

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

# Contents

- Introduction..... 3**
  - About Ascom..... 3
  - About Fortinet..... 3
- Site Information..... 4**
  - Verification site..... 4
  - Participants ..... 4
  - Verification topology..... 4
- Summary ..... 5**
  - General conclusions ..... 5
  - Verification overview ..... 6
  - Known limitations.....7
- Appendix A: Verification Configurations..... 8**
  - Fortinet MC1550 WLAN Controller version 8.5-2-5..... 8
  - Ascom i63 .....14
- Appendix B: Interoperability Verification Records .....16**
- Document History .....16**

# Introduction

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

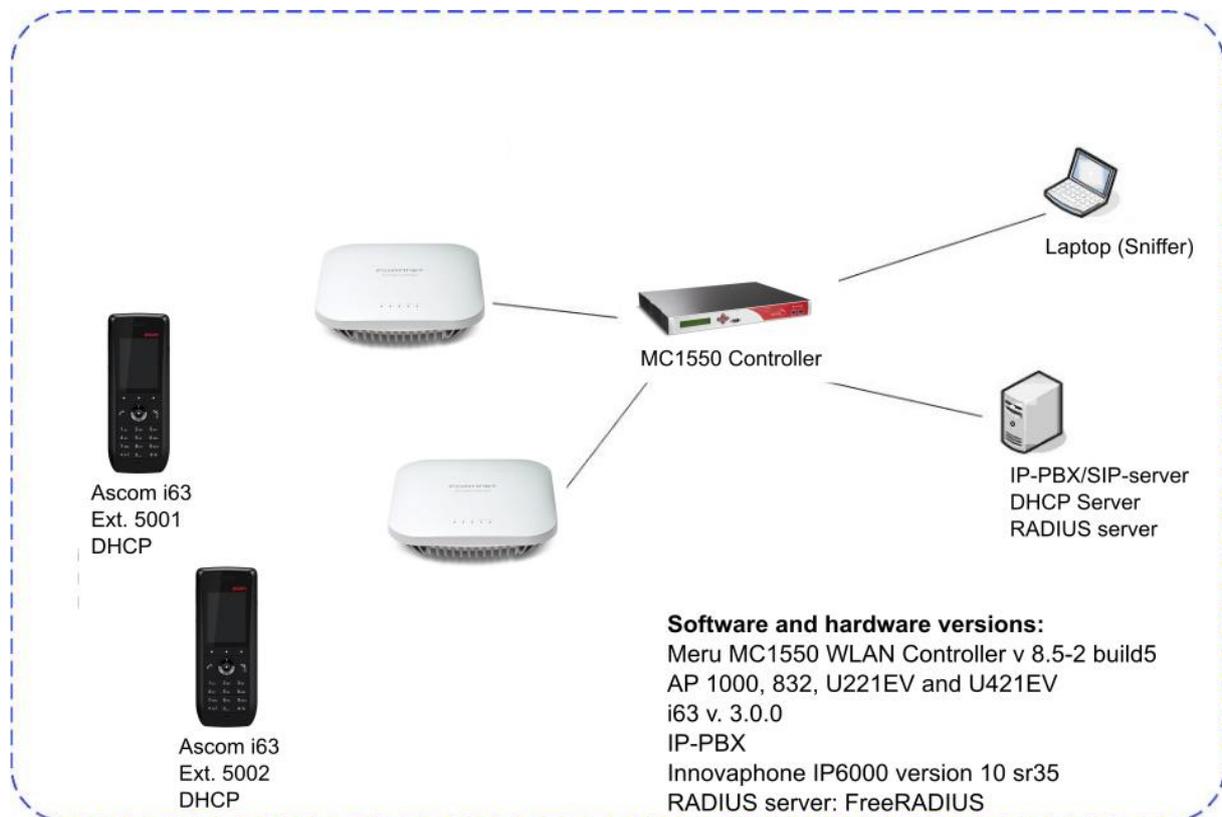
## Verification site

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
<p>RF Virtualization Mode considerations.</p> <ul style="list-style-type: none"> <li>- Virtual Cell mode (single-channel): Supported with all tested AP models</li> <li>- Native cell mode (multi-channel) with PSK authentication: Supported with all tested AP models using 802.11r/FT</li> <li>- Native cell mode (multi-channel) with EAP authentication: Not supported with AP 1000 series*</li> </ul> <p>*AP1000 have no support for OKC or 802.11r/FT hence making roaming times unacceptable long for voice applications.</p>		
<p>802.11k is not supported with AP1000 series access points. Applicable for Native cell mode (multi-channel) only.</p>	<p>Setting “Use 802.11k neighbor list” needs to be set to NO</p>	
<p>WPA3-SAE (PSK): Known problems with i63. Refer to i63 release note</p> <p>WPA3-Enterprise: Not supported by Fortinet WLC.</p>	<p>Use WPA2</p>	

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 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

The screenshot shows the Fortinet FortiWLC interface for a FortiWLC 8.5-2build-5 MC1550. The left sidebar shows the navigation menu with 'ESS' selected under the 'Wireless' section. The main content area displays 'ESS Profiles (3 entries)' with a table of configurations. The table has columns for ESS Profile, Enable/Disable, SSID, Security Profile, EsId Type, SSID Broadcast, Tunnel Interface Type, Dataplane Mode, Owner, 802.11r, 802.11r Group, Client Idle Timeout, and VHT 1024 QAM Support. Three profiles are listed: Merulntop, MerulntopPSK, and Merulntop1x, all with 'Enable' status and 'WPA2dot1x' security profile.

