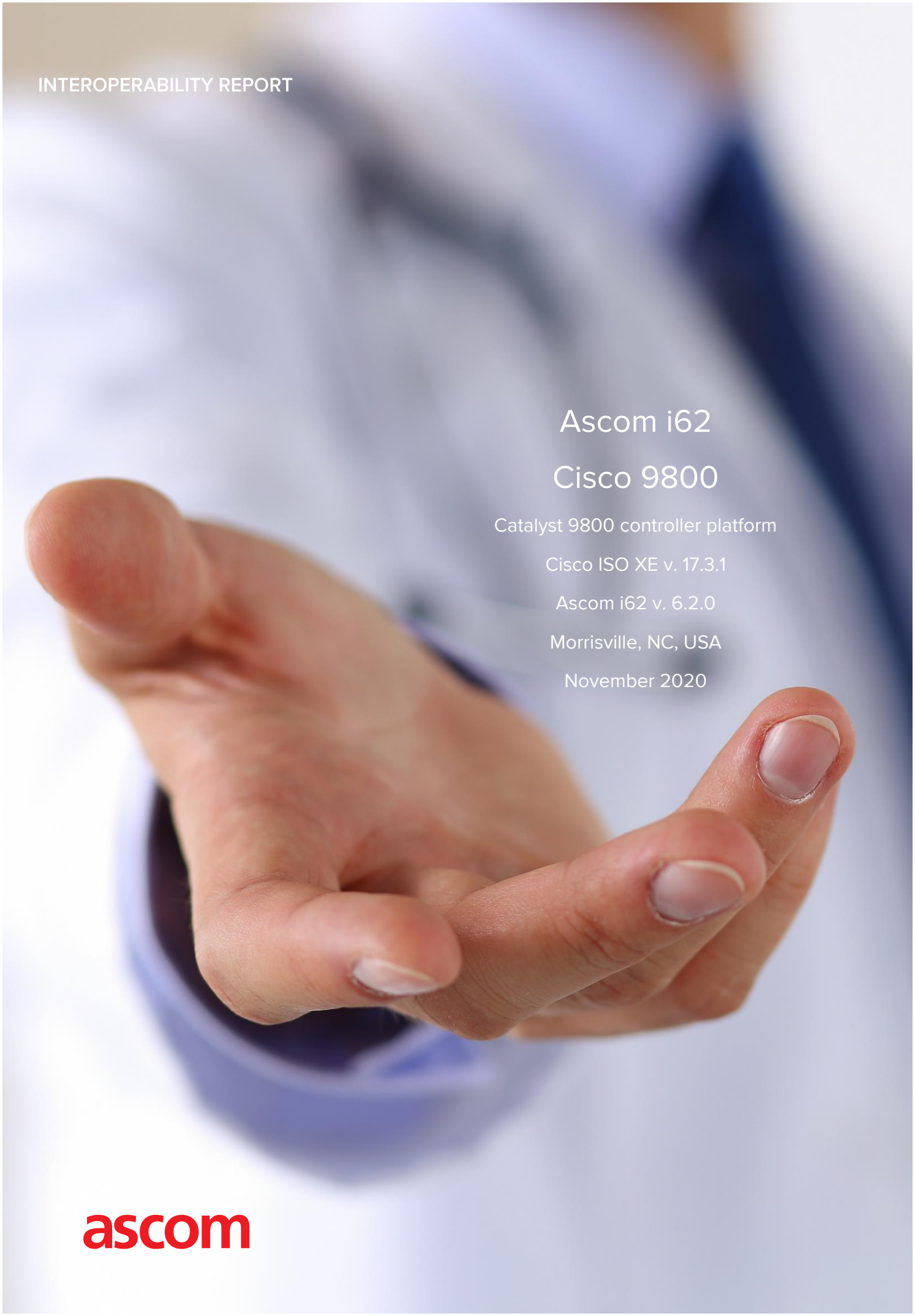
INTEROPERABILITY REPORT



Ascom i62

Cisco 9800

Catalyst 9800 controller platform

Cisco ISO XE v. 17.3.1

Ascom i62 v. 6.2.0

Morrisville, NC, USA

November 2020

ascom

Contents

Introduction

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

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at thenetwork.cisco.com and follow us on Twitter at @Cisco.

Site Information

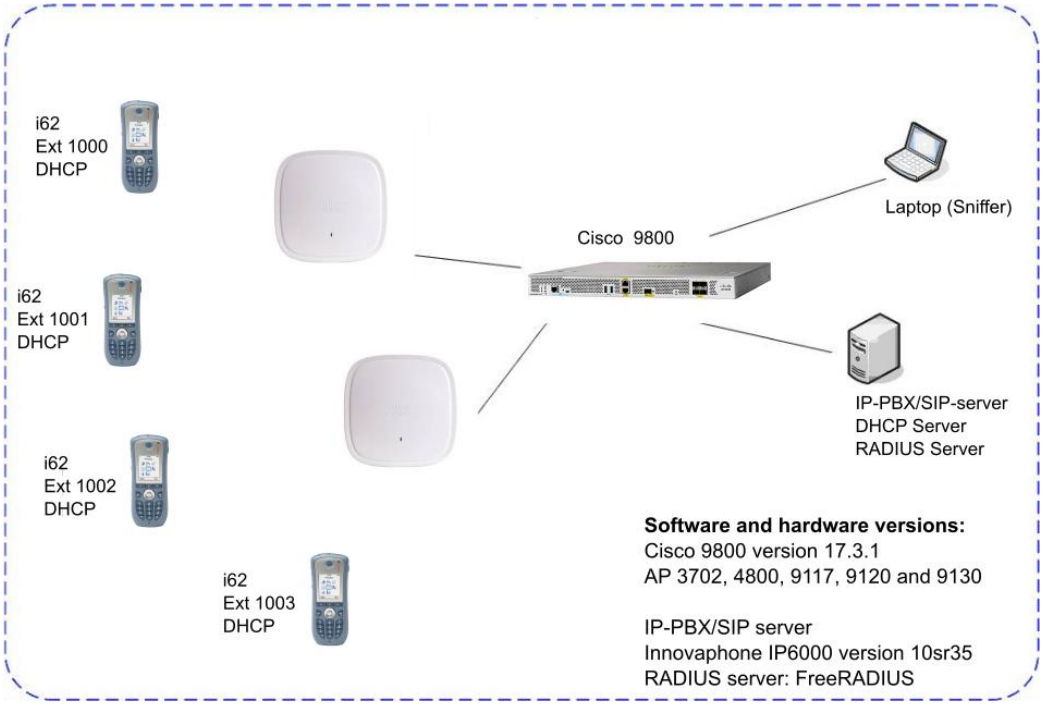
Verification site

Ascom US
300 Perimeter park drive
Morrisville, NC, US-27560
USA

Participants

Karl-Magnus Olsson, Ascom, Morrisville

Verification topology



Summary

General conclusions

The Ascom interoperability verification produced very good results with regards to all test areas including authentication, stability, roaming, QoS and power save related areas.

Issues with OKC basically prevents all other Auth methods than PSK from being viable options. Refer to Known Issues section for details.

Compatibility information

One Access point model from every product generation has been selected as a representation (AP 3702, 4800, 9117, 9120 and 9130). By testing these access points we are considered cover all supported major Cisco access points based on chipset compatibility listed below.

Supported Partner Access Points with SW version 17.3.1:

AP1702, 2702, 3702

AP1832, 1852

AP2802, 3802, 4800

AP 9115, 9117, 9120, 9130

Supported Partner Controller Platforms with SW version 17.3.1:

Cisco Catalyst 9800-80 Wireless Controller

Cisco Catalyst 9800-40 Wireless Controller

Cisco Catalyst 9800 Wireless Controller for Cloud

Cisco Catalyst 9800 Embedded Wireless Controller for Switch

Cisco Catalyst 9800-L Wireless Controller

Verification 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	NOK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	OK	
802.11e U-APSD (load test)	OK	
Roaming, WPA2-PSK, AES Encryption	OK *	Typical roaming time 50 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	NOK	Issue with OKC
Roaming, EAP-FAST, CCKM	OK	40ms

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

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
OKC not working. Roaming with 802.1X authentication methods always results in full EAP key exchange. Depending on infrastructure (RADIUS server etc.) roaming times could be above 1 second with significant loss of voice as result. Only viable authentication method supported until resolved is PSK	Use PSK	Contact Ascom interop team or Cisco Tac.
CAC/TSPEC problem. Significant voice gap during roaming when using CAC/TSPEC. Under investigation.	Make sure CAC is disabled in the 9800 system as well as in the i62 device	

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

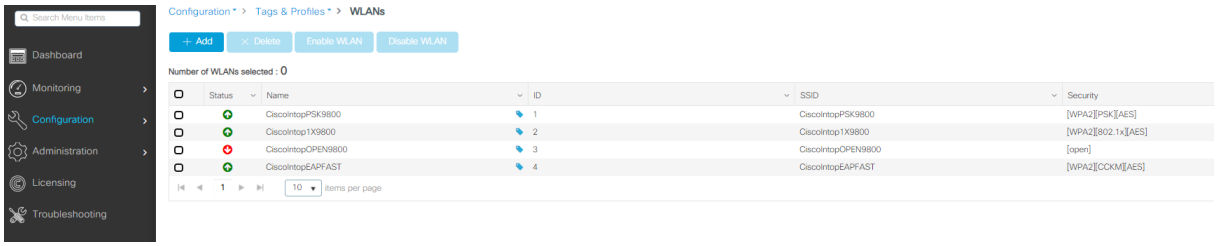
For detailed verification results, refer to Appendix B: Interoperability Validation Records.

