INTEROPERABILITY REPORT

Ascom i63

Fortinet

Fortinet MC/WLC platform

Fortinet MC/WLC v. 8.5-2build5

Ascom i63 v. 3.0.0

Morrisville, NC, USA

June 2021

ascom

Contents

Introduction

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

About Ascom

Ascom is a global provider of mobile workflow solutions. The vision of Ascom is to close digital information gaps allowing for the best possible decisions – anytime and anywhere. We provide mission-critical, real-time solutions for highly mobile, ad hoc, and time-sensitive environments. We use 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 has a strong global market presence and a loyal installed base of highly visible customers. With solid and proven products, technologies and service capabilities and a great team with unique information, communication and workflow technology experts in particular in healthcare, Ascom is well positioned to be a comprehensive solution provider in the healthcare ICT, industry, retail and security markets worldwide.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networked, application, multi-cloud or edge environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses. Both a technology company and a learning organization, the Fortinet Network Security Expert (NSE) Training Institute has one of the largest and broadest cybersecurity training programs in the industry. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Site Information

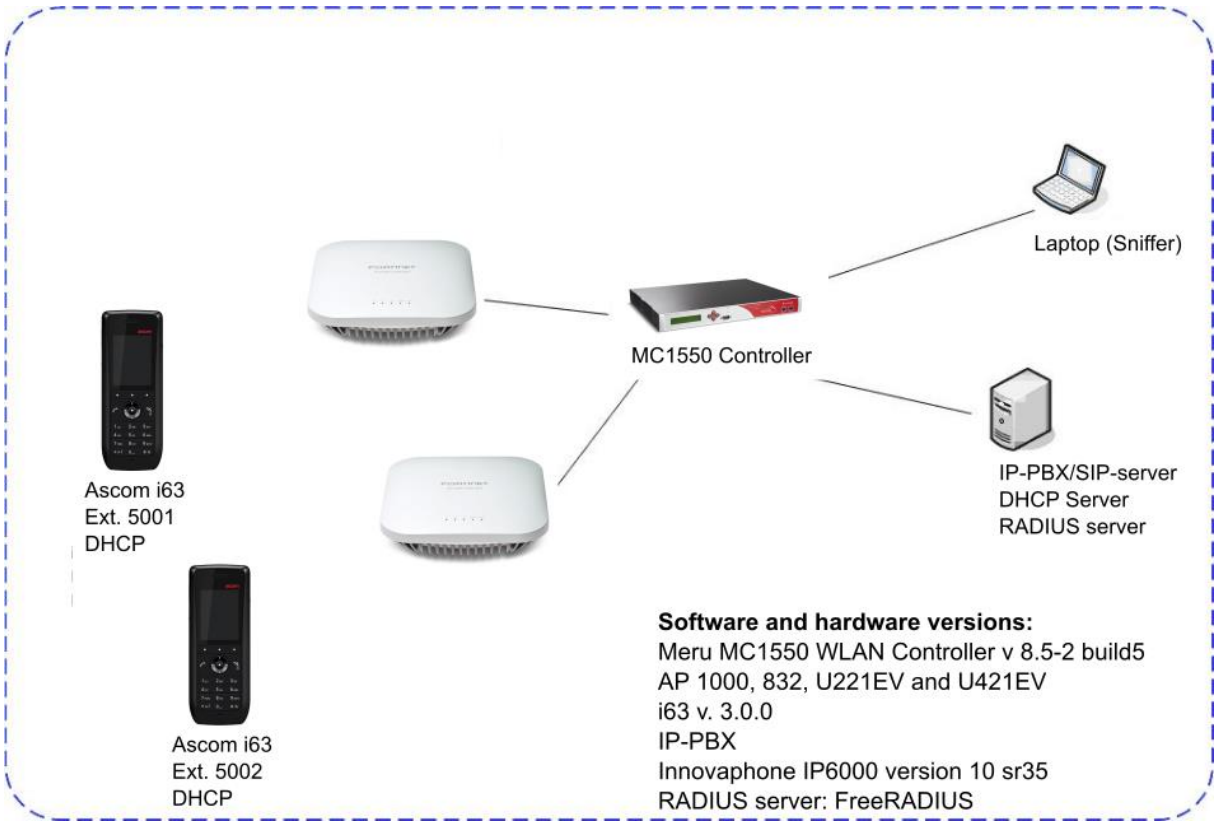
Verification site

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

Participants

Karl-Magnus Olsson, Ascom, Morrisville

Verification topology



Summary

General conclusions

The result of the verified test areas, such as authentication, association, handover and call stability tests, produced in general good test result. Due to Fortinet's single channel architecture, no traditional roaming is made which makes the roaming seamless.

Note. The parameter "Expedited Forwarding Override" will mark Voice packets DSCP 46 instead of 48. This is mandatory for appropriate mapping in the "air" (Access Category 6). Refer to ESS configuration on page 15.

Please refer to Fortinet's documentation for information regarding co-existence and between different access point models within the same wireless network.

