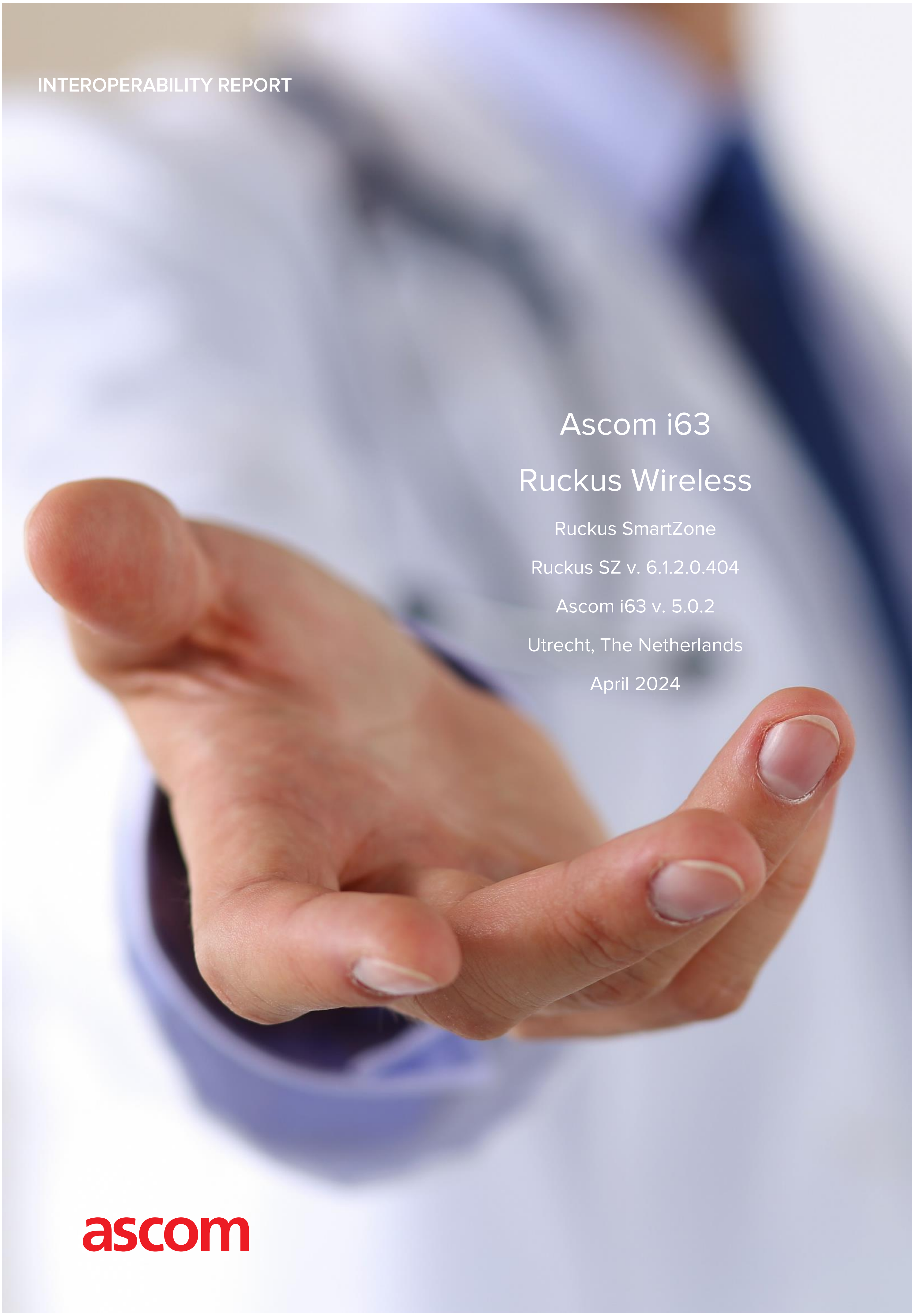
INTEROPERABILITY REPORT



# Ascom i63

# Ruckus Wireless

Ruckus SmartZone

Ruckus SZ v. 6.1.2.0.404

Ascom i63 v. 5.0.2

Utrecht, The Netherlands

April 2024

# Contents

# Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Ruckus Wireless platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Ruckus Wireless 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, 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 Ruckus Networks

Ruckus Networks is redefining connectivity around the globe. With our partners, we build secure wired and wireless access networks for organizations that place a premium on connectivity experiences for end users as well as simplicity. Follow Ruckus on Twitter, Facebook, LinkedIn, Instagram, YouTube and subscribe to our blog.

### About CommScope & Ruckus

CommScope (NASDAQ: COMM) and the recently acquired ARRIS and Ruckus Networks are redefining tomorrow by shaping the future of wired and wireless communications. Our combined global team of employees, innovators and technologists have empowered customers in all regions of the world to anticipate what's next and push the boundaries of what's possible. Discover more at www.commscope.com.Site Information

# Site Information

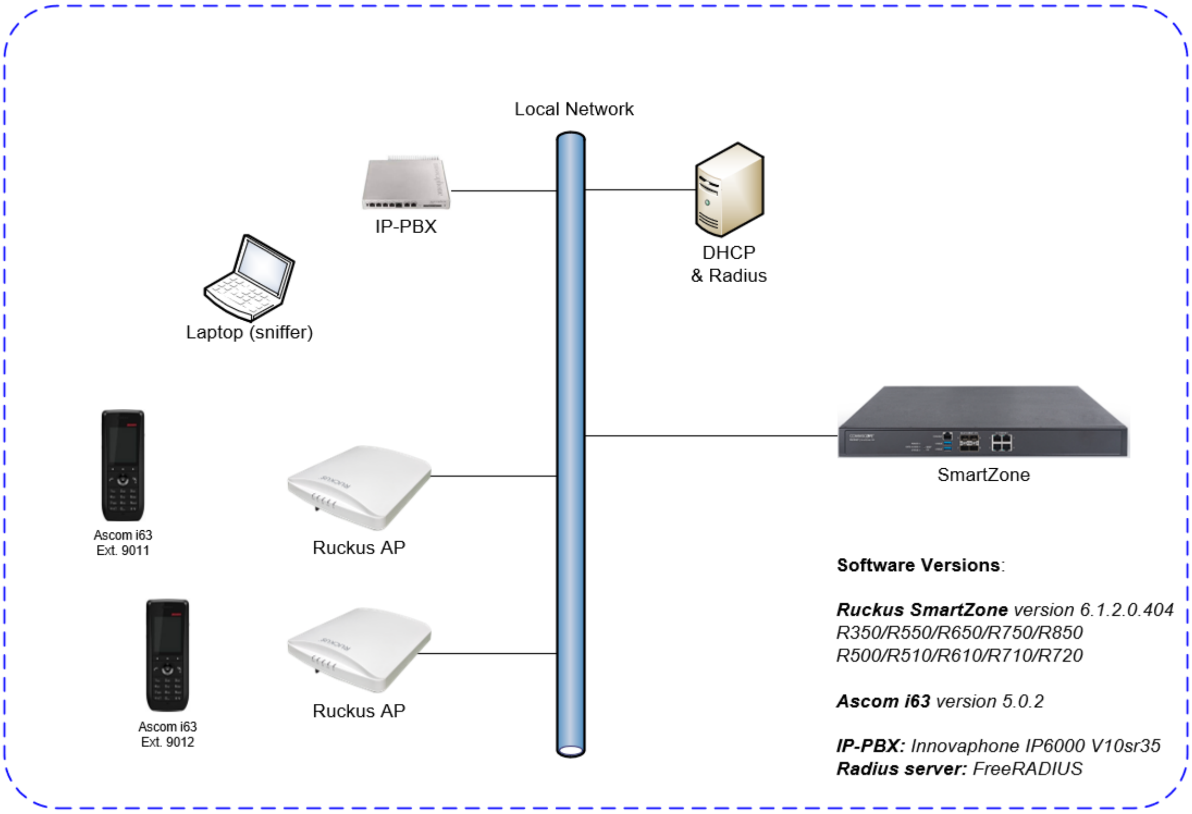
### Verification site

Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

### Participants

Remco van den Pangaart, Ascom

Verification topology



**Software Versions**:

***Ruckus SmartZone*** *version 6.1.2.0.404*
*R350/R550/R650/R750/R850*
*R500/R510/R610/R710/R720*

***Ascom i63*** *version 5.0.2*

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

# Summary

## General conclusions

This Ascom interoperability validation produced good results with regards 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 recommended.