Appendix A: Validation Configurations

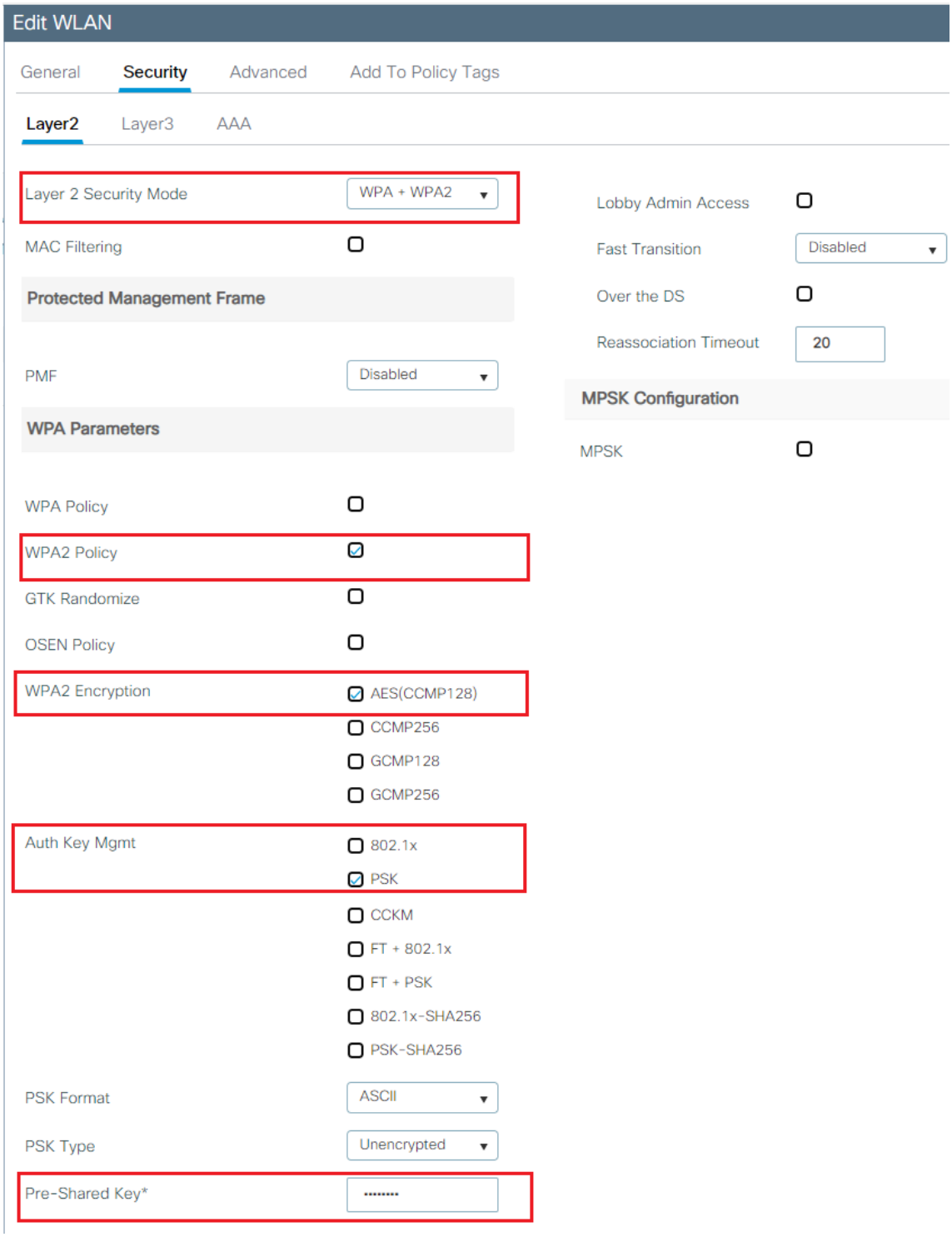
Cisco Catalyst 9800 platform Version 17.3.1

In the following chapter you will find screenshots and explanations of basic settings in order to get a Cisco 9800 WLAN system to operate with an Ascom i62. Please note that security settings were modified according to requirements in individual test cases.

WLAN settings



WLAN overview



WLAN PSK configuration

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

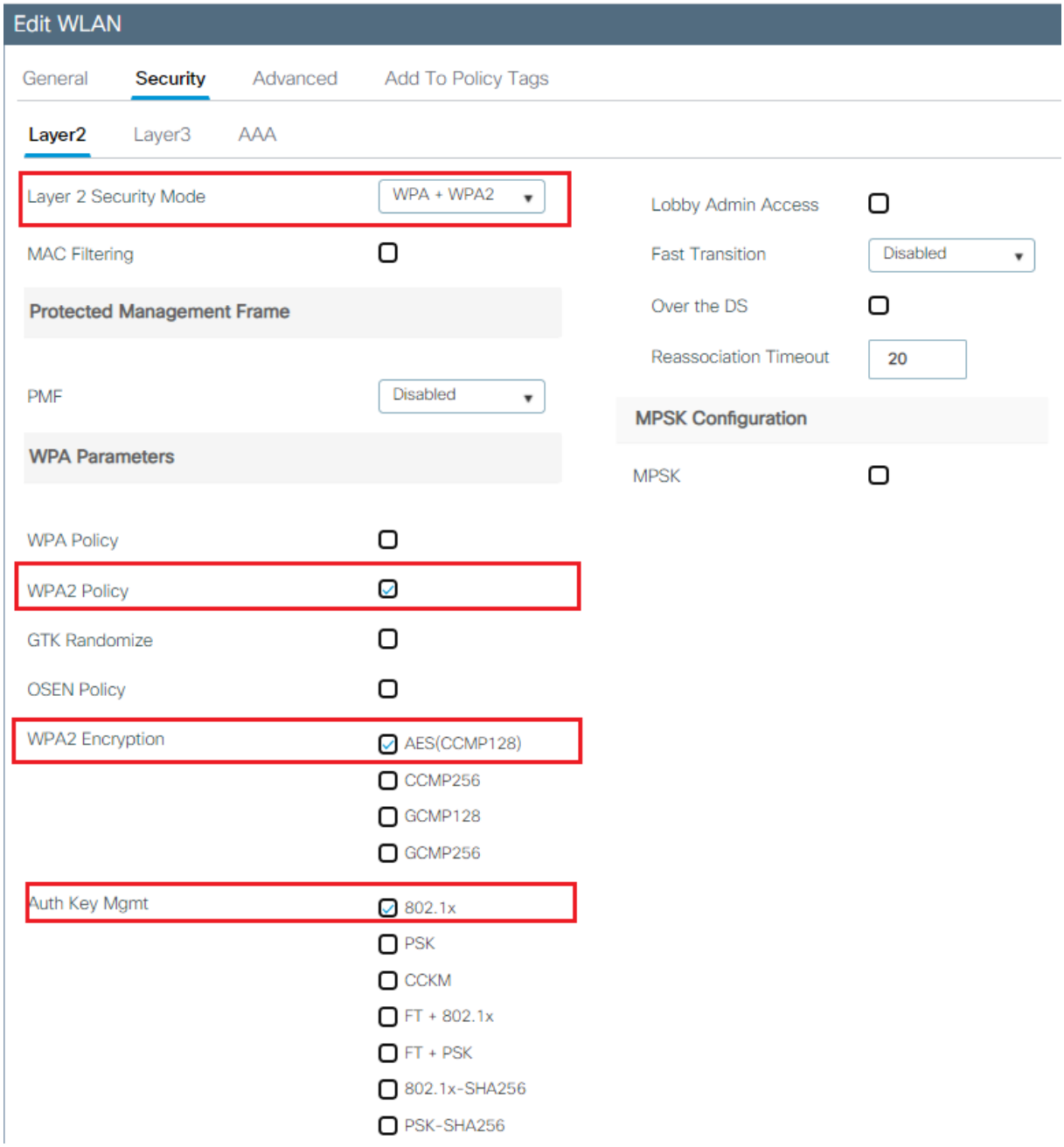
Security profile WPA2-PSK, AES encryption

- Select WPA2 Policy with AES encryption.
- Select PSK and enter a key (Here in ASCII format)

Note. Select both PSK and FT+PSK for compatibility with i63 and Myco 3 on the same SSID.