Supported Partner Access Points with SW version 8.5-2-5:

AP 1010, 1014, 1020 (i/e variants)

AP 822 and AP832 (i/e variants)

AP U221EV, U223EV

AP U321EV, U323EV

AP U421EV, U423EV

Supported Partner Controller Platforms with SW version 8.5-2.5:

MC MC1550, MC3200

FortiWLC-50D ,200D, 500D, 1000D, 3000D

FWC- VM-50, 200, 500, 1000, 3000

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 with WPA3 SAE (PSK) authentication	Not tested	Known issues (refer to i63 release notes)
Association with WPA3 Enterprise authentication	N/A	Not supported by Fortinet
Association, Multiple ESSIDs	OK	
Beacon Interval and DTIM Period	OK	
PMKSA Caching	OK	
WPA2-opportunistic/proactive Key Caching	NOK	Not supported by Fortinet
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	Virtual Cell: Roam transparent to handset Native cell: Typical roaming time 35-100ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Roam transparent to handset Native cell: NOK due to lack of OKC support.
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK NOK (AP1000)	Virtual Cell: Roam transparent to handset Native cell: Typical roaming time 20-40ms
Channel usage controlled by 802.11k	OK NOK (AP1000)	Applicable for Native Cell only
Roaming, WPA3-PSK Authentication	Not tested	Known issues (refer to i63 release notes)
Roaming, WPA3-Enterprise Authentication	N/A	Not supported by Fortinet

Known limitations

Description and Symptoms	Workaround	Ticket(s) raised
RF Virtualization Mode considerations. - Virtual Cell mode (single-channel): Supported with all tested AP models - Native cell mode (multi-channel) with PSK authentication: Supported with all tested AP models using 802.11r/FT - Native cell mode (multi-channel) with EAP authentication: Not supported with AP 1000 series* *AP1000 have no support for OKC or 802.11r/FT hence making roaming times unacceptable long for voice applications.		
802.11k is not supported with AP1000 series access points. Applicable for Native cell mode (multi-channel) only.	Setting “Use 802.11k neighbor list” needs to be set to NO	
WPA3-SAE (PSK): Known problems with i63. Refer to i63 release note WPA3-Enterprise: Not supported by Fortinet WLC.	Use WPA2	

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 Verification Records.

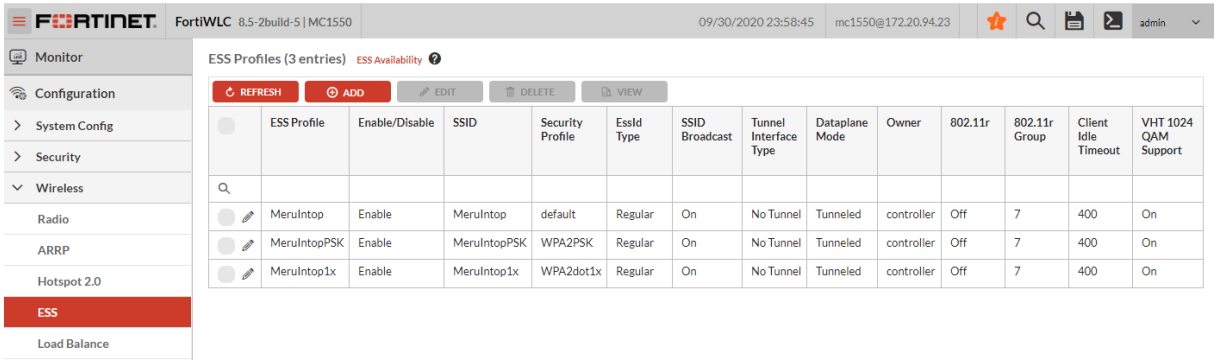
Appendix A: Verification Configurations

Fortinet MC1550 WLAN Controller version 8.5-2-5

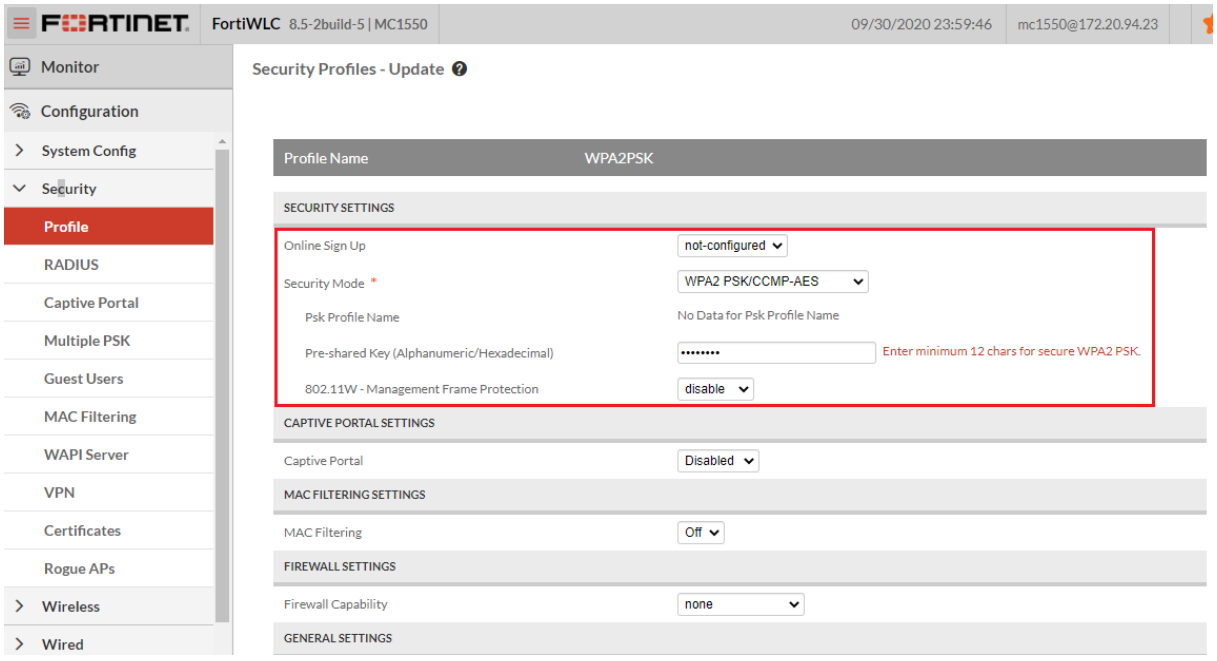
In the following chapter you will find screenshots and explanations of basic settings in order to get a Fortinet WLAN system to operate with an Ascom i63. Please note that security settings were modified according to requirements in individual test cases.

