).

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**

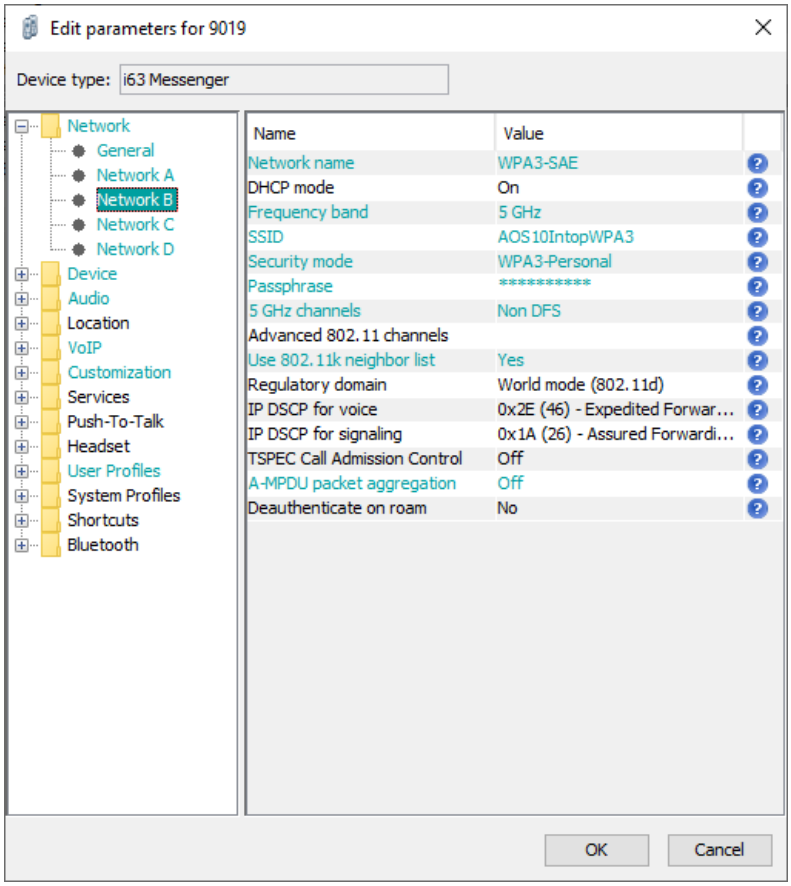
### WPA2-Personal (PSK) Network Settings




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

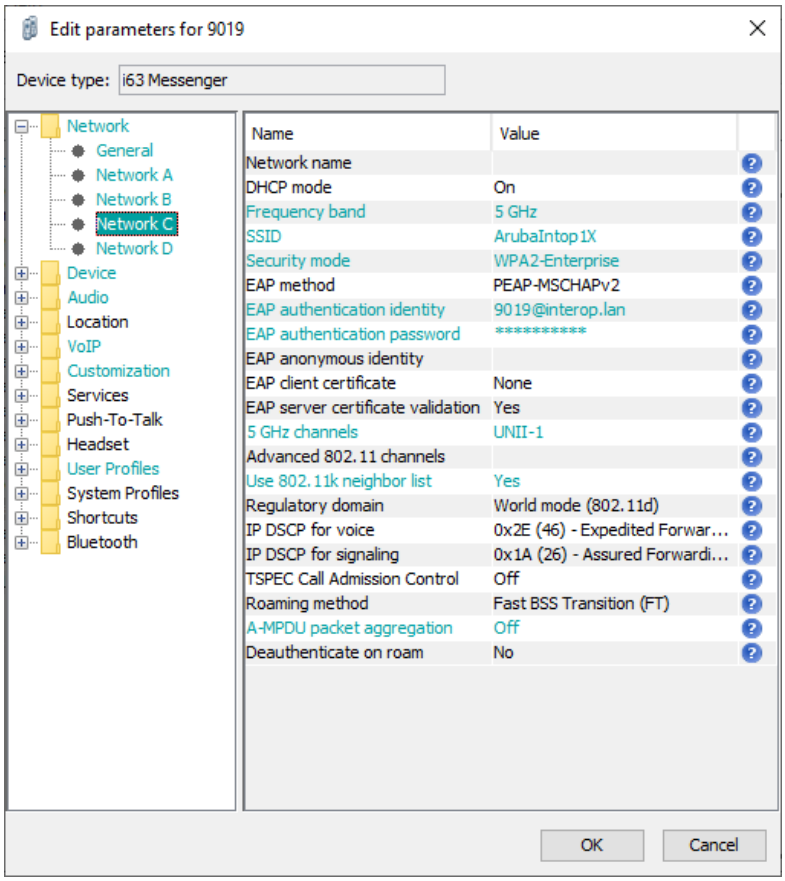



Network settings for WPA3-SAE

- 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”.