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.

802.1X authentication (PEAP-MSCHAPv2).



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

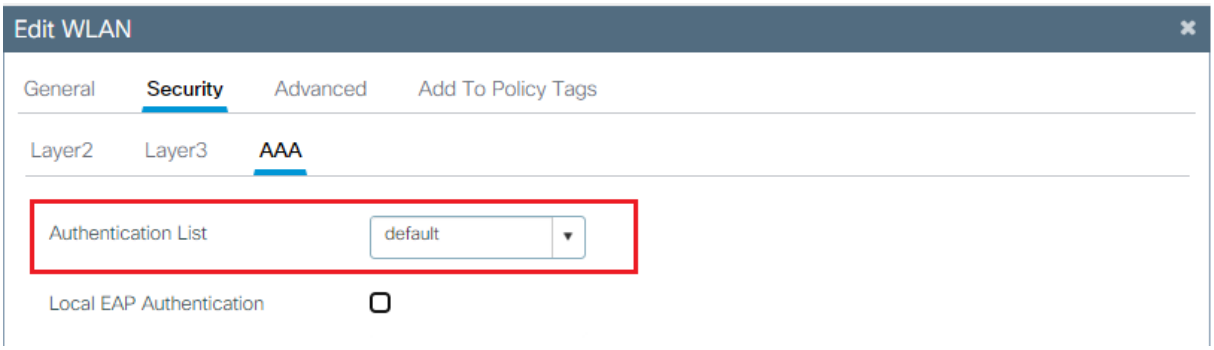
Not recommended until OKC issue is resolved

Configuration of authentication using external Radius server, 802.1X. In this example is WPA2-AES used. Select 802.1X as Authentication Key Management.

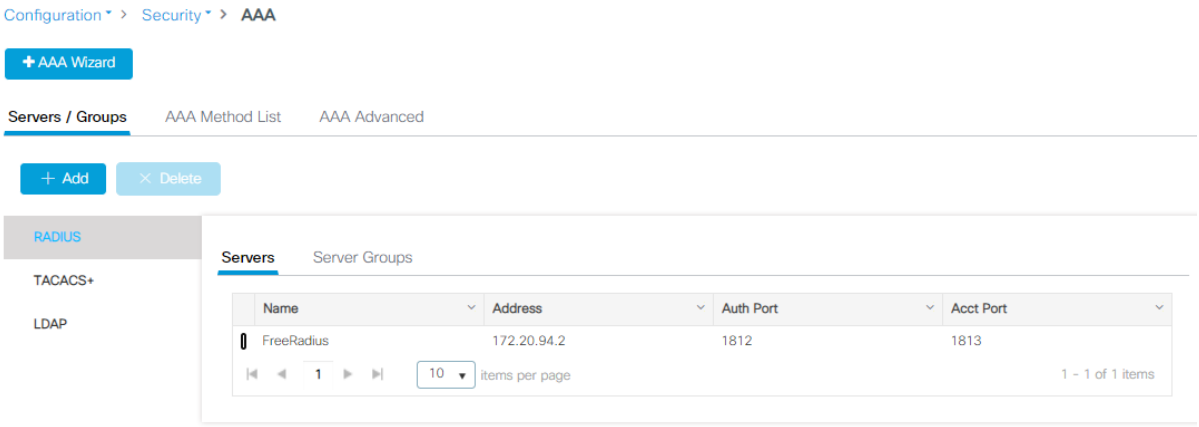
- Select WPA2 Policy with AES encryption.

Note. Select both 802.1X and FT + 802.1X for compatibility with i63 and Myco 3 on the same SSID.

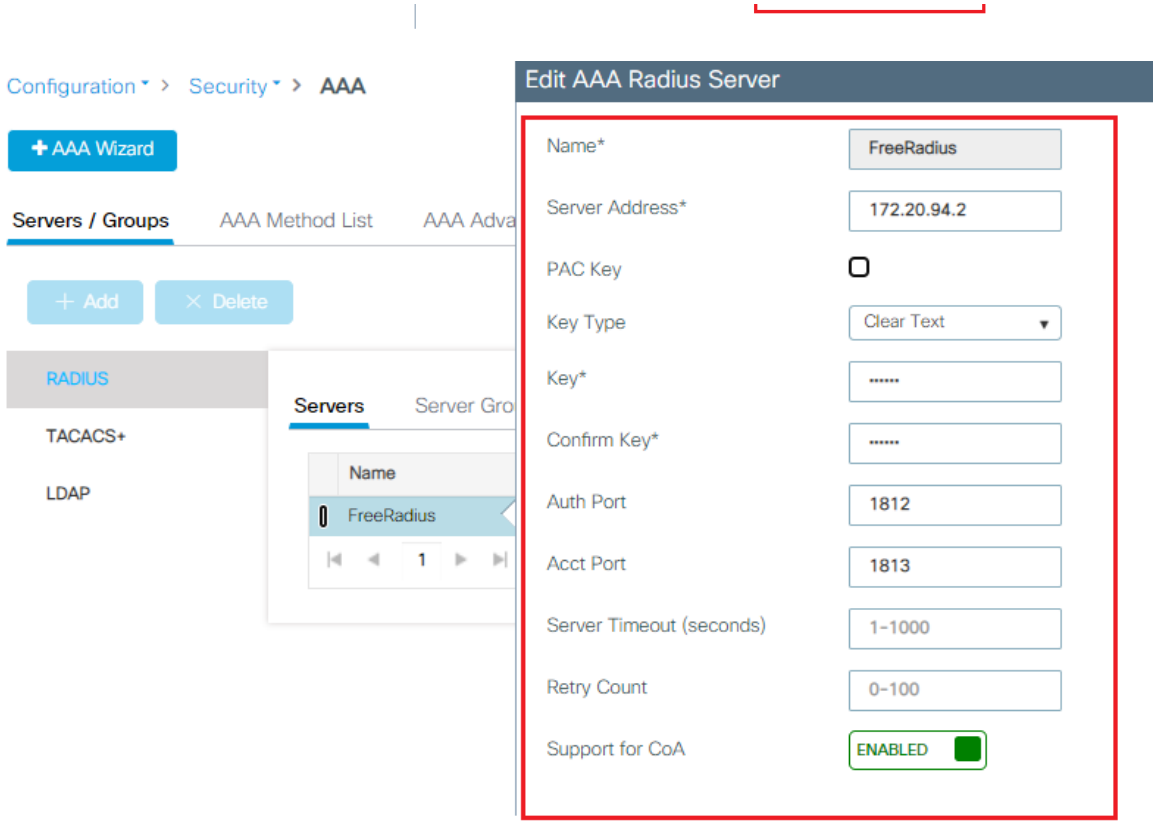
802.11r is not supported by Ascom i62 and Myco 1 & 2 but the devices have no problem operating on a SSIDs were 802.11r (FT) is advertised in conjunction with a legacy method.



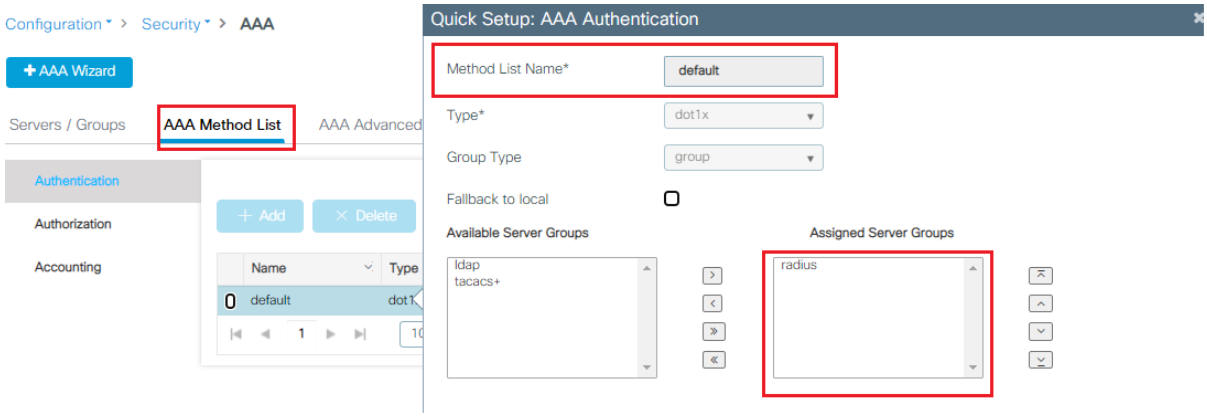
Example of authentication configuration using external Radius server. Select the Authentication list. The server is configured under tab Security/Radius. See configuration of server below.