The configuration file is found at the bottom of this chapter.

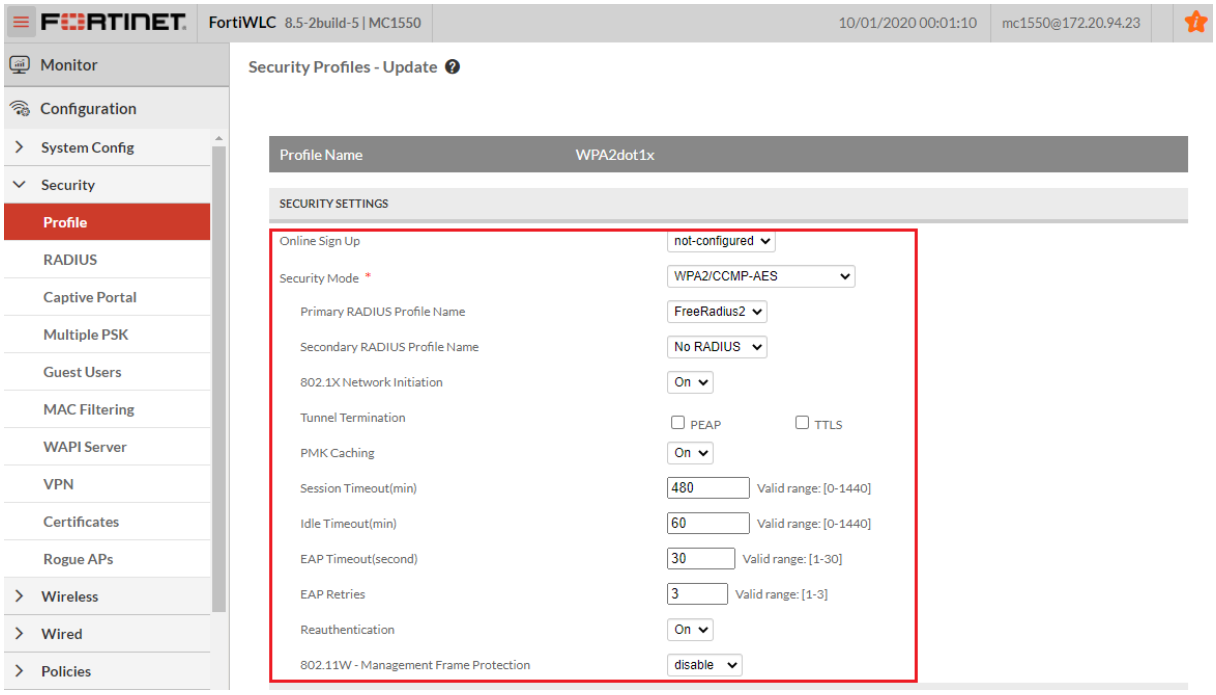
Security settings



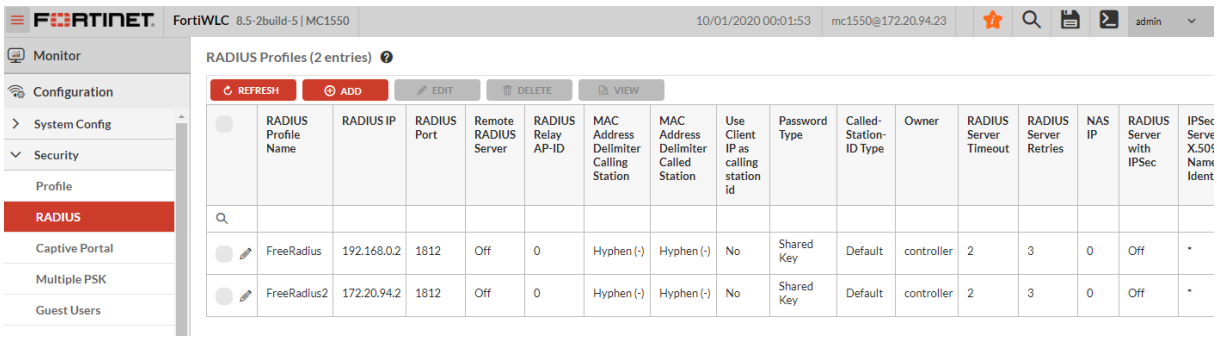
ESS profiles.