## Compatibility information

All test were performed using a Virtual SmartZone E. We ensure compatibility/interoperability with all the access points and controllers listed below given that they run the software tested.

**Supported Partner Access Points with Ruckus Wireless version SmartZone 6.1.2.0.404:**

R350, R350e, T350, R550, R650, R750, T750, R850

R500, R510, R610, R710, R720

### Supported controller platforms with Ruckus Wireless version SmartZone 6.1.2.0.404:

Virtual SmartZone H (vSZ-H)

Virtual SmartZone E (vSZ-E)

Virtual SmartZone D (vSZ-D)

SmartZone 144 & 300

## Verification overview

### WLAN Compatibility and Performance

| High Level Functionality | Result | Comments |
|---|---|---|
| Association, Open with No Encryption | OK | |
| Association, WPA2-PSK / AES Encryption | OK | |
| Association, WPA2-PSK, AES Encryption, 802.11r/FT | OK | |
| Association, PEAP-MSCHAPv2 Auth, AES Encryption | OK | |
| Association, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT | OK | |
| Association with EAP-TLS authentication | OK | |
| Association, Multiple ESSIDs | OK | |
| Association with Protected Management Frames 802.11w | OK | |
| Beacon Interval and DTIM Period | OK | |
| PMKSA Caching | 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 | Avg. typical roaming time 60-65 ms |
| Roaming, WPA2-PSK, AES Encryption, 802.11r/FT | OK | Avg. typical roaming time 25-30 ms |
| Roaming, PEAP-MSCHAPv2 Auth, AES Encryption | OK * | Avg. typical roaming time 75-80 ms |
| Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT | OK | Avg. typical roaming time 25-35 ms |
| Channel usage controlled by 802.11k | OK | |

Average roaming times are measured 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**.

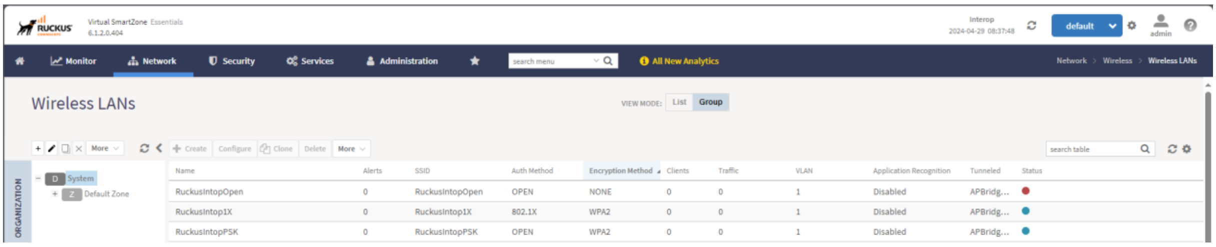
For detailed verification results, refer to Appendix B: Detailed Verification Records.

# Appendix A: Verification Configurations

## Ruckus Wireless SmartZone version 6.1.2.0.404

In the following chapter you will find screenshots and explanations of basic settings to get a Ruckus Smartzone WLAN system to operate with an Ascom i63. Please note that security settings were modified according to requirements in individual test cases.

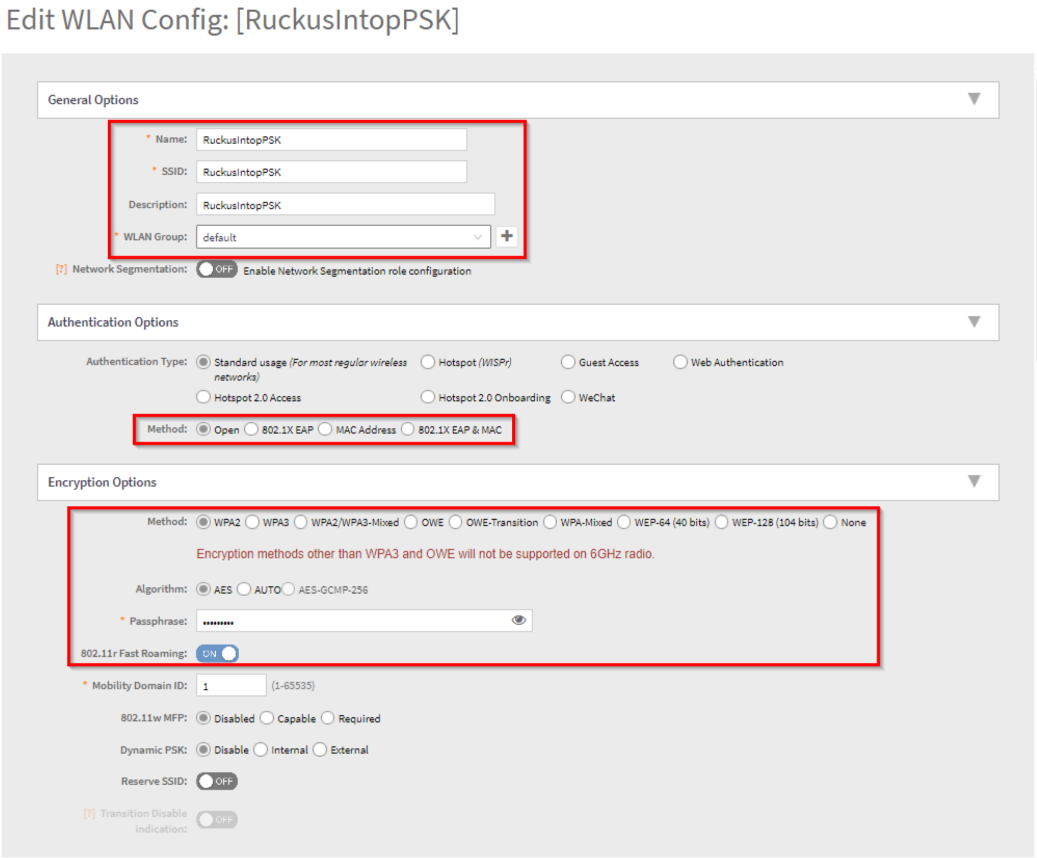
Wireless LAN overview



Wireless LANs

| Name | Alerts | SSID | Auth Method | Encryption Method | Clients | Traffic | VLAN | Application Recognition | Tunneled | Status |
|---|---|---|---|---|---|---|---|---|---|---|
| RuckusIntopOpen | 0 | RuckusIntopOpen | OPEN | NONE | 0 | 0 | 1 | Disabled | APBridg... | ● |
| RuckusIntop1X | 0 | RuckusIntop1X | 802.1X | WPA2 | 0 | 0 | 1 | Disabled | APBridg... | ● |
| RuckusIntopPSK | 0 | RuckusIntopPSK | OPEN | WPA2 | 0 | 0 | 1 | Disabled | APBridg... | ● |

### Security settings (WPA2-PSK)



Edit WLAN Config: [RuckusIntopPSK]

General Options

* Name: RuckusIntopPSK

* SSID: RuckusIntopPSK

Description: RuckusIntopPSK

* WLAN Group: default

[?] Network Segmentation: OFF Enable Network Segmentation role configuration

Authentication Options

Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

Method: ● Open ○ 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

Encryption Options

Method: ● WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ OWE-Transition ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

Encryption methods other than WPA3 and OWE will not be supported on 6GHz radio.

Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

* Passphrase: •••••••••

802.11r Fast Roaming: ON

* Mobility Domain ID: 1 (1-65535)

802.11w MFP: ● Disabled ○ Capable ○ Required

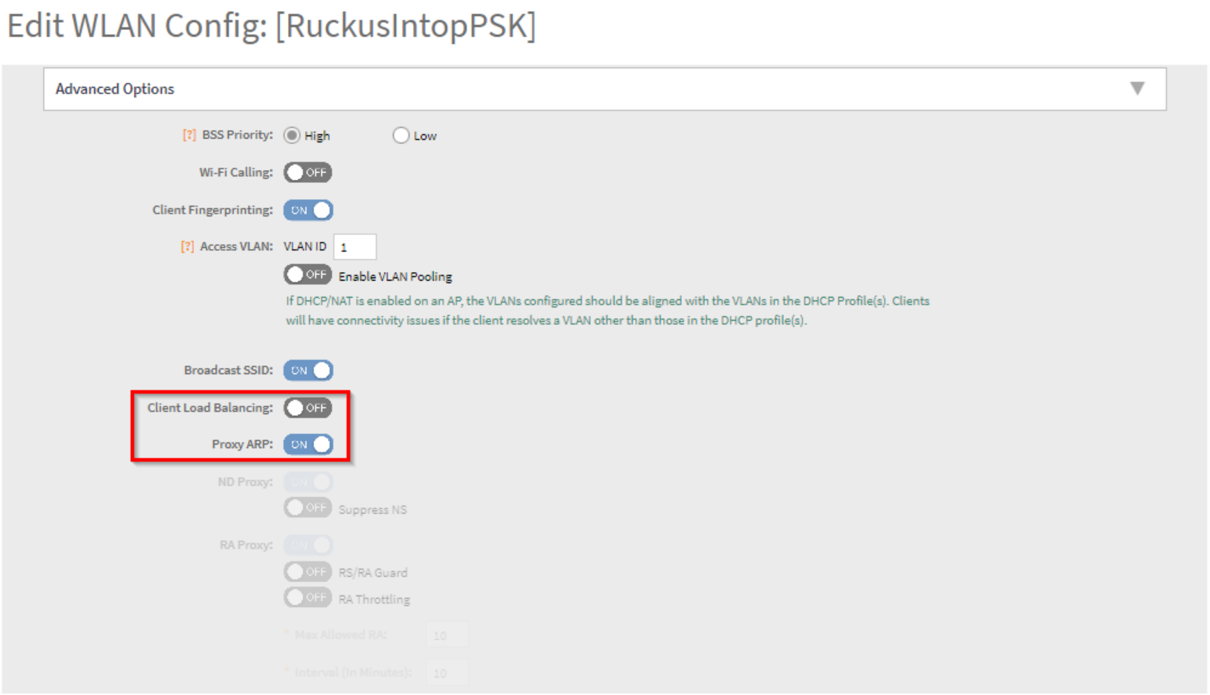
Dynamic PSK: ● Disable ○ Internal ○ External

Reserve SSID: OFF

[?] Transition Disable indication: OFF

Example of how to configure the system for PSK security (WPA2-AES)

- Select open Authentication
- Select WPA2 and AES
- It is recommended to use Fast Transition (802.11r) for enhanced roaming performance.



Edit WLAN Config: [RuckusIntopPSK]

Advanced Options ▼

[?] BSS Priority: ● High ○ Low

Wi-Fi Calling: OFF

Client Fingerprinting: ON

[?] Access VLAN: VLAN ID 1

OFF Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP profile(s).

Broadcast SSID: ON

Client Load Balancing: OFF

Proxy ARP: ON

ND Proxy: ON

OFF Suppress NS

RA Proxy: ON

OFF RS/RA Guard

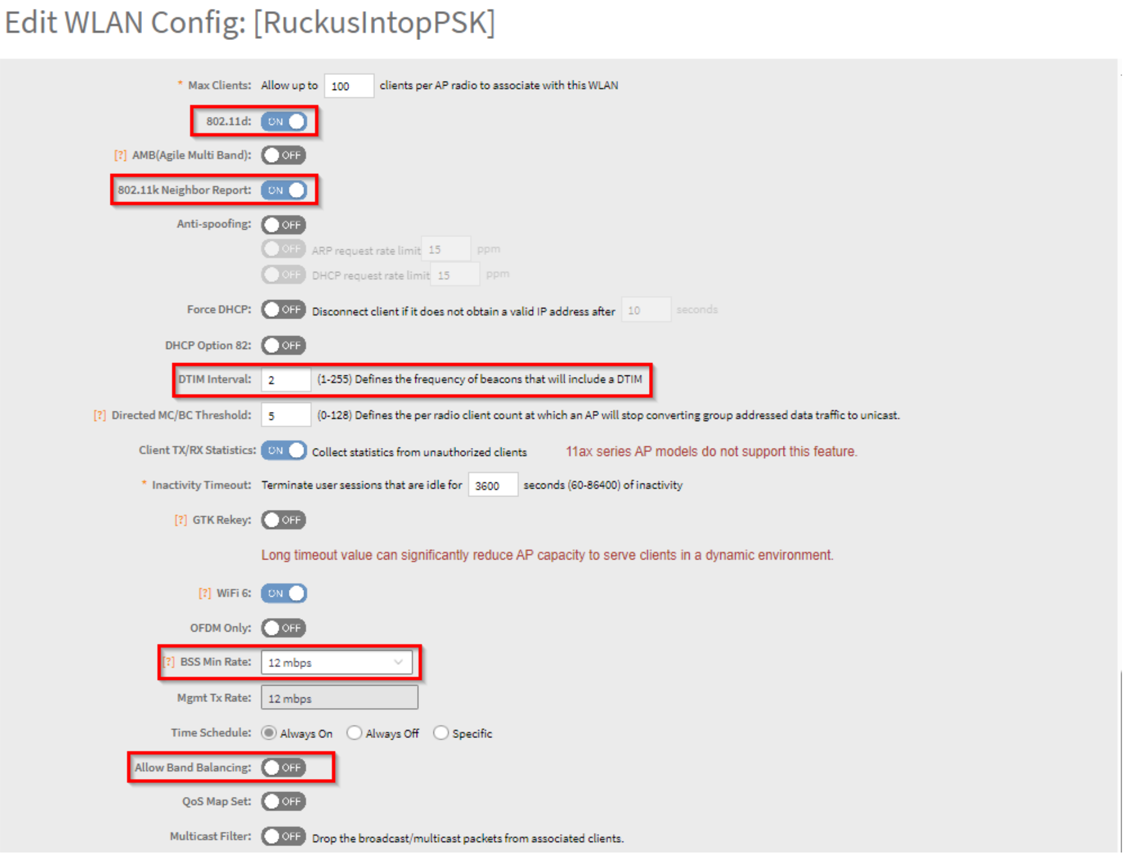
OFF RA Throttling

* Max Allowed RA: 10

* Interval (in Minutes): 10

Advanced WLAN configuration

- Make sure Client Load Balancing is disabled
- Enable Proxy ARP



Edit WLAN Config: [RuckusIntopPSK]

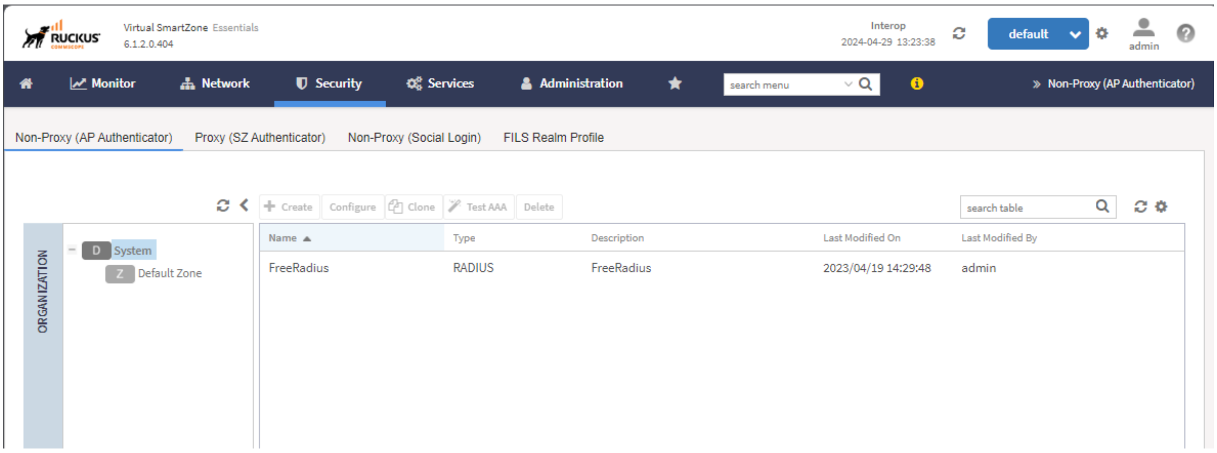
* Max Clients: Allow up to 100 clients per AP radio to associate with this WLAN
802.11d: ON
[?] AMB(Agile Multi Band): OFF
802.11k Neighbor Report: ON
Anti-spoofing: OFF
OFF ARP request rate limit 15 ppm
OFF DHCP request rate limit 15 ppm
Force DHCP: OFF Disconnect client if it does not obtain a valid IP address after 10 seconds
DHCP Option 82: OFF
DTIM Interval: 2 (1-255) Defines the frequency of beacons that will include a DTIM
[?] Directed MC/BC Threshold: 5 (0-128) Defines the per radio client count at which an AP will stop converting group addressed data traffic to unicast.
Client TX/RX Statistics: ON Collect statistics from unauthorized clients 11ax series AP models do not support this feature.
* Inactivity Timeout: Terminate user sessions that are idle for 3600 seconds (60-86400) of inactivity
[?] GTK Rekey: OFF
Long timeout value can significantly reduce AP capacity to serve clients in a dynamic environment.
[?] WiFi 6: ON
OFDM Only: OFF
[?] BSS Min Rate: 12 mbps
Mgmt Tx Rate: 12 mbps
Time Schedule: ● Always On ○ Always Off ○ Specific
Allow Band Balancing: OFF
QoS Map Set: OFF
Multicast Filter: OFF Drop the broadcast/multicast packets from associated clients.