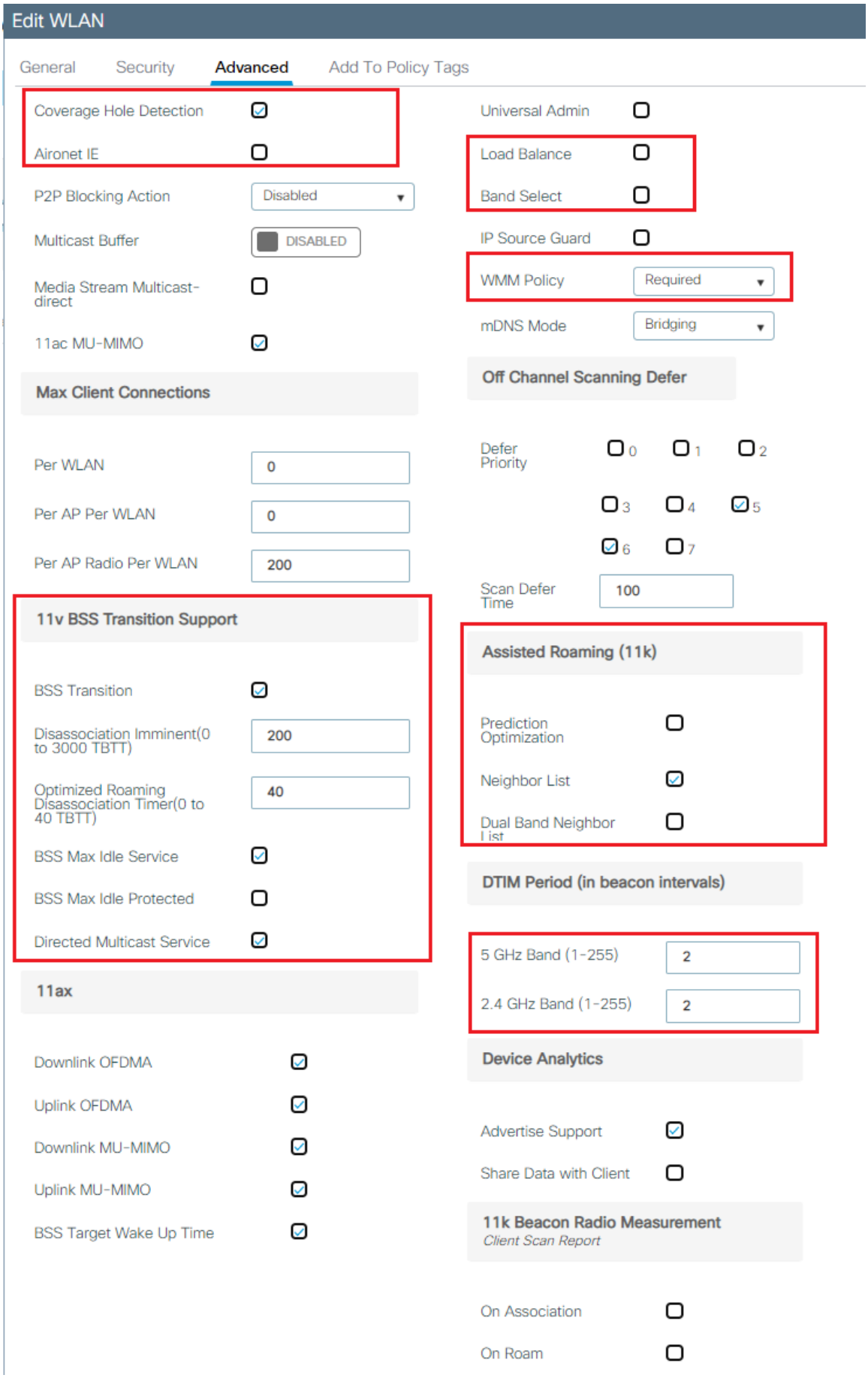
AAA overview



Configuration of RADIUS server. The IP address and the secret must correspond to the IP and the credential used by the Radius server. Tests were performed using FreeRadius as RADIUS server.

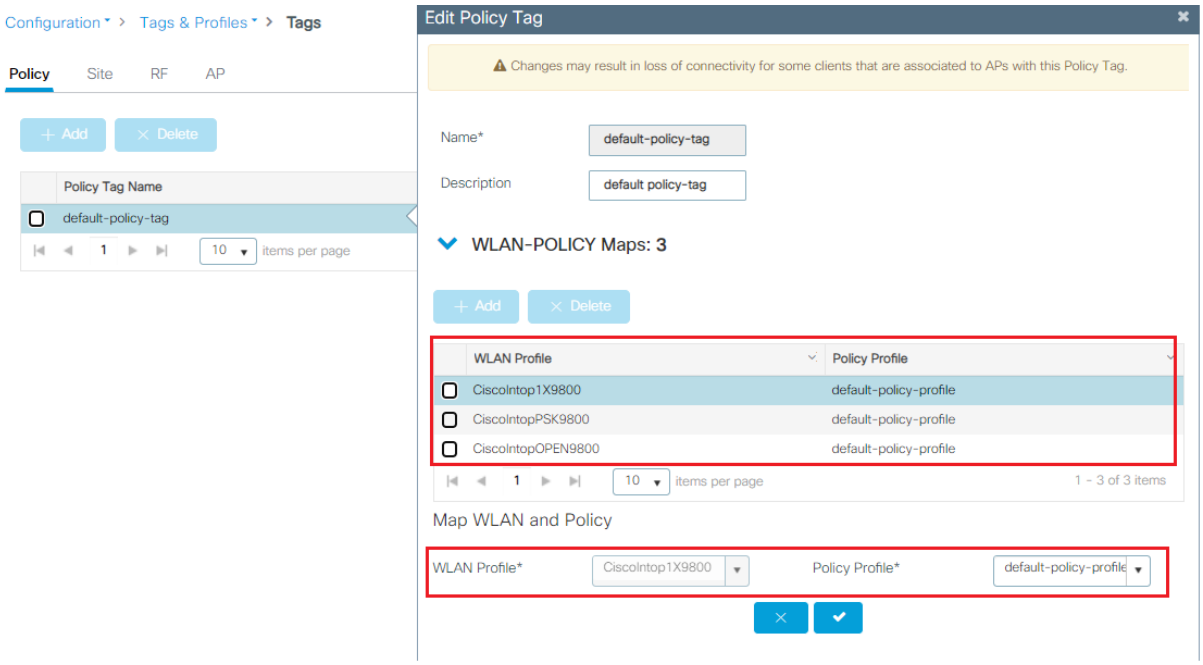


Assign radius server to Method List (default)

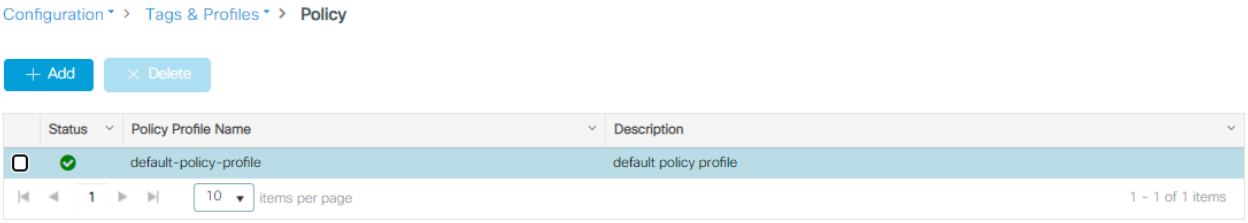

Edit WLAN
General
Security
Advanced
Add To Policy Tags
Coverage Hole Detection
Aironet IE
P2P Blocking Action
Disabled
Multicast Buffer
DISABLED
Media Stream Multicast-direct
11ac MU-MIMO
Max Client Connections
Per WLAN
0
Per AP Per WLAN
0
Per AP Radio Per WLAN
200
11v BSS Transition Support
BSS Transition
Disassociation Imminent(0 to 3000 TBTT)
200
Optimized Roaming Disassociation Timer(0 to 40 TBTT)
40
BSS Max Idle Service
BSS Max Idle Protected
Directed Multicast Service
11ax
Downlink OFDMA
Uplink OFDMA
Downlink MU-MIMO
Uplink MU-MIMO
BSS Target Wake Up Time
Universal Admin
Load Balance
Band Select
IP Source Guard
WMM Policy
Required
mDNS Mode
Bridging
Off Channel Scanning Defer
Defer Priority
0
1
2
3
4
5
6
7
Scan Defer Time
100
Assisted Roaming (11k)
Prediction Optimization
Neighbor List
Dual Band Neighbor List
DTIM Period (in beacon intervals)
5 GHz Band (1-255)
2
2.4 GHz Band (1-255)
2
Device Analytics
Advertise Support
Share Data with Client
11k Beacon Radio Measurement
Client Scan Report
On Association
On Roam

- Coverage Hole Detection can be left enabled if RRM is used in the system.
- Aironet IE is not needed.
- Ascom recommends a DTIM period of at least 2 but no higher than 5.
- Make sure Client Load Balancing and Client Band select is disabled.
- Even though 11k features are not supported by Ascom i62 it can coexist in a network were it is enabled.