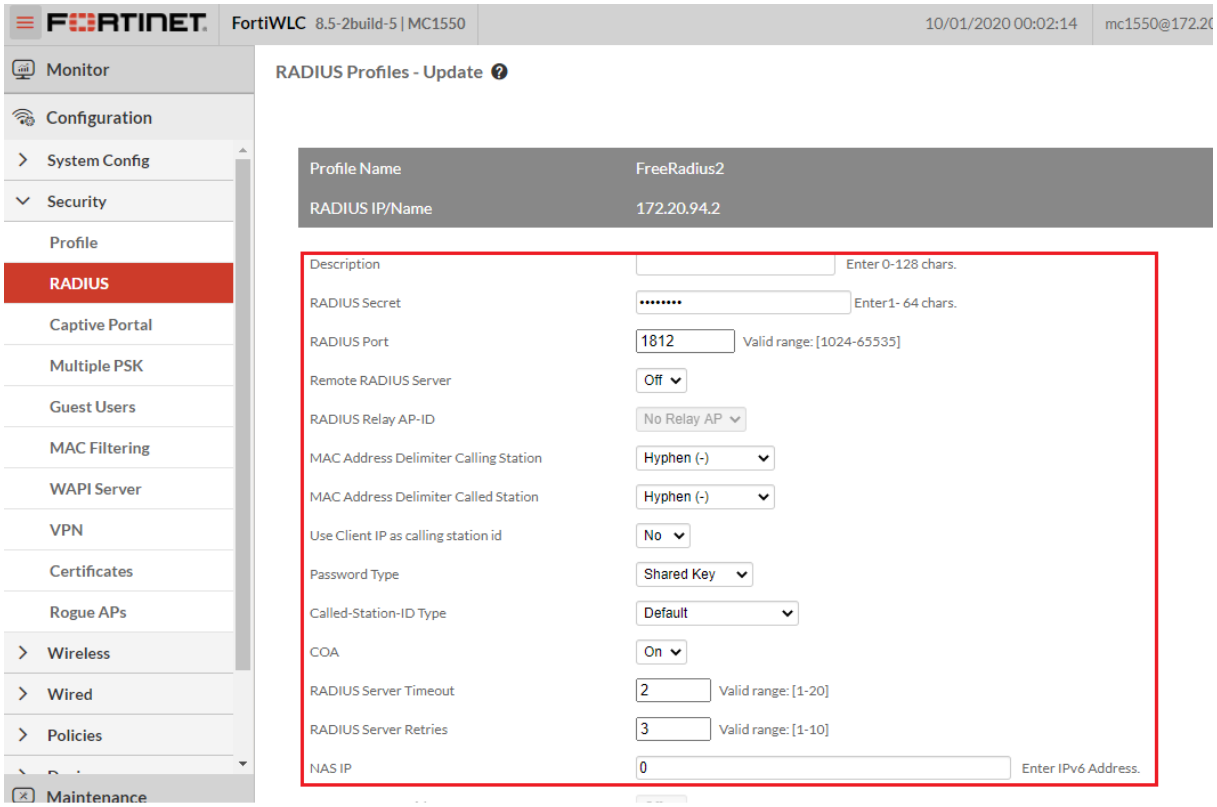
Security profile WPA2-PSK, AES/CCMP encryption.



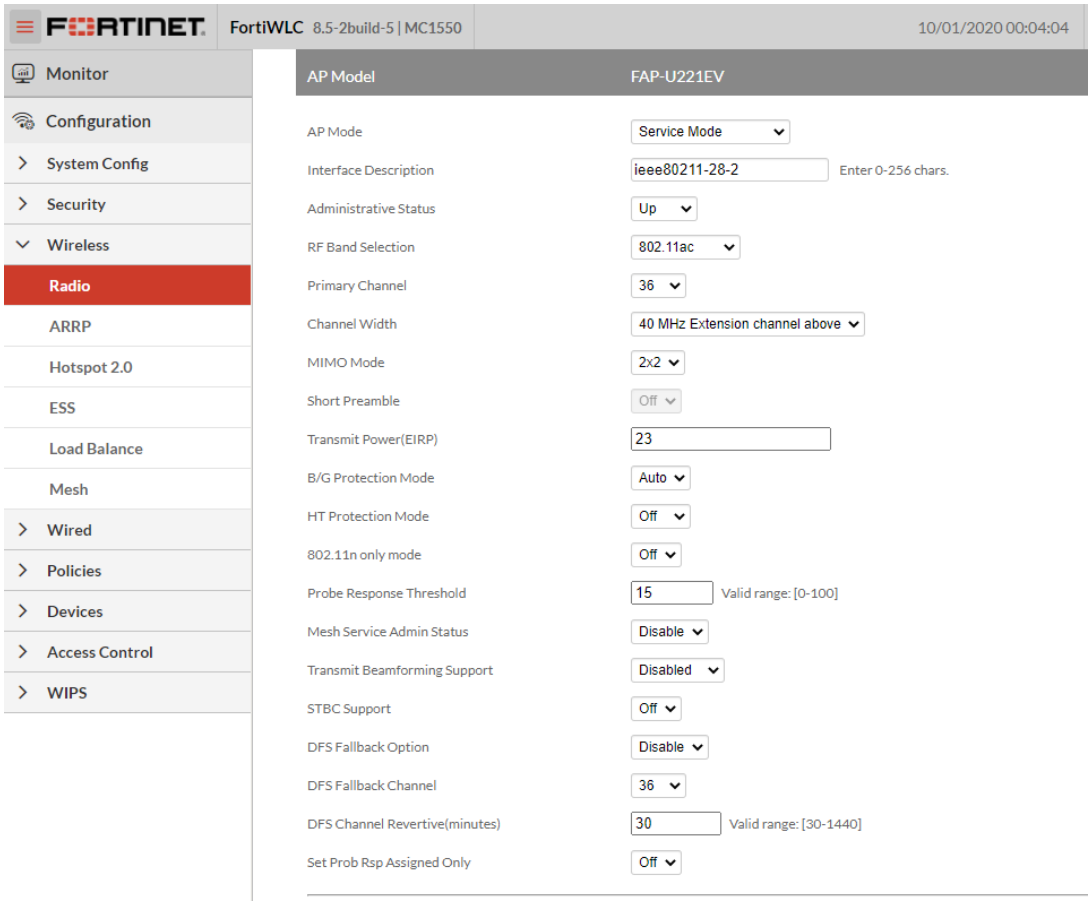
Security profile WPA2-Enterprise, AES-CCMP encryption Primary RADIUS Profile Name “FreeRadius 2” refers to the RADIUS profile set up in the controller. See radius profile below for additional details.