Advanced WLAN configuration (Continued)

- Enable 802.11d
- Enable 802.11k Neighbor report.
  Note for i63 to use 802.11k neighbor list needs to be set to on handset side.
  See i63 configuration section below.
- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- Set BSS Min Rate to 12mbps
- Make sure Allow Band Balancing is disabled

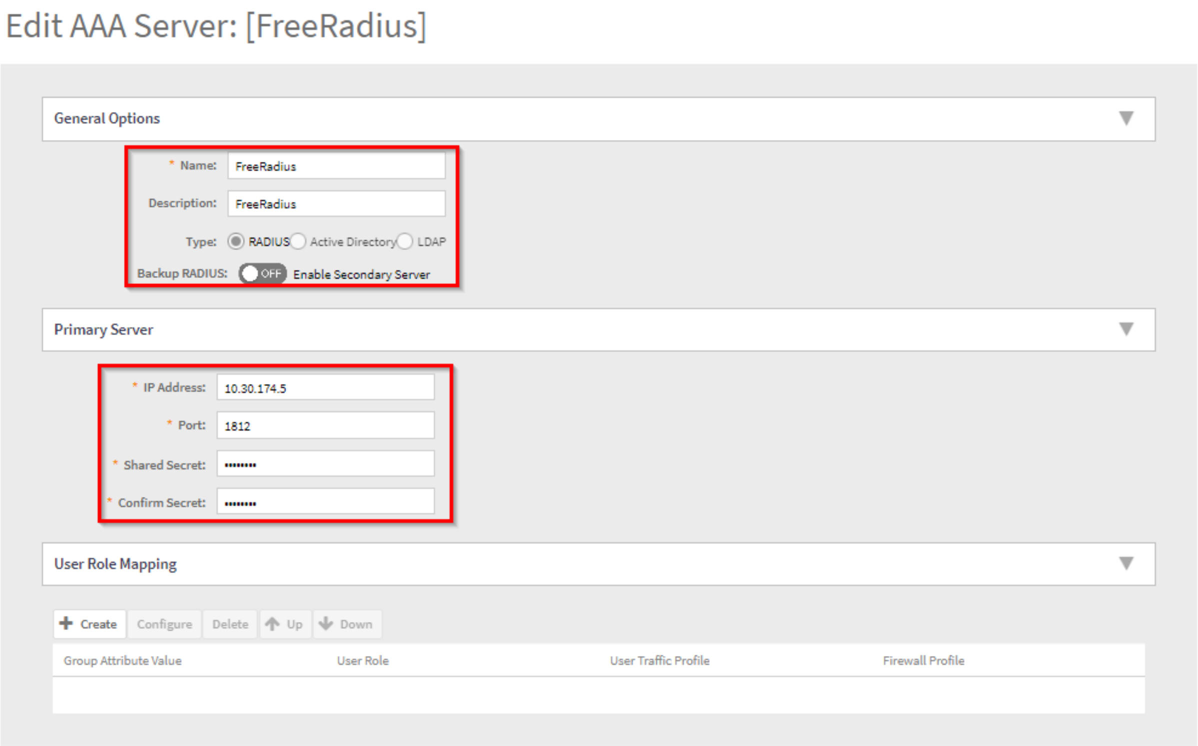
Note. Ascom i62 and Myco 1 & 2 do not support 11k but have no problem operating on an SSID were these settings are enabled. (Assuming i62 version 6.0.0 and later)

### Security settings (Radius configuration)



| Name | Type | Description | Last Modified On | Last Modified By |
|---|---|---|---|---|
| FreeRadius | RADIUS | FreeRadius | 2023/04/19 14:29:48 | admin |

RADIUS server configuration overview.


Edit AAA Server: [FreeRadius]

General Options

* Name: FreeRadius

Description: FreeRadius

Type: ● RADIUS ○ Active Directory ○ LDAP

Backup RADIUS: OFF Enable Secondary Server

Primary Server

* IP Address: 10.30.174.5

* Port: 1812

* Shared Secret: ••••••••

* Confirm Secret: ••••••••

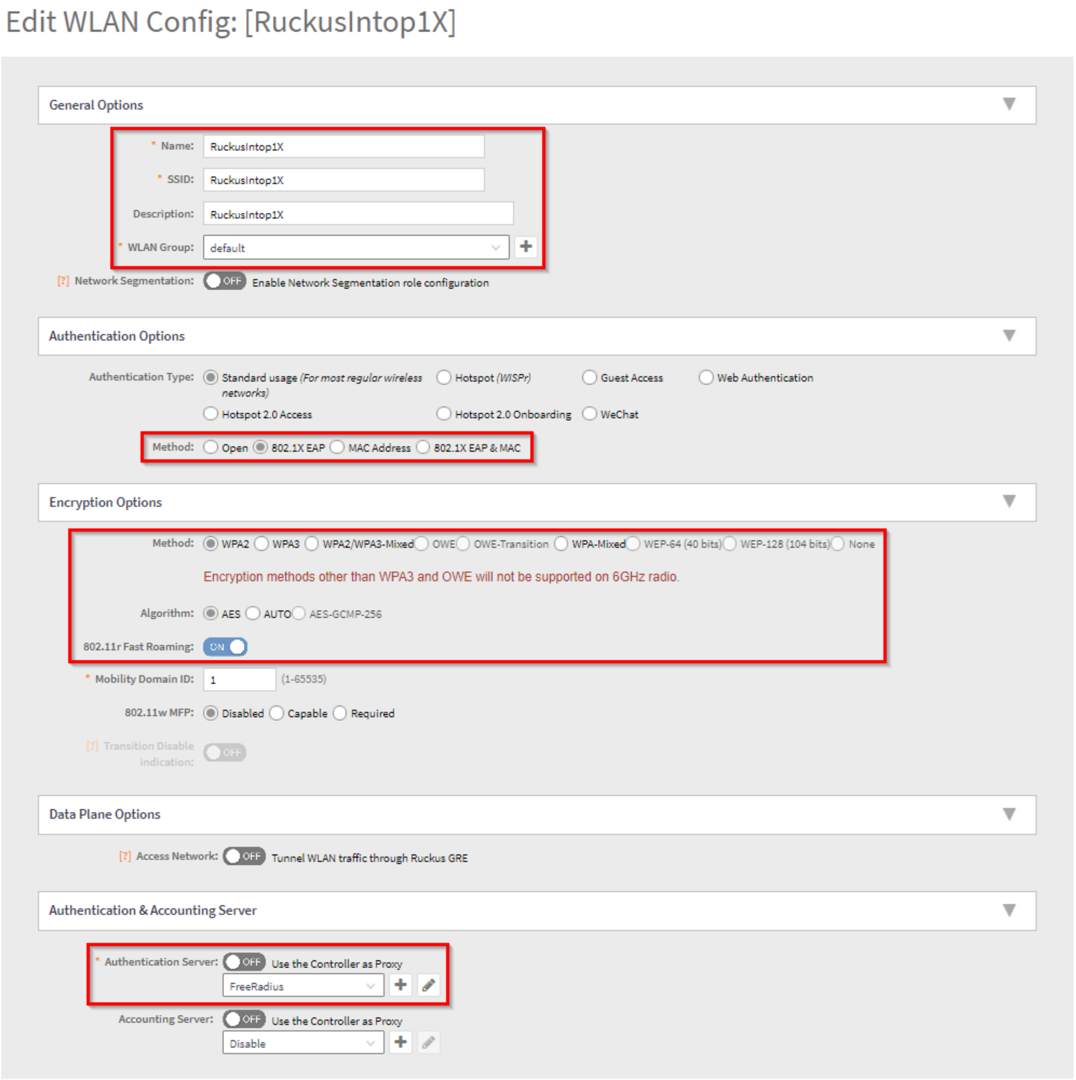
User Role Mapping

| Group Attribute Value | User Role | User Traffic Profile | Firewall Profile |
|---|---|---|---|

Example of how to configure the system for .1X authentication.