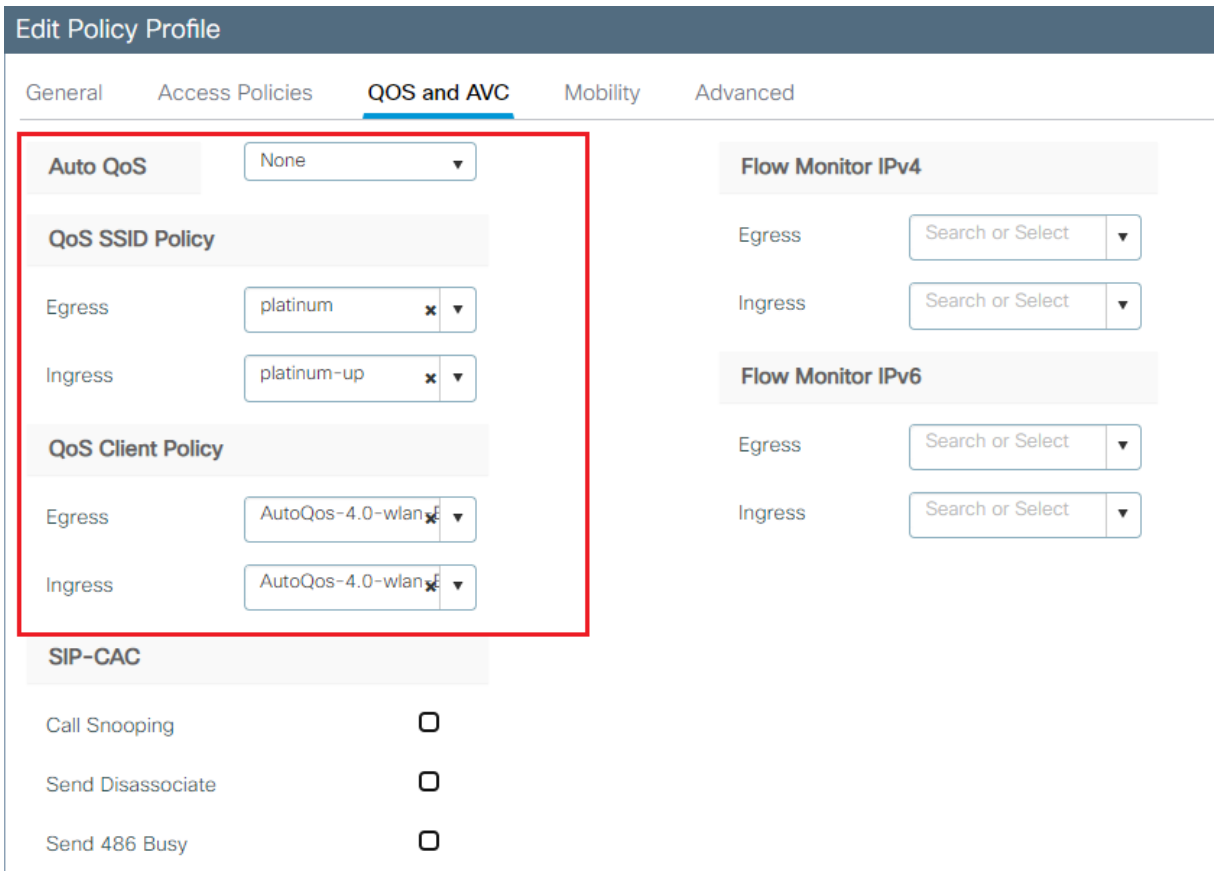
Policy and general settings (QoS, Radio)



Assign your policy profile to WLAN. (here default-policy-profile). See next step for policy profile settings.