ESS Profile	Enable/Disable	SSID	Security Profile	EsId Type	SSID Broadcast	Tunnel Interface Type	Dataplane Mode	Owner	802.11r	802.11r Group	Client Idle Timeout	VHT 1024 QAM Support
Merulntop	Enable	Merulntop	default	Regular	On	No Tunnel	Tunneled	controller	Off	7	400	On
MerulntopPSK	Enable	MerulntopPSK	WPA2PSK	Regular	On	No Tunnel	Tunneled	controller	Off	7	400	On
Merulntop1x	Enable	Merulntop1x	WPA2dot1x	Regular	On	No Tunnel	Tunneled	controller	Off	7	400	On

ESS profiles.

The screenshot shows the 'Security Profiles - Update' configuration page for the 'WPA2PSK' profile. The 'SECURITY SETTINGS' section is highlighted with a red box. It includes fields for 'Online Sign Up' (not-configured), 'Security Mode' (WPA2 PSK/CCMP-AES), 'Psk Profile Name' (No Data for Psk Profile Name), 'Pre-shared Key (Alphanumeric/Hexadecimal)' (masked with dots), and '802.11W - Management Frame Protection' (disable). Other sections include 'CAPTIVE PORTAL SETTINGS' (Captive Portal: Disabled), 'MAC FILTERING SETTINGS' (MAC Filtering: Off), 'FIREWALL SETTINGS' (Firewall Capability: none), and 'GENERAL SETTINGS'.

Security profile WPA2-PSK, AES/CCMP encryption.

Fortinet FortiWLC 8.5-2build-5 | MC1550 10/01/2020 00:01:10 mc1550@172.20.94.23

Monitor Configuration System Config Security Profile RADIUS Captive Portal Multiple PSK Guest Users MAC Filtering WAPI Server VPN Certificates Rogue APs Wireless Wired Policies

### Security Profiles - Update

Profile Name: WPA2dot1x

SECURITY SETTINGS

Online Sign Up	not-configured
Security Mode *	WPA2/CCMP-AES
Primary RADIUS Profile Name	FreeRadius2
Secondary RADIUS Profile Name	No RADIUS
802.1X Network Initiation	On
Tunnel Termination	<input type="checkbox"/> PEAP <input type="checkbox"/> TTLS
PMK Caching	On
Session Timeout(min)	480 Valid range: [0-1440]
Idle Timeout(min)	60 Valid range: [0-1440]
EAP Timeout(second)	30 Valid range: [1-30]
EAP Retries	3 Valid range: [1-3]
Reauthentication	On
802.11W - Management Frame Protection	disable

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.