The IP Address and Shared Secret must correspond to the IP and the credential used by the Radius server.

### Security settings (WPA2-802.1X / PEAP-MSCHAPv2)



Edit WLAN Config: [RuckusIntop1X]

General Options

* Name: RuckusIntop1X

* SSID: RuckusIntop1X

Description: RuckusIntop1X

* WLAN Group: default

[?] Network Segmentation: OFF Enable Network Segmentation role configuration

Authentication Options

Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

Method: ○ Open ● 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

Encryption Options

Method: ● WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ OWE-Transition ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

Encryption methods other than WPA3 and OWE will not be supported on 6GHz radio.

Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

802.11r Fast Roaming: ON

* Mobility Domain ID: 1 (1-65535)

802.11w MFP: ● Disabled ○ Capable ○ Required

[?] Transition Disable indication: OFF

Data Plane Options

[?] Access Network: OFF Tunnel WLAN traffic through Ruckus GRE

Authentication & Accounting Server

* Authentication Server: OFF Use the Controller as Proxy

FreeRadius

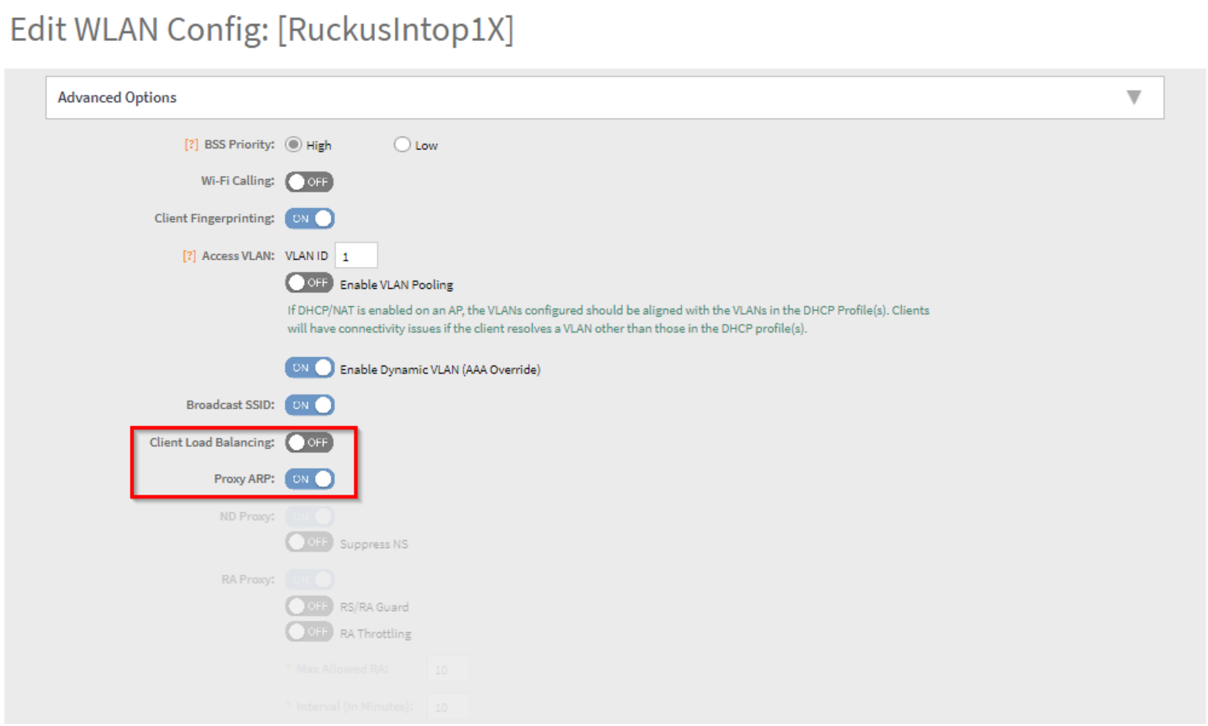
Accounting Server: OFF Use the Controller as Proxy

Disable

Configuration of ESS profile for utilization of 802.1X authentication.

- Select 802.1X EAP
- Select WPA2 and AES
- It is recommended to use Fast Transition (802.11r) for enhanced roaming performance.
- Authentication server “FreeRadius” corresponds to the server configured in previous step.

Note. 802.11r is not supported by Ascom i62 and Myco 1 & 2 but the devices have no problem operating on a SSIDs were 802.11r (FT) is advertised in conjunction with a legacy method.



Edit WLAN Config: [RuckusIntop1X]

Advanced Options

[?] BSS Priority: ● High ○ Low

Wi-Fi Calling: OFF

Client Fingerprinting: ON

[?] Access VLAN: VLAN ID 1

OFF Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP profile(s).

ON Enable Dynamic VLAN (AAA Override)

Broadcast SSID: ON

Client Load Balancing: OFF

Proxy ARP: ON

ND Proxy: ON

OFF Suppress NS

RA Proxy: ON

OFF RS/RA Guard

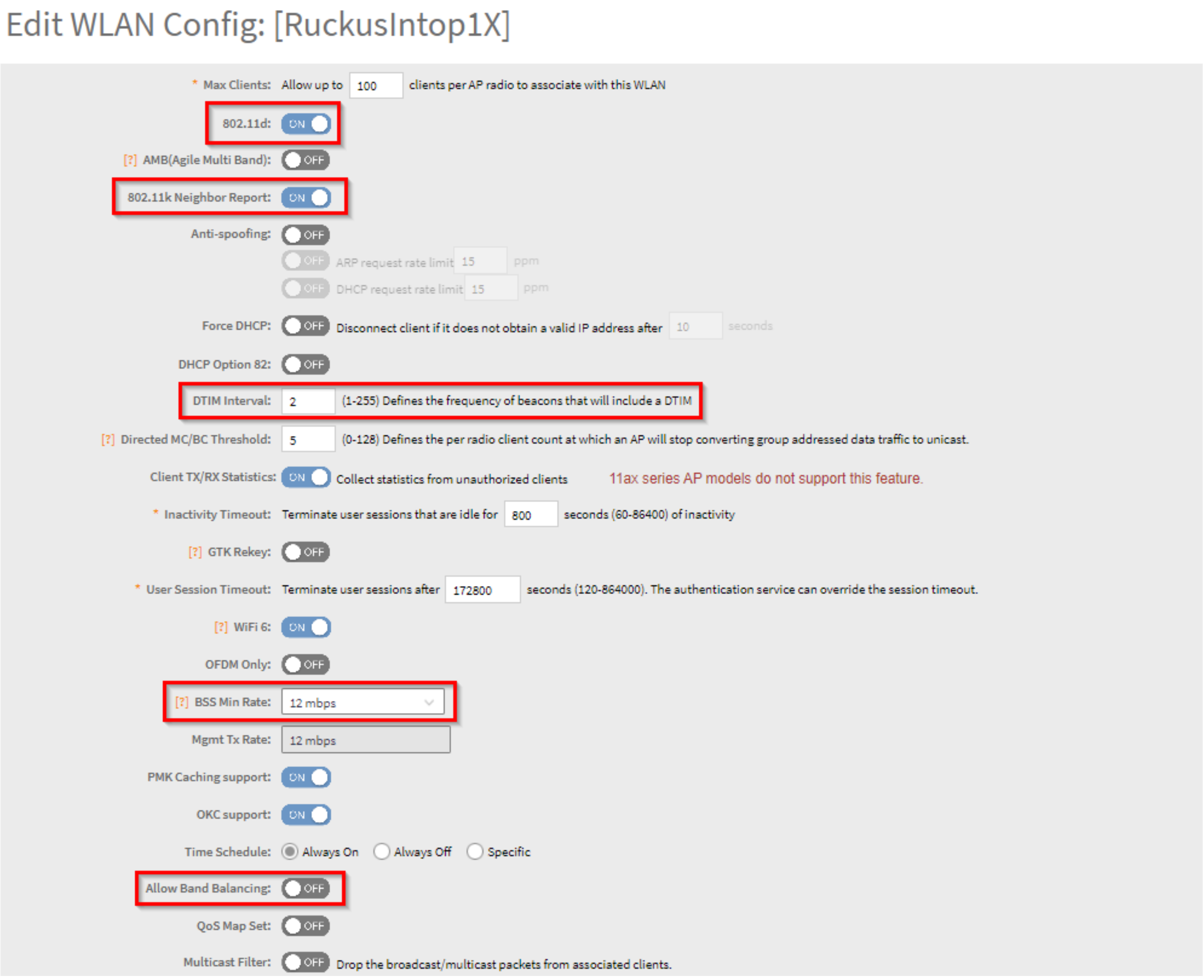
OFF RA Throttling

* Max Allowed RA: 10

* Interval (in Minutes): 10

Advanced WLAN configuration

- Make sure Client Load Balancing is disabled.
- Enable Proxy ARP.