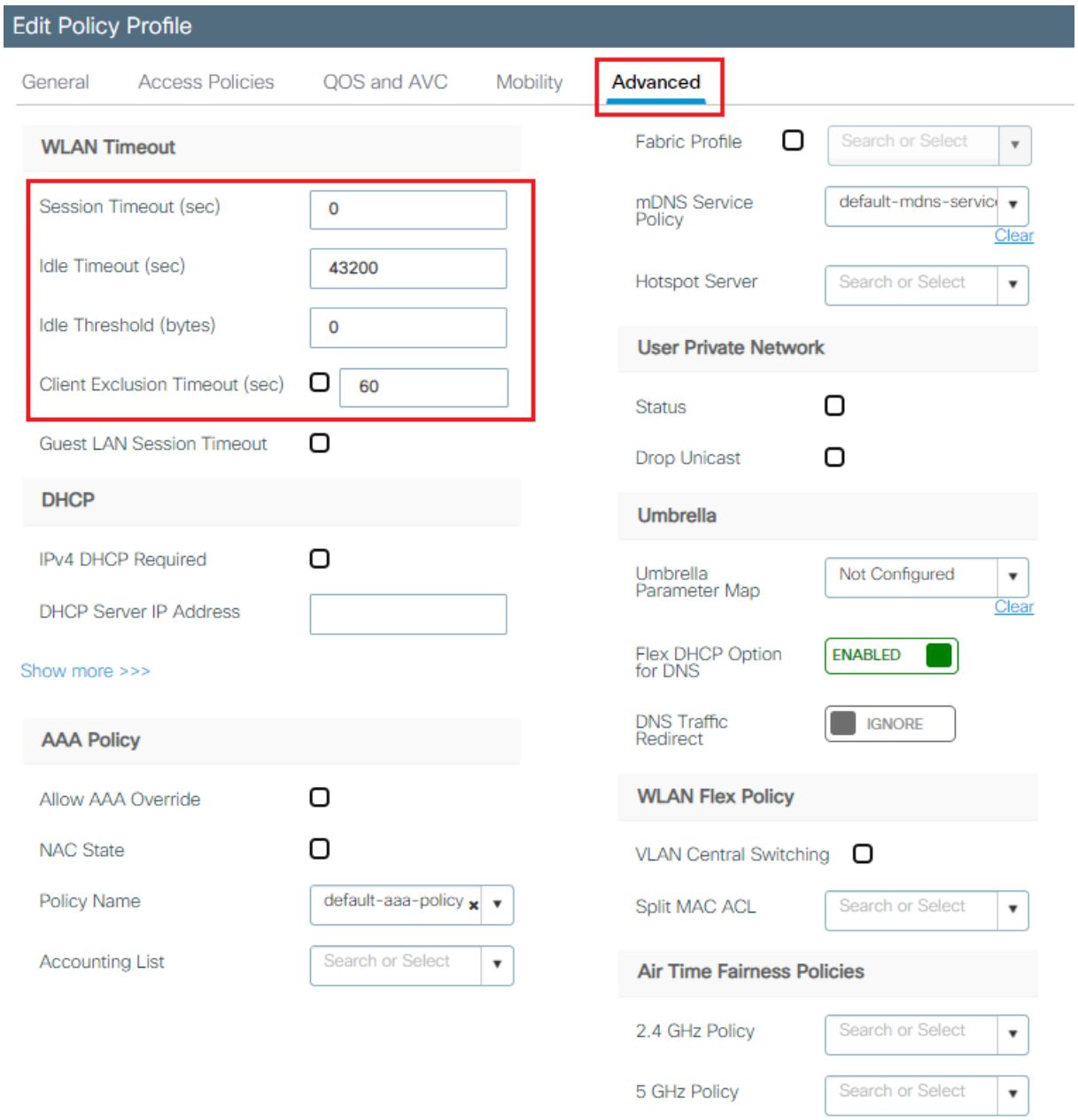


Policy overview



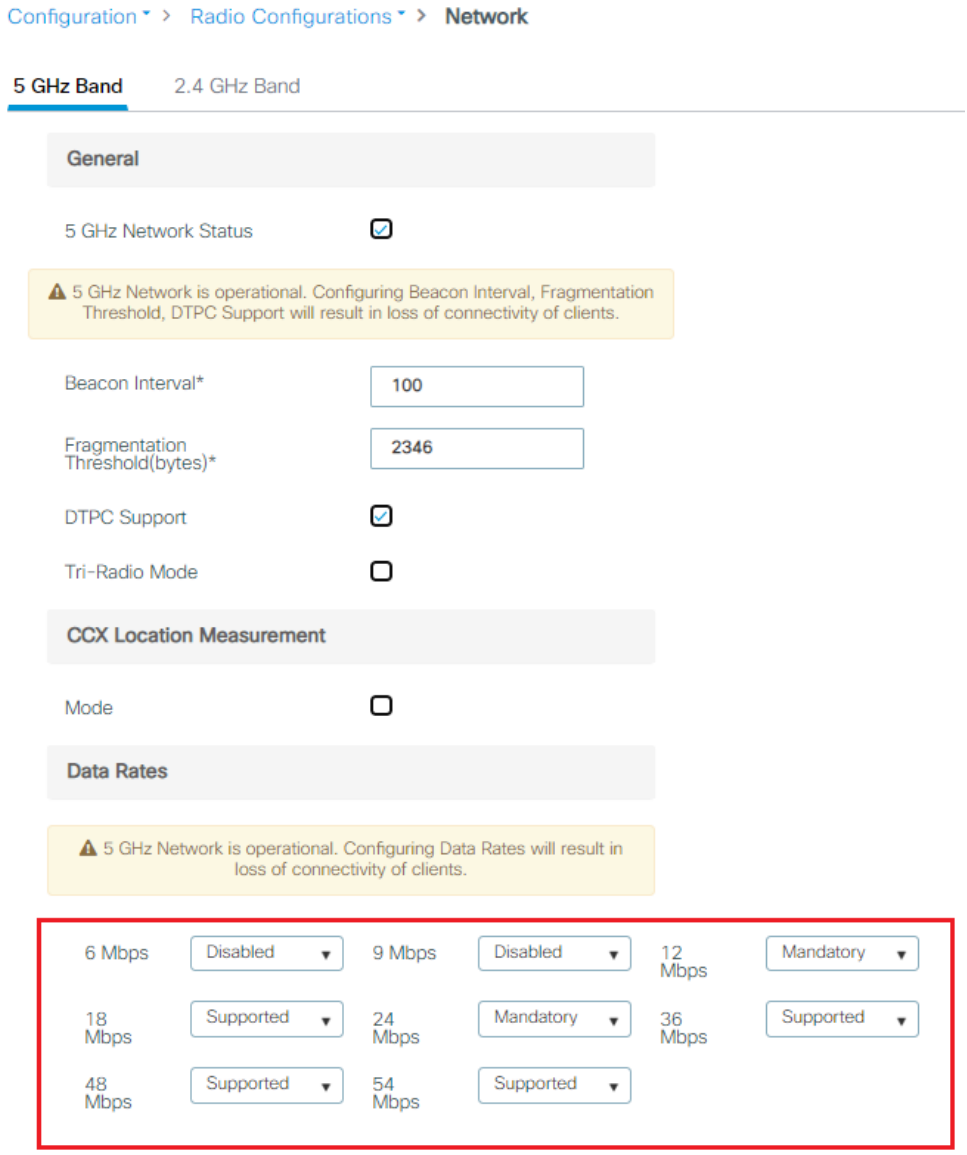
QoS and AVC settings

- Set Auto QoS to none
- Set QoS SSID Policy Egress to “platinum” and ingress value to “platinum-up”
- Set QoS Client Policy Egress to “AutoQoS-4.0-wlan-ET-SSID-Output-policy” and ingress to “AutoQoS-4.0-wlan-ET-SSID-Input-AVC-policy”

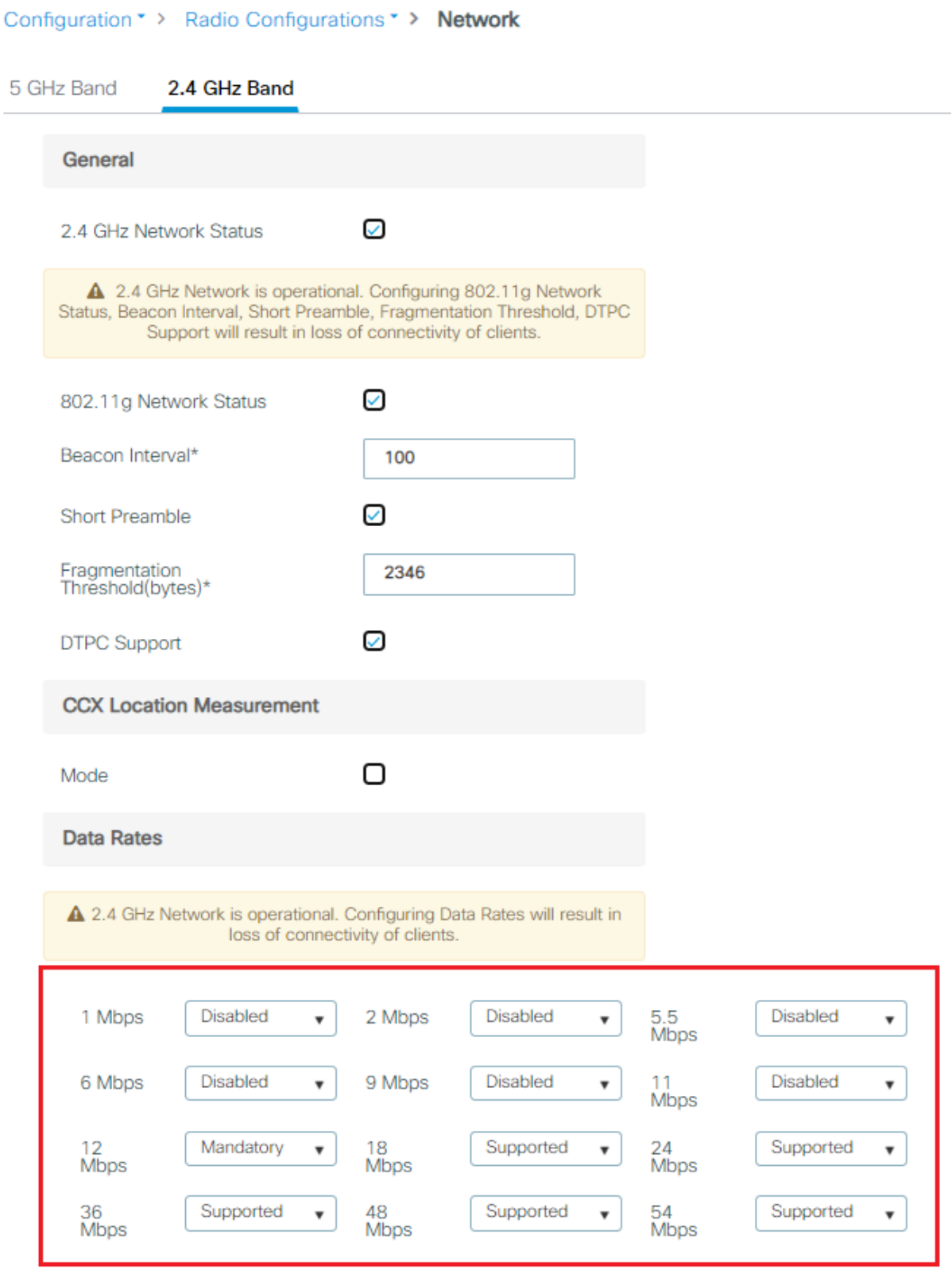


- Make sure “Session timeout” is disabled or set to a very large value.
- Disable Client Exclusion