Configuration of Radius profile.



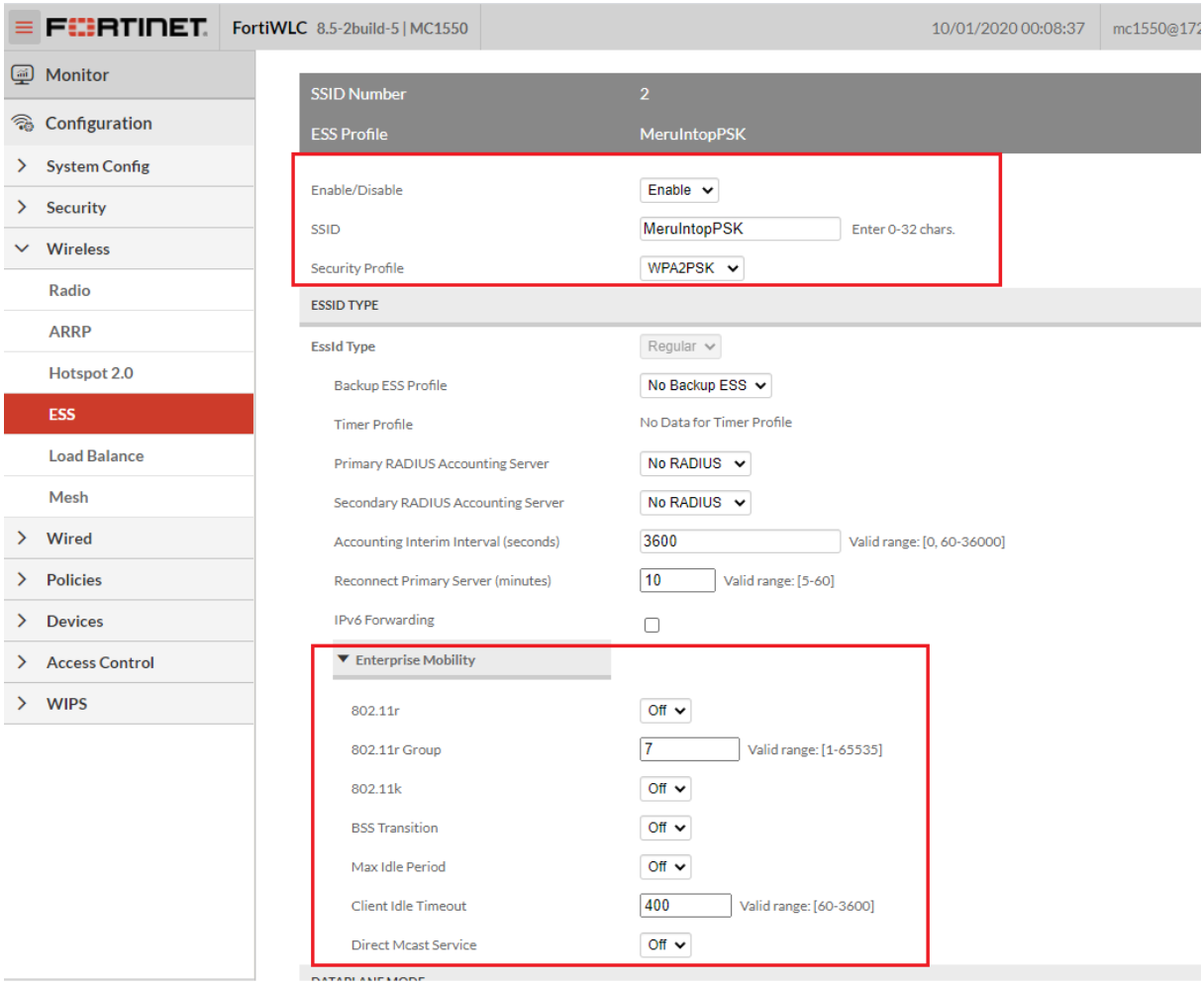
Radius profile configuration. Note that the profile “FreeRadius 2”, the RADIUS IP and the secret must correspond to the authentication server running in the network.