Edit WLAN Config: [RuckusIntop1X]

* Max Clients: Allow up to 100 clients per AP radio to associate with this WLAN

802.11d: ON

[?] AMB(Agile Multi Band): OFF

802.11k Neighbor Report: ON

Anti-spoofing: OFF

OFF ARP request rate limit 15 ppm

OFF DHCP request rate limit 15 ppm

Force DHCP: OFF Disconnect client if it does not obtain a valid IP address after 10 seconds

DHCP Option 82: OFF

DTIM Interval: 2 (1-255) Defines the frequency of beacons that will include a DTIM

[?] Directed MC/BC Threshold: 5 (0-128) Defines the per radio client count at which an AP will stop converting group addressed data traffic to unicast.

Client TX/RX Statistics: ON Collect statistics from unauthorized clients 11ax series AP models do not support this feature.

* Inactivity Timeout: Terminate user sessions that are idle for 800 seconds (60-86400) of inactivity

[?] GTK Rekey: OFF

* User Session Timeout: Terminate user sessions after 172800 seconds (120-864000). The authentication service can override the session timeout.

[?] WiFi 6: ON

OFDM Only: OFF

[?] BSS Min Rate: 12 mbps

Mgmt Tx Rate: 12 mbps

PMK Caching support: ON

OKC support: ON

Time Schedule: ● Always On ○ Always Off ○ Specific

Allow Band Balancing: OFF

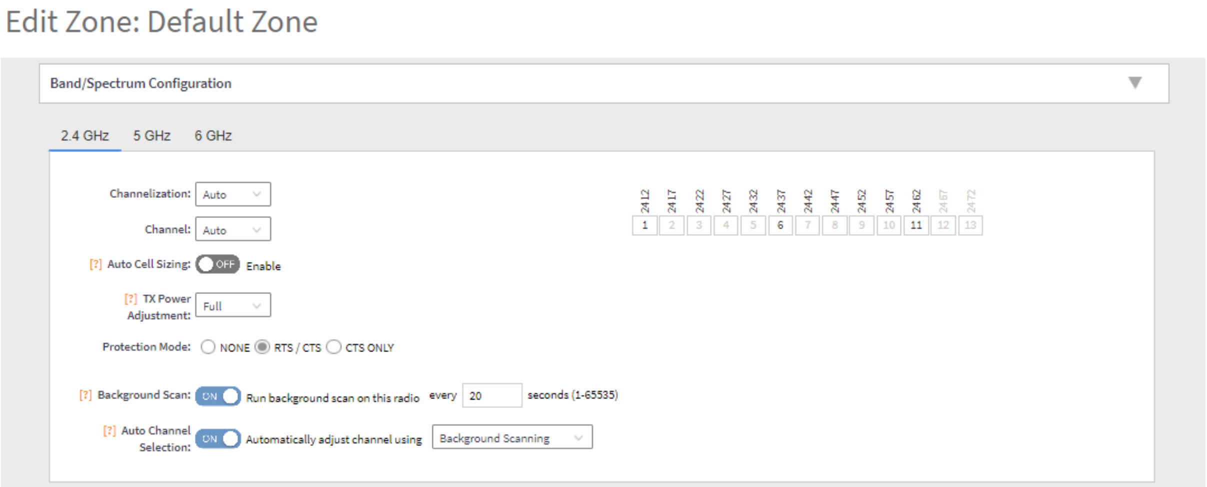
QoS Map Set: OFF

Multicast Filter: OFF Drop the broadcast/multicast packets from associated clients.

Advanced WLAN configuration (Continued)

- Enable 802.11d
- Enable 802.11k Neighbor report.
  Note for i63 to use 802.11k neighbor list needs to be set to on handset side.
  See i63 configuration section below.
- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- Set BSS Min Rate to 12mbps
- Make sure Allow Band Balancing is disabled

### General settings (QoS, Radio)



Edit Zone: Default Zone

Band/Spectrum Configuration

Channelization: Auto

Channel: Auto

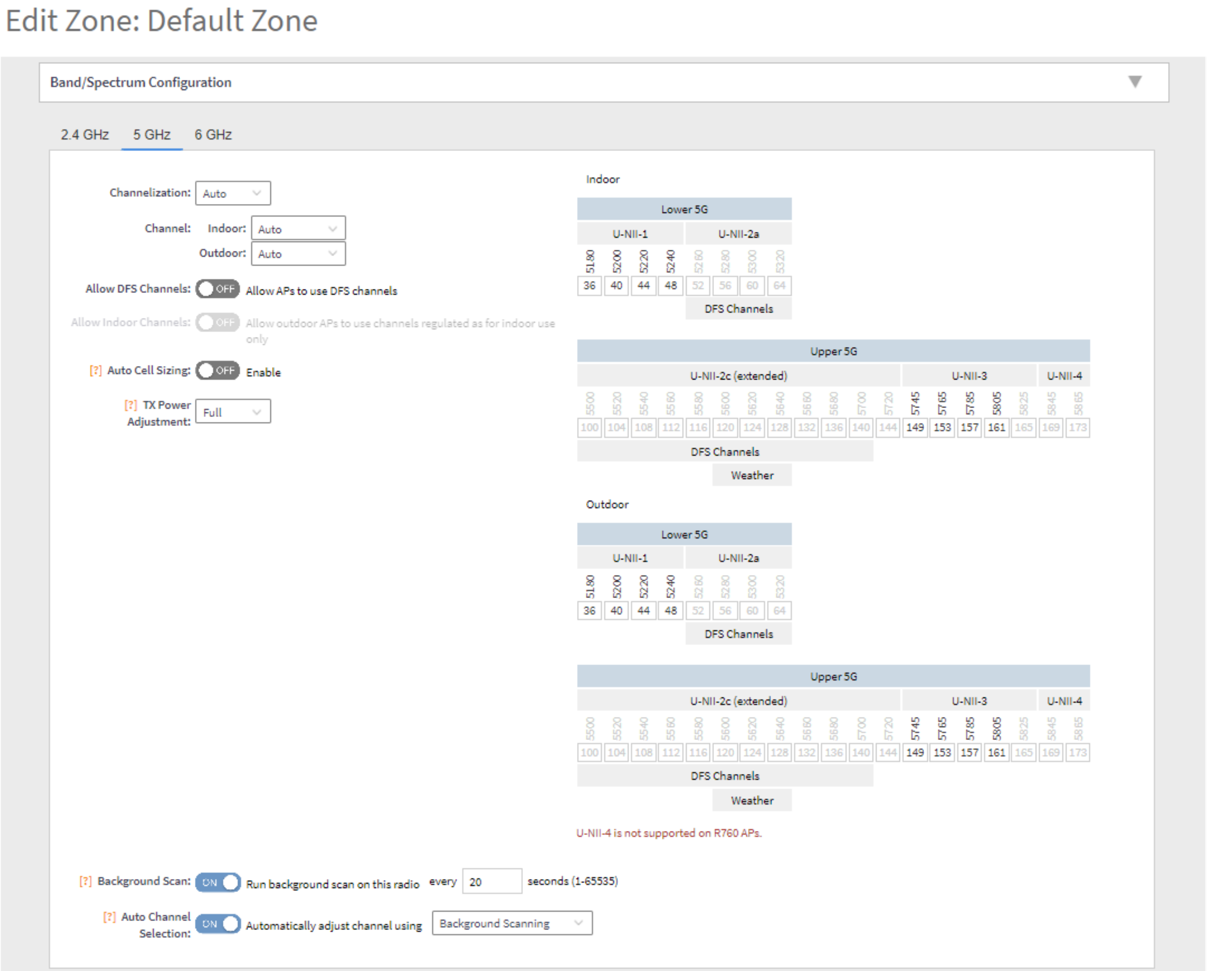
[?] Auto Cell Sizing: OFF Enable

[?] TX Power Adjustment: Full

Protection Mode: ○ NONE ● RTS / CTS ○ CTS ONLY

[?] Background Scan: ON Run background scan on this radio every 20 seconds (1-65535)

[?] Auto Channel Selection: ON Automatically adjust channel using Background Scanning



Edit Zone: Default Zone

Band/Spectrum Configuration

Channelization: Auto

Channel: Indoor: Auto

Outdoor: Auto

Allow DFS Channels: OFF Allow APs to use DFS channels

Allow Indoor Channels: OFF Allow outdoor APs to use channels regulated as for indoor use only

[?] Auto Cell Sizing: OFF Enable

[?] TX Power Adjustment: Full

U-NII-4 is not supported on R760 APs.