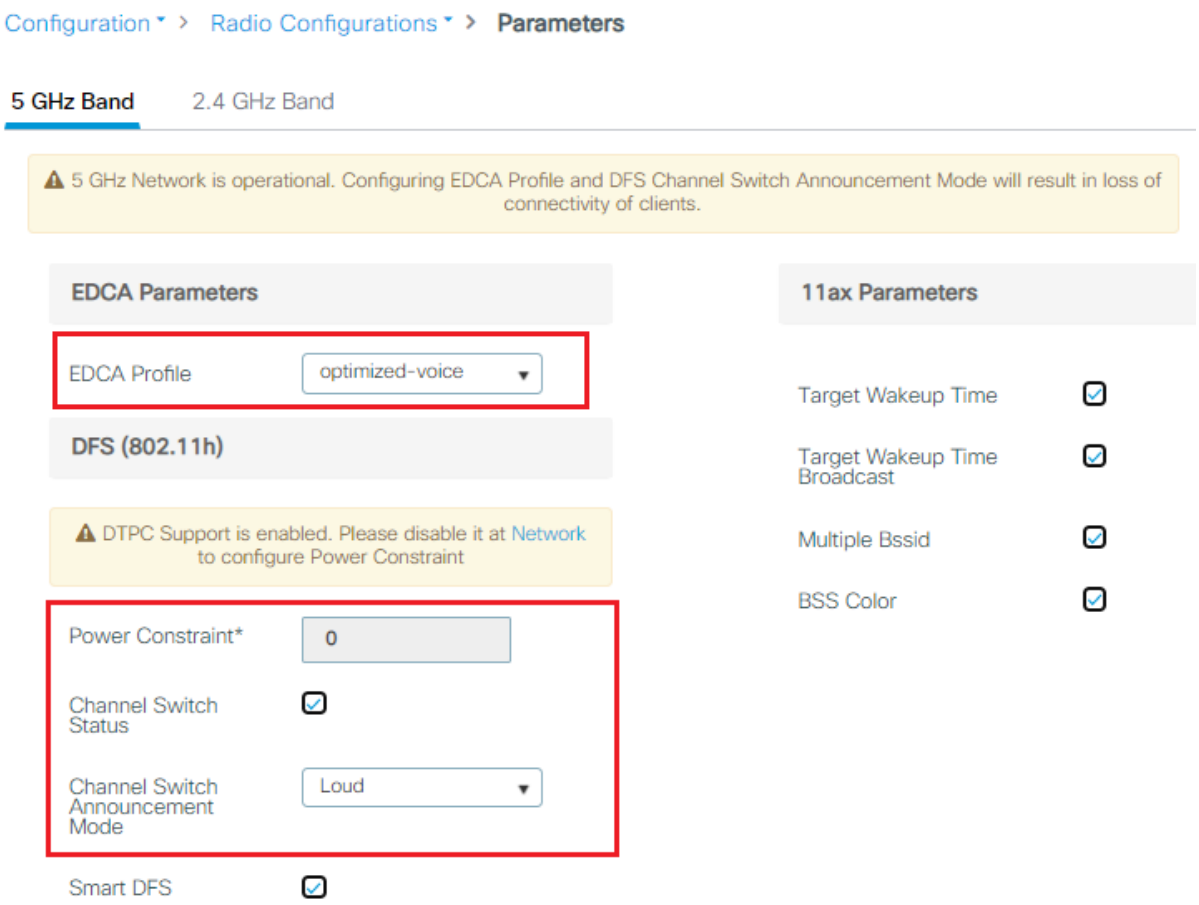
Network Settings and



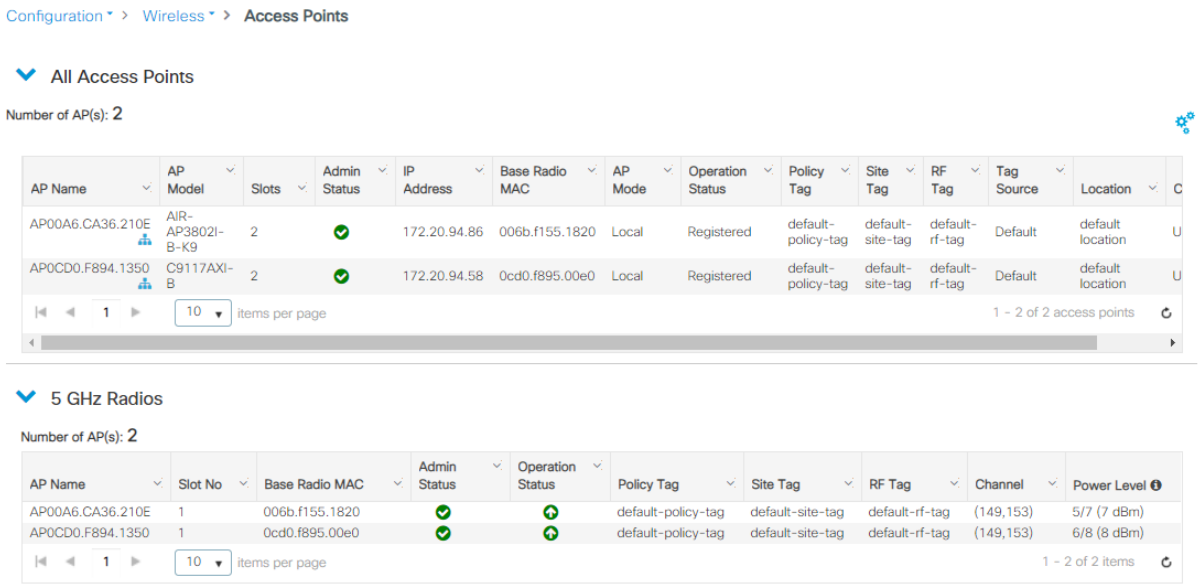
Data rates 5GHz. The default data rate set will work just fine, however Ascom recommends disabling the lowest data rates and have 12Mbps as lowest data rate.



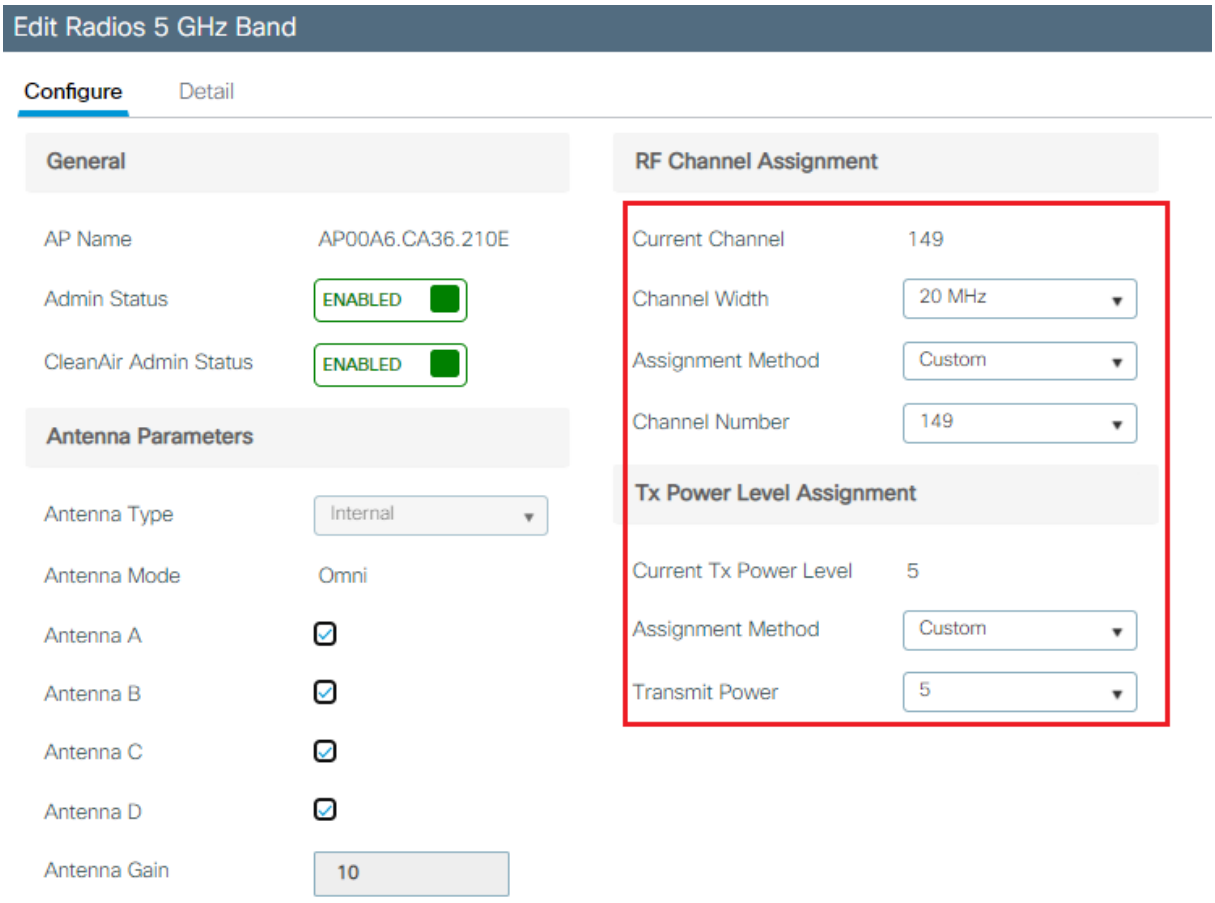
Ascom recommends disabling the lowest data rates and have 12Mbps as lowest data rate.



- Set EDCA profile to optimized-voice. (Using EDCA Profile “WMM” is acceptable but “Voice Optimized” is to prefer when voice clients are present in the system=
- As Ascom do support Channel Switch Announcement it’s recommended to have this setting enabled in the system (loud). Only applicable when DFS channels are used.



Access points and channel overview. See next picture for specific radio configuration.



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, country regulations and per guidelines below.