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

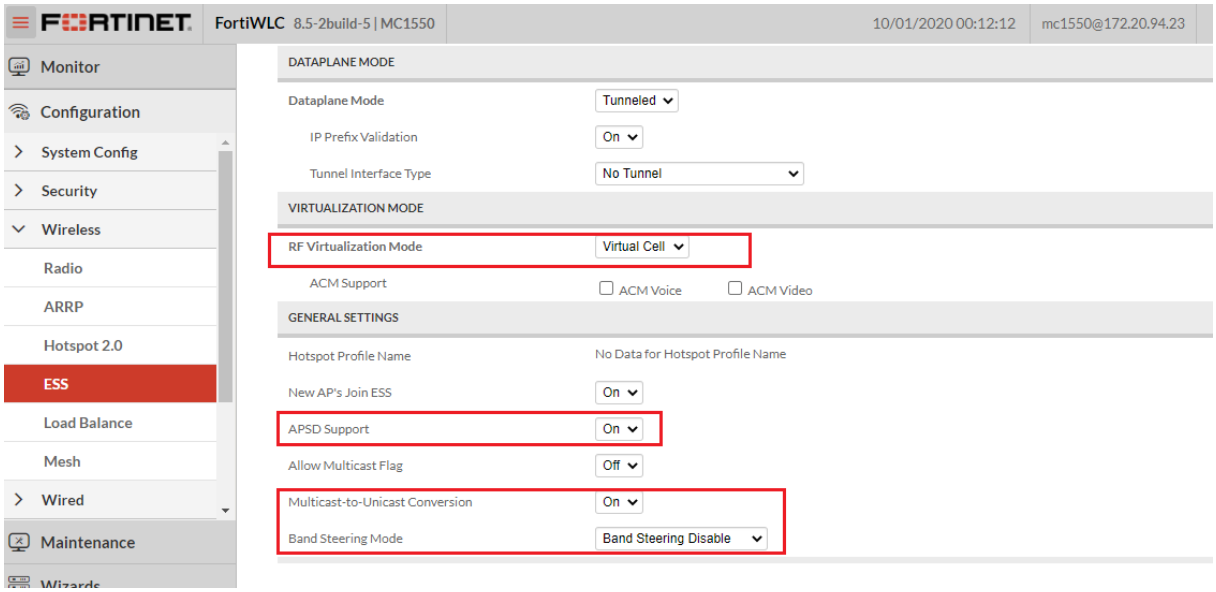
General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac environments (Applicable to Native cell deployments only)

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.**



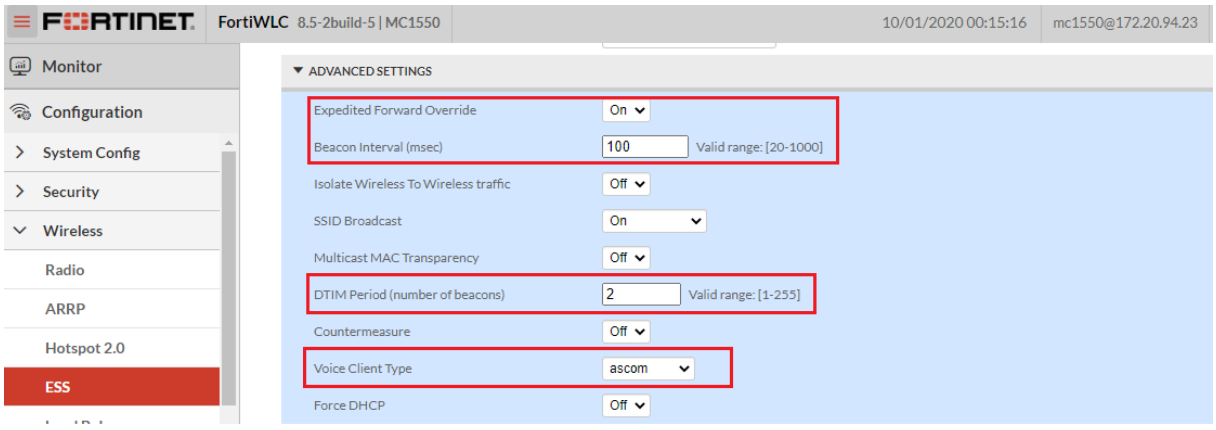
ESS settings.

- Enable corresponding security profile (WPA2PSK)
- Enterprise Mobility Settings: 802.11r and 802.11k are only necessary for Native Cell (multi-channel) deployments. See known limitations for additional information regarding AP1000.



ESS settings (continued).