[?] Background Scan: ON Run background scan on this radio every 20 seconds (1-65535)

[?] Auto Channel Selection: ON Automatically adjust channel using Background Scanning

Access Points Common Settings per AP group.

Ascom recommended settings for 802.11b/g/n are to only use channel 1, 6 and 11. For 802.11a/n/ac use channels according to the infrastructure manufacturer and country regulations.

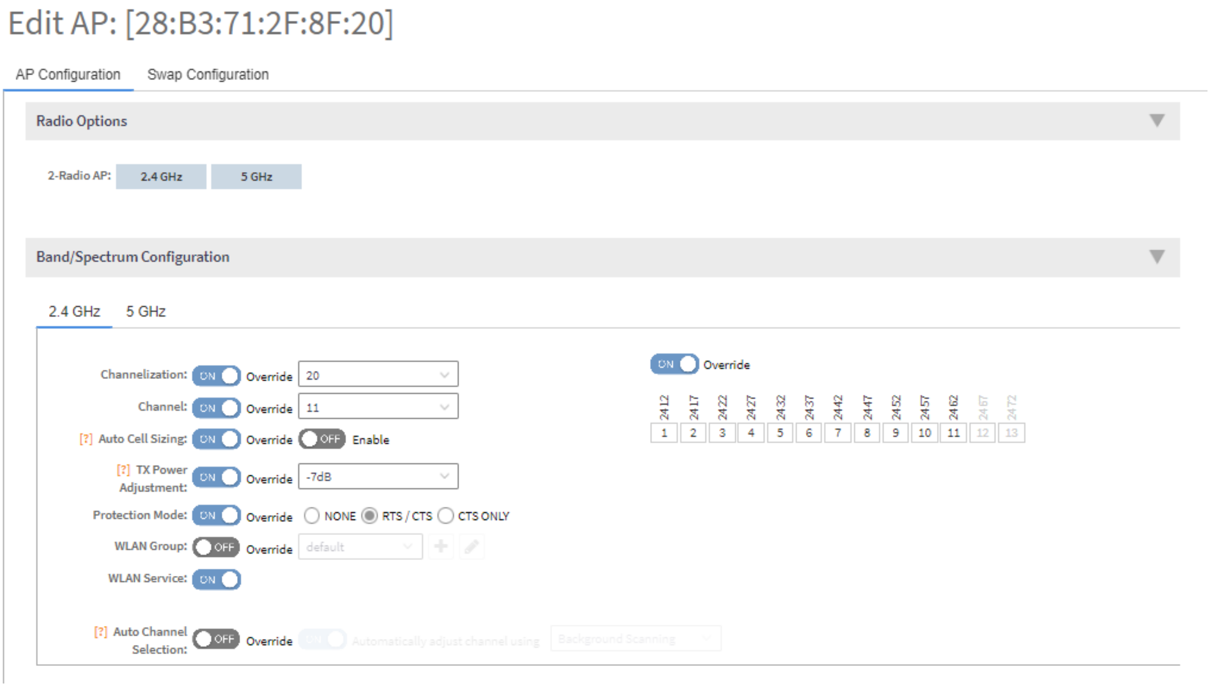
Note that Tx power level and channel was manually set for test purpose.

**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 this limit unless 802.11k is in use.**

2. **Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations 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 VoWIFI deployments.**



Edit AP: [28:B3:71:2F:8F:20]

AP Configuration | Swap Configuration

Radio Options

2-Radio AP: 2.4 GHz | 5 GHz

Band/Spectrum Configuration

2.4 GHz | 5 GHz

Channelization: ON Override 20

Channel: ON Override 11

[?] Auto Cell Sizing: ON Override OFF Enable

[?] TX Power Adjustment: ON Override -7dB

Protection Mode: ON Override ○ NONE ● RTS / CTS ○ CTS ONLY

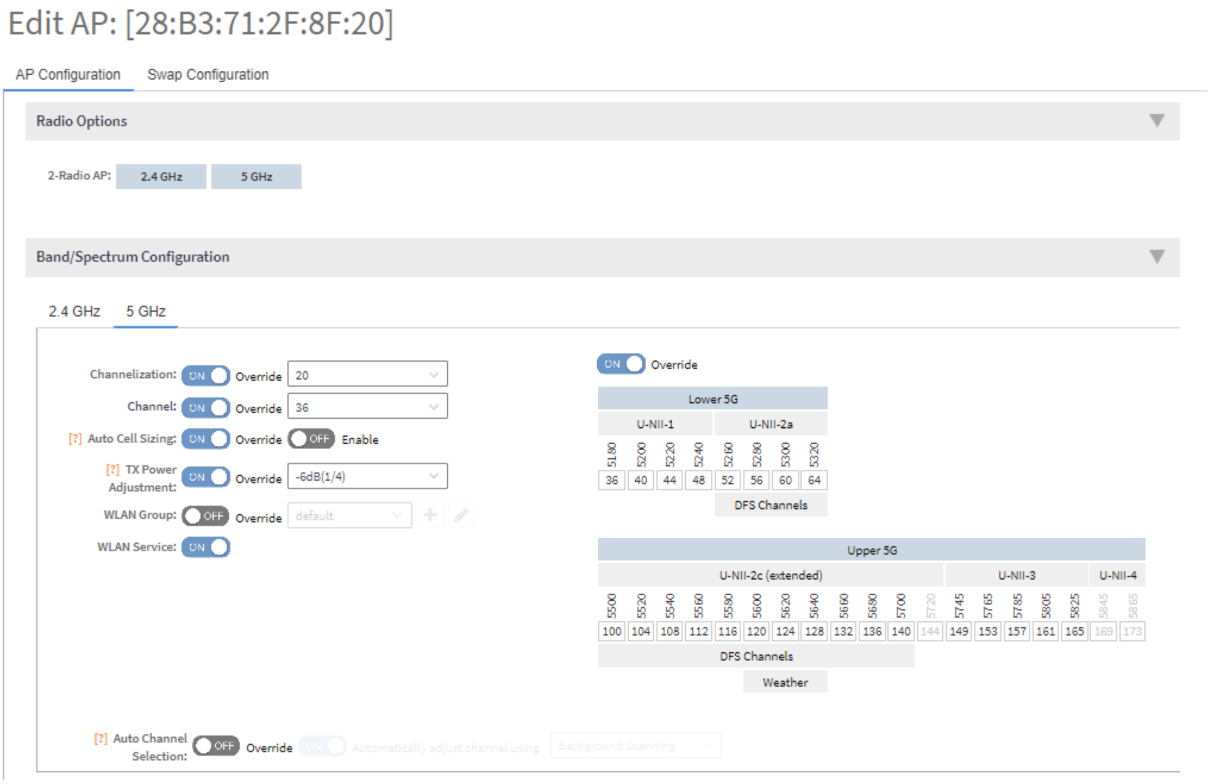
WLAN Group: OFF Override default

WLAN Service: ON

[?] Auto Channel Selection: OFF Override ON Automatically adjust channel using Background Scanning

ON Override

Individual AP configuration 2.4Ghz



Edit AP: [28:B3:71:2F:8F:20]

AP Configuration | Swap Configuration

Radio Options

2-Radio AP: 2.4 GHz | 5 GHz

Band/Spectrum Configuration

2.4 GHz | 5 GHz

Channelization: ON Override 20

Channel: ON Override 36

[?] Auto Cell Sizing: ON Override OFF Enable

[?] TX Power Adjustment: ON Override -6dB(1/4)