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

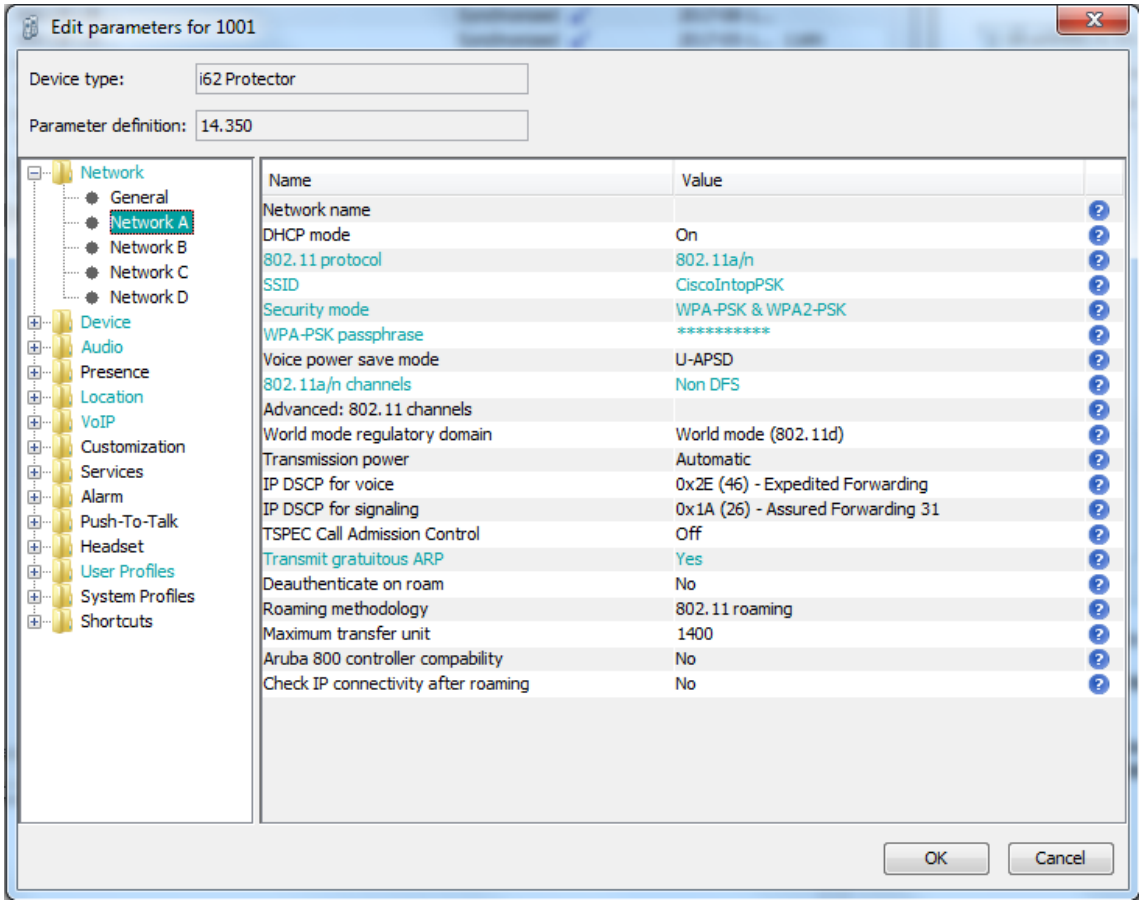
1. ***Enabling more than 8 channels will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed.***
   Ascom does not recommend exceeding this limit.

2. ***Using 40 MHz channels (or "channel-bonding") will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 20MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.***

3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***

4. ***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.***

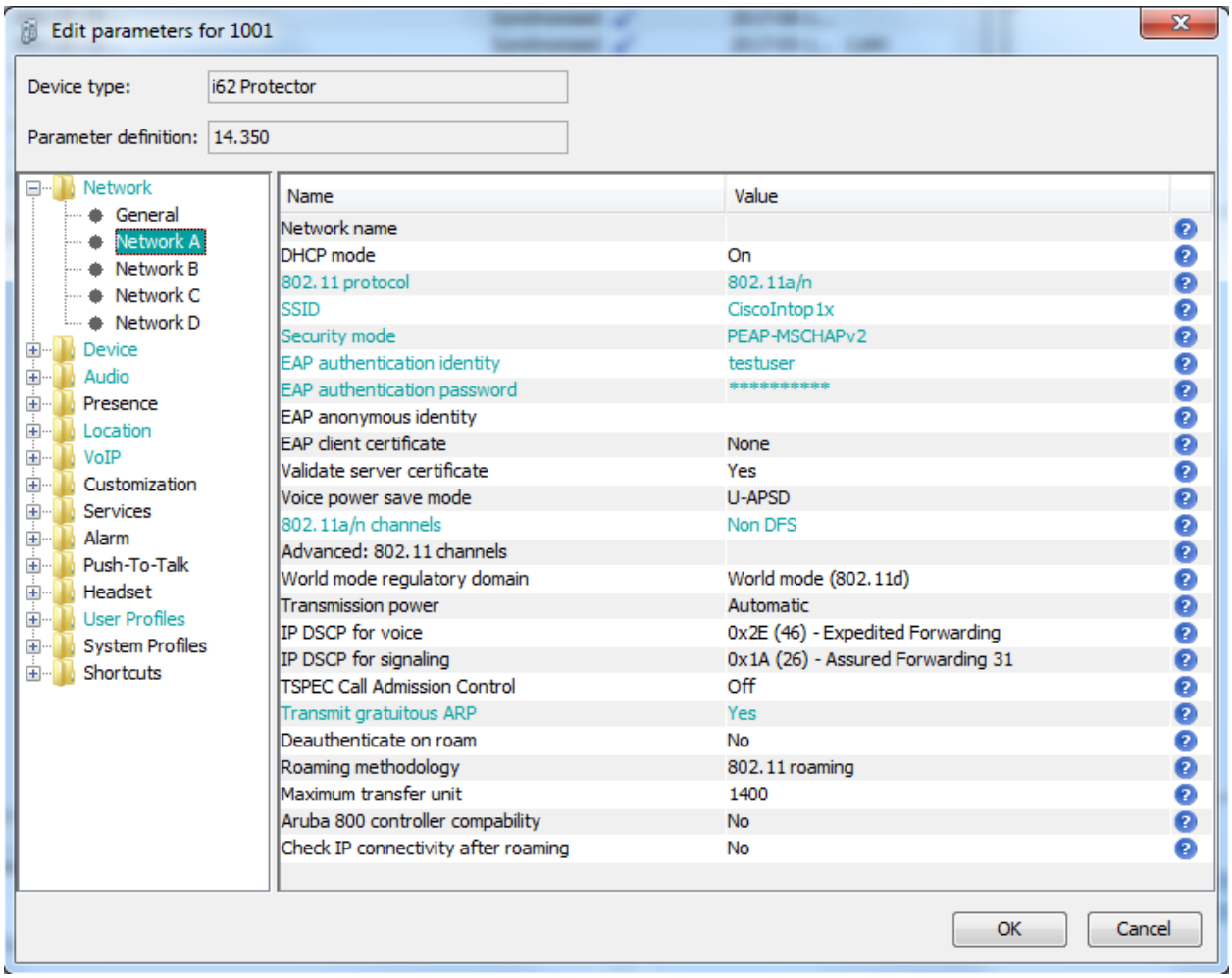
***) Dynamic Frequency Selection (radar detection)**



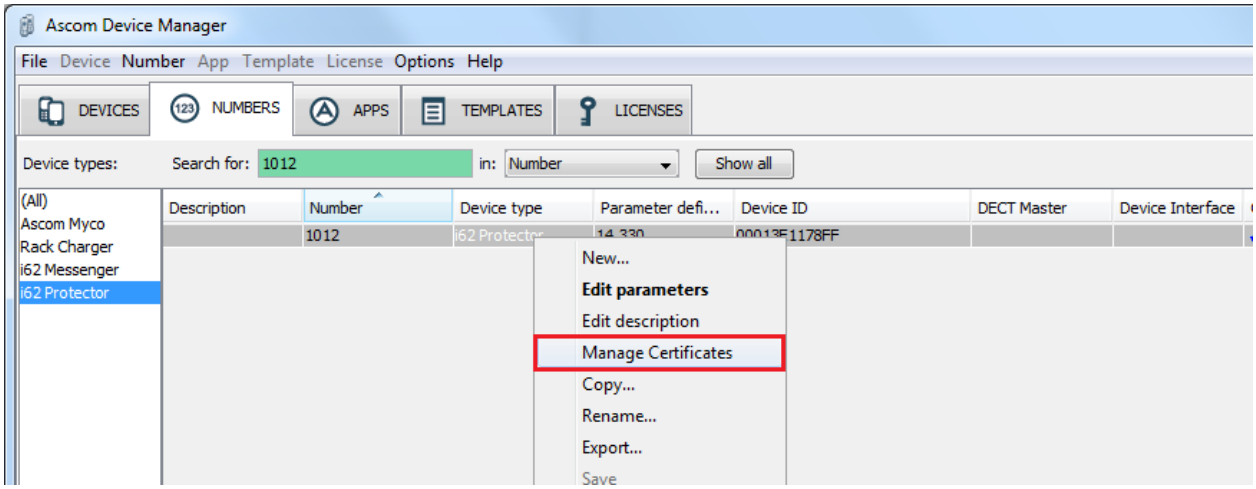
Network settings for WPA2-PSK

Note. Make sure that the enabled channels in the i62 handset match the channel plan used in the system.

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



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



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

Note that both a CA and a client certificate are needed for TLS. Otherwise only a CA certificate is needed. Server certificate validation can be overridden in version 4.1.12 and above per handset setting.

Appendix B: Interoperability Validation Records

Pass	13
Fail	3
Comments	1
Not validated	5
Total	20

Refer to the attached file for detailed validation results.

Refer to the validation specification for explicit information regarding each validation case.
The specification can be found here (requires login):
https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability/Templates/

Document History

Rev	Date	Author	Description
P1	3-Nov-20	SEKMO	Draft
R1	9-Nov-20	SEKMO	Internal review. R1