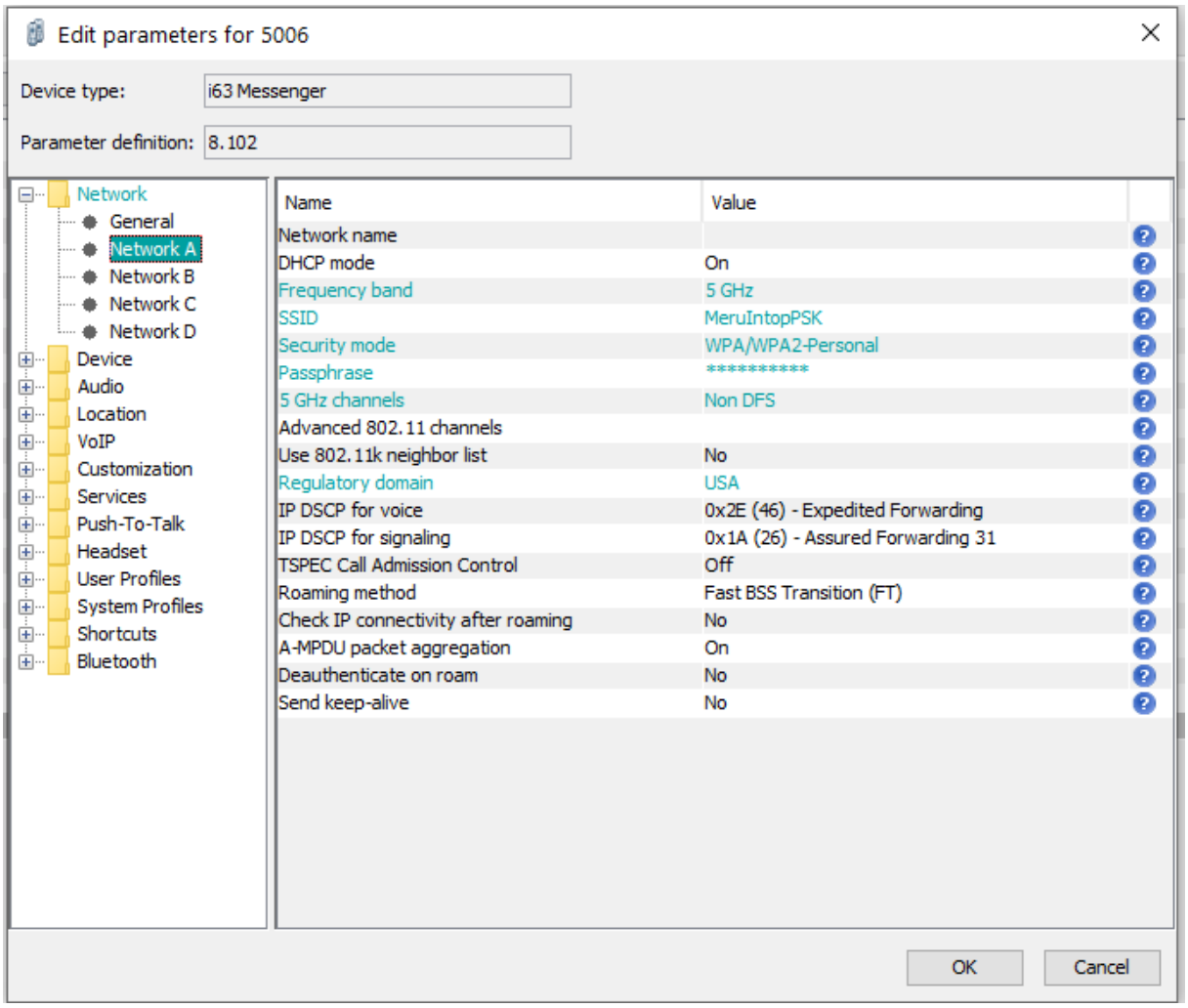
- Select preferred RF Virtualization mode. Ascom support both Native cell and Virtual cell.
- Make sure APSD support is enabled.
- Make sure band steering is disabled
- Make sure Multicast-to-Unicast Conversion is enabled



ESS advanced settings

- Ascom recommends a DTIM period of at least 2 but no higher than 5 and a DTIM interval of 100ms. These values are recommended in order to allow maximum battery conservation without impacting the quality.
- Expedited Forwarding Override will map DSCP 46 (EF) to the AC_VO.
- Select Voice Client Type - ascom