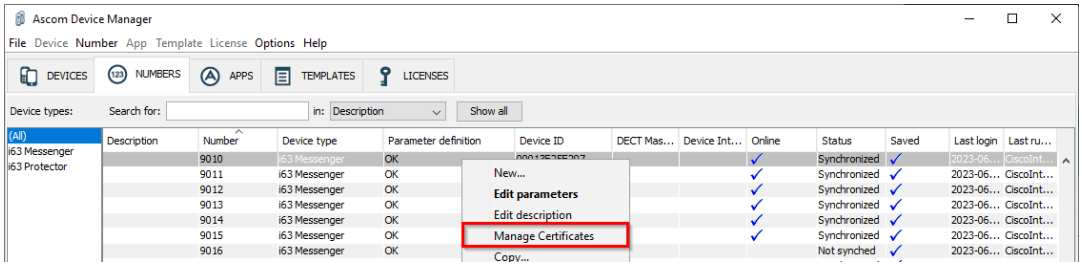
### WPA2-Enterprise (PEAP-MSCHAPv2) Network Settings




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

- Select frequency band according to system setup (here 5GHz)
- Select Security mode WPA2-Entreprise
- 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

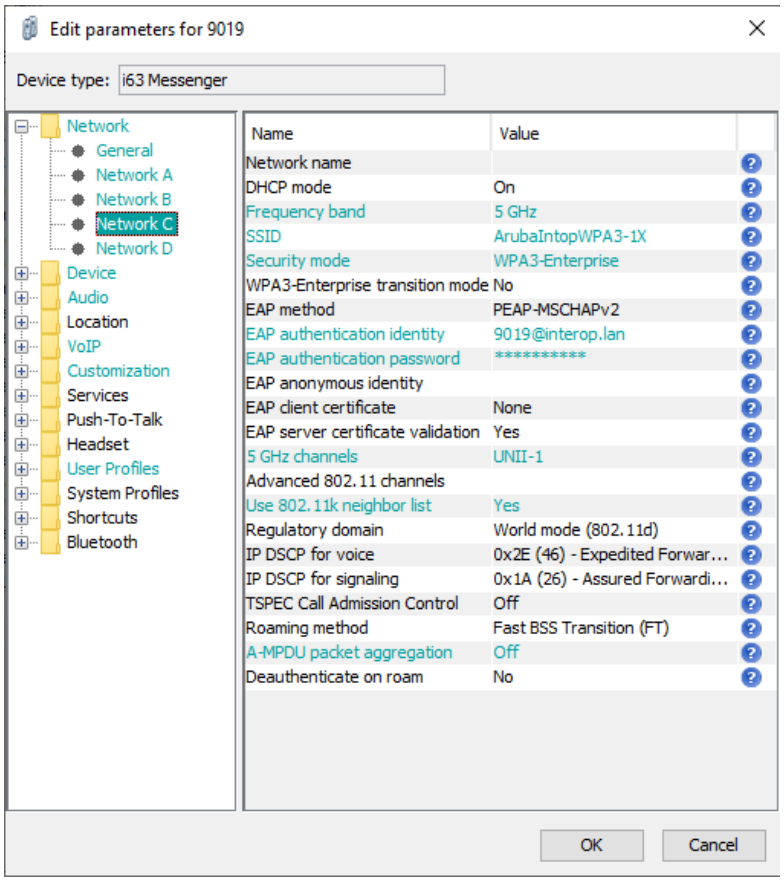
- Note: The FCC does not allow 802.11d to determine the regulatory domain. Consequently, devices deployed in the USA must have the “Regulatory Domain” set to “FCC”.




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

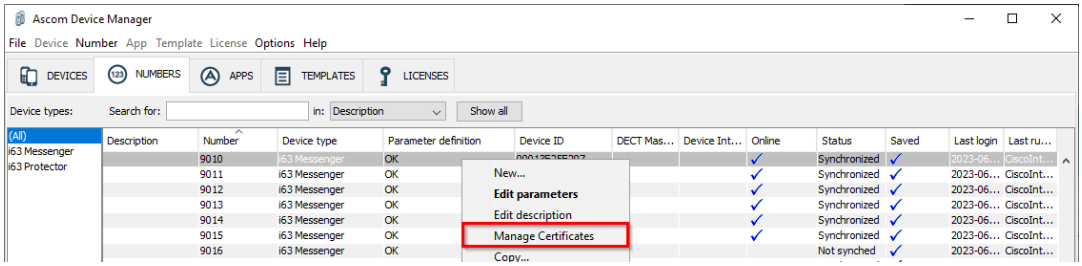
Note that both a CA and a client certificate are needed for TLS.

### 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-Entreprise
- 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 |
| **Total** | 26 |

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. |
| | | | |
| | | | |
| | | | |