WLAN Group: OFF Override default

WLAN Service: ON

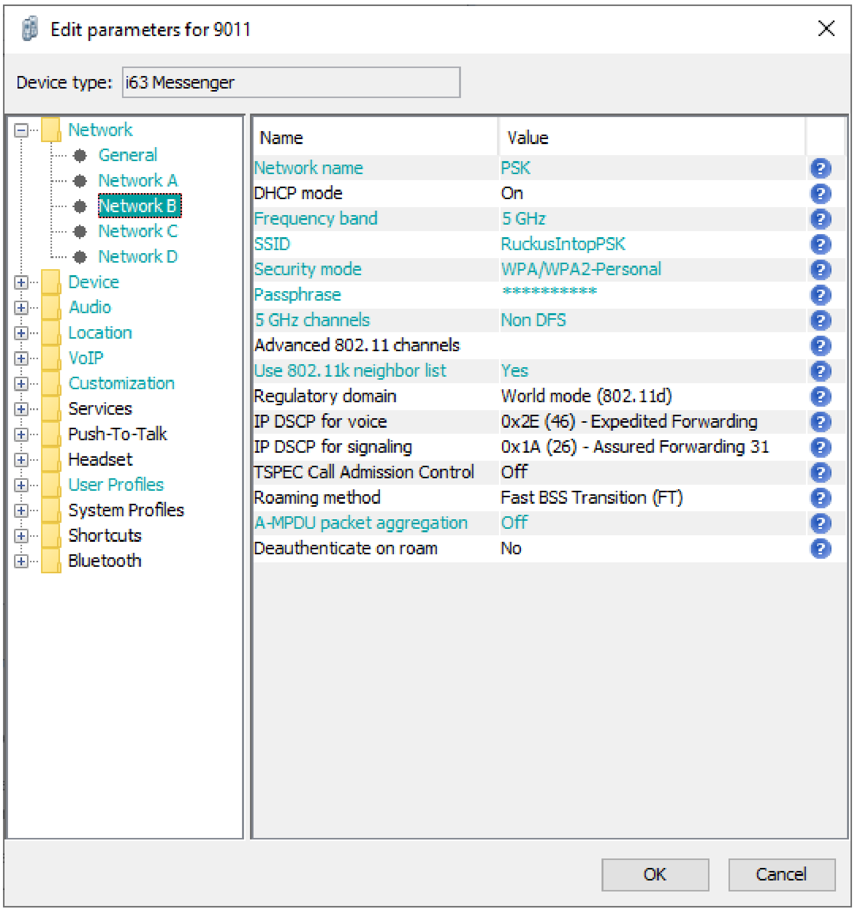
[?] Auto Channel Selection: OFF Override ON Automatically adjust channel using Background Scanning

ON Override

Individual AP configuration 5Ghz.

Channel and Tx power override was used to create suitable cell overlap for test purposes.

### Ascom i63

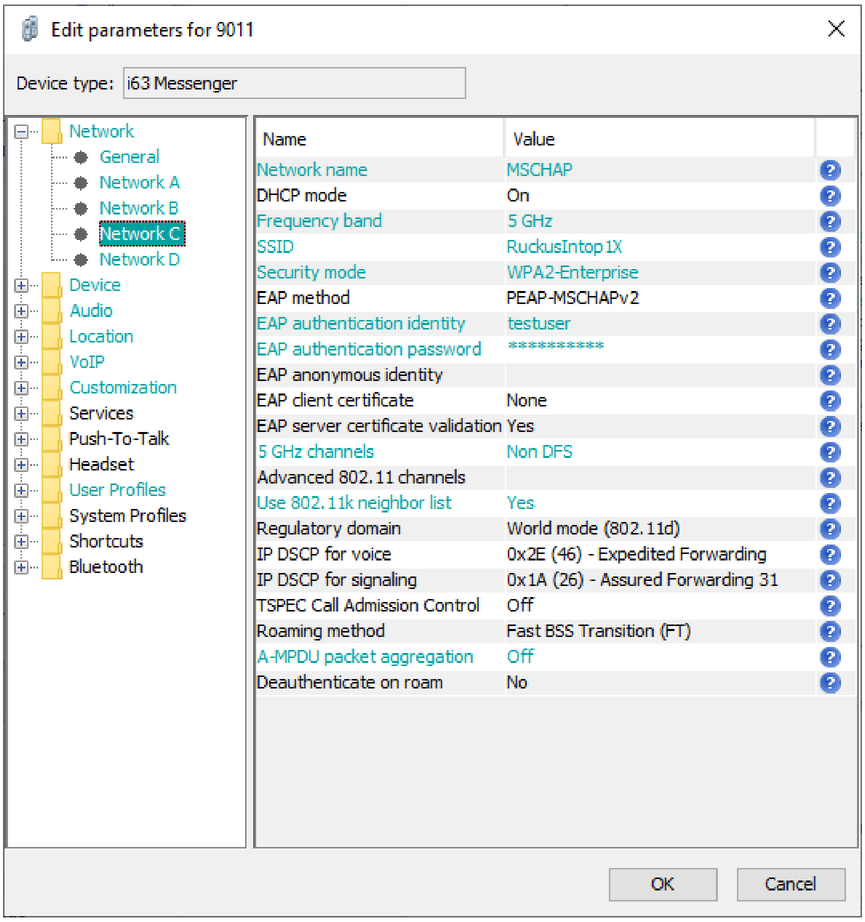


| Name | Value |
|---|---|
| Network name | PSK |
| DHCP mode | On |
| Frequency band | 5 GHz |
| SSID | RuckusIntopPSK |
| Security mode | WPA/WPA2-Personal |
| Passphrase | ********** |
| 5 GHz channels | Non DFS |
| Advanced 802.11 channels | |
| Use 802.11k neighbor list | Yes |
| Regulatory domain | 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-PSK

- Select frequency band according to system setup (here 5GHz)
- 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”.



Edit parameters for 9011

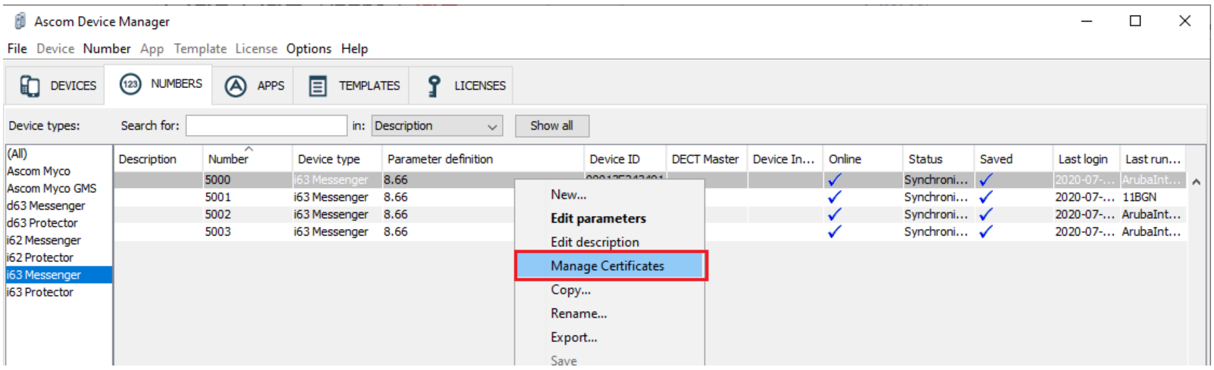
Device type: i63 Messenger

| Name | Value |
|---|---|
| Network name | MSCHAP |
| DHCP mode | On |
| Frequency band | 5 GHz |
| SSID | RuckusIntop1X |
| 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 | 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)
- 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”.



| Description | Number | Device type | Parameter definition | Device ID | DECT Master | Device In... | Online | Status | Saved | Last login | Last run... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 5000 | i63 Messenger | 8.66 | [illegible] | | | ✓ | Synchroni... | ✓ | 2020-07-... | ArubaInt... |
| | 5001 | i63 Messenger | 8.66 | | | | ✓ | Synchroni... | ✓ | 2020-07-... | 11BGN |
| | 5002 | i63 Messenger | 8.66 | | | | ✓ | Synchroni... | ✓ | 2020-07-... | ArubaInt... |
| | 5003 | i63 Messenger | 8.66 | | | | ✓ | Synchroni... | ✓ | 2020-07-... | ArubaInt... |

802.1X Authentication requires a root certificate to be uploaded to the phone by “right clicking” - > Edit certificates. EAP-TLS will require both a CA and a client certificate.

# Appendix B: Detailed Verification Records

| | |
|---|---|
| Pass | 16 |
| Fail | 0 |
| Comments | 6 |
| Not verified | 6 |
| Total | 28 |

Refer to the attached file for detailed verification results.

# Document History

| Rev | Date | Author | Description |
|---|---|---|---|
| D1 | 29-April-2024 | NLRPa | Draft |
| P1 | 13-May-2024 | NLRPa | Adjusted Screenshots |
| | | | |
| | | | |