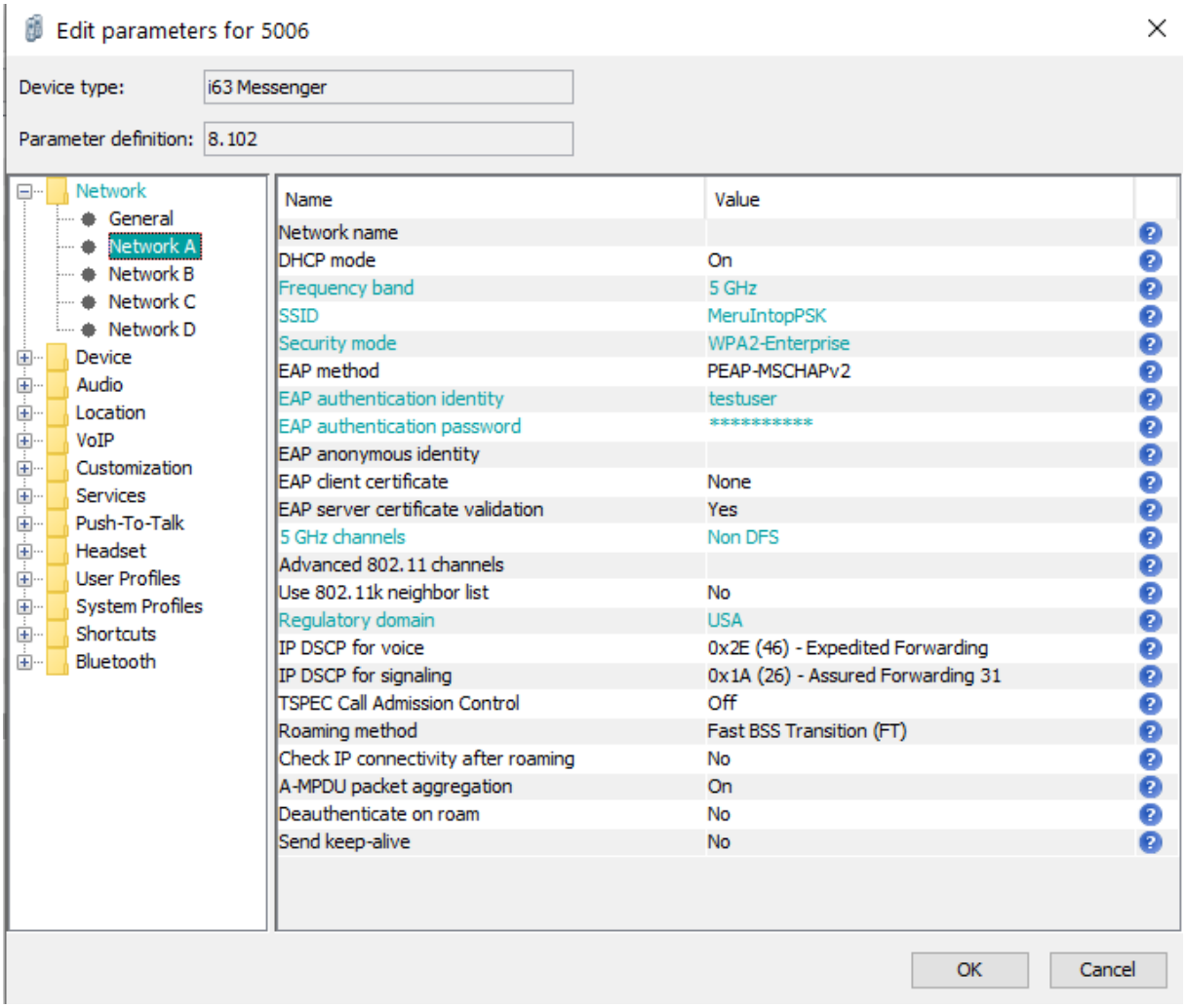
Ascom i63



Network settings for WPA2-PSK

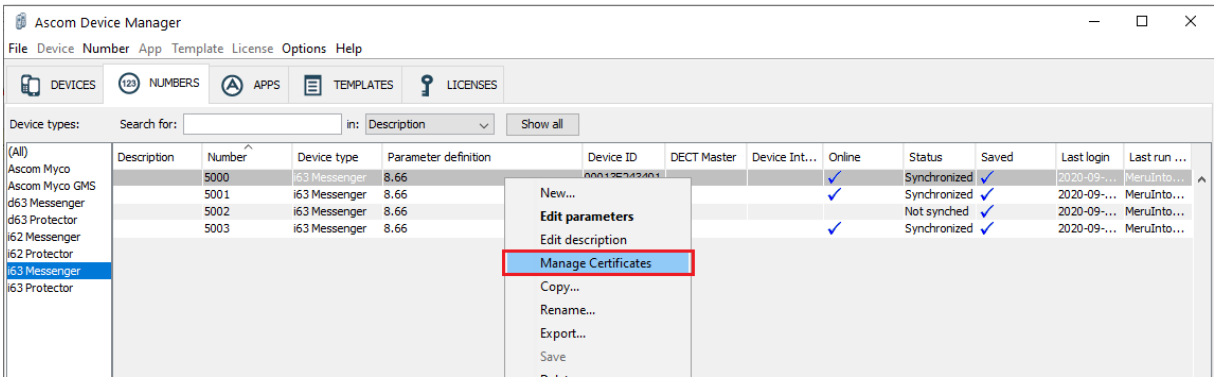
Make sure that the enabled channels in the i63 handset match the channel plan used in the system. For Virtual Cell/Single channel deployments it might only be necessary to specify 1 channel in the i63

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)

Make sure that the enabled channels in the i63 handset match the channel plan used in the system. For Virtual Cell/Single channel deployments it might only be necessary to specify 1 channel in the i63



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

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

Appendix B: Interoperability Verification Records

Pass	20
Fail	0
Comments	1
Not verified	4
Total	25

Refer to the attached file for detailed verification results.

Refer to the verification specification for explicit information regarding each verification 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	06-April-21	SEKMO	Draft
P2	03-June-21	SEKMO	Updates after test with i63 v. 3.0.0
R1	15-june-21	SEKMO	Corrections after review.