Fortinet FortiWLC 8.5-2build-5 | MC1550 10/01/2020 00:01:53 mc1550@172.20.94.23 admin

Monitor Configuration System Config Security Profile RADIUS Captive Portal Multiple PSK Guest Users

### RADIUS Profiles (2 entries)

	RADIUS Profile Name	RADIUS IP	RADIUS Port	Remote RADIUS Server	RADIUS Relay AP-ID	MAC Address Delimiter Calling Station	MAC Address Delimiter Called Station	Use Client IP as calling station id	Password Type	Called-Station-ID Type	Owner	RADIUS Server Timeout	RADIUS Server Retries	NAS IP	RADIUS Server with IPSec	IPSec Serve X.509 Name Ident
	FreeRadius	192.168.0.2	1812	Off	0	Hyphen (-)	Hyphen (-)	No	Shared Key	Default	controller	2	3	0	Off	*
	FreeRadius2	172.20.94.2	1812	Off	0	Hyphen (-)	Hyphen (-)	No	Shared Key	Default	controller	2	3	0	Off	*

Configuration of Radius profile.

Fortinet FortiWLC 8.5-2build-5 | MC1550 10/01/2020 00:02:14 mc1550@172.20.94.2

Monitor Configuration

- System Config
- Security
  - Profile
  - RADIUS**
  - Captive Portal
  - Multiple PSK
  - Guest Users
  - MAC Filtering
  - WAPI Server
  - VPN
  - Certificates
  - Rogue APs
- Wireless
- Wired
- Policies
- Maintenance

### RADIUS Profiles - Update ?

Profile Name	FreeRadius2
RADIUS IP/Name	172.20.94.2

Description	<input type="text"/>	Enter 0-128 chars.
RADIUS Secret	<input type="password" value="....."/>	Enter 1- 64 chars.
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]
Remote RADIUS Server	<input type="button" value="Off"/>	
RADIUS Relay AP-ID	<input type="button" value="No Relay AP"/>	
MAC Address Delimiter Calling Station	<input type="button" value="Hyphen (-)"/>	
MAC Address Delimiter Called Station	<input type="button" value="Hyphen (-)"/>	
Use Client IP as calling station id	<input type="button" value="No"/>	
Password Type	<input type="button" value="Shared Key"/>	
Called-Station-ID Type	<input type="button" value="Default"/>	
COA	<input type="button" value="On"/>	
RADIUS Server Timeout	<input type="text" value="2"/>	Valid range: [1-20]
RADIUS Server Retries	<input type="text" value="3"/>	Valid range: [1-10]
NAS IP	<input type="text" value="0"/>	Enter IPv6 Address.

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.

The screenshot displays the Fortinet FortiWLC configuration interface for the AP Model FAP-U221EV. The left sidebar shows the navigation menu with 'Radio' selected under the 'Wireless' section. The main configuration area lists various radio parameters and their current settings:

- AP Mode: Service Mode
- Interface Description: ieee80211-28-2 (with a note: Enter 0-256 chars.)
- Administrative Status: Up
- RF Band Selection: 802.11ac
- Primary Channel: 36
- Channel Width: 40 MHz Extension channel above
- MIMO Mode: 2x2
- Short Preamble: Off
- Transmit Power(EIRP): 23
- B/G Protection Mode: Auto
- HT Protection Mode: Off
- 802.11n only mode: Off
- Probe Response Threshold: 15 (Valid range: [0-100])
- Mesh Service Admin Status: Disable
- Transmit Beamforming Support: Disabled
- STBC Support: Off
- DFS Fallback Option: Disable
- DFS Fallback Channel: 36
- DFS Channel Revertive(minutes): 30 (Valid range: [30-1440])
- Set Prob Rsp Assigned Only: Off

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.

Fortinet FortiWLC 8.5-2build-5 | MC1550 10/01/2020 00:08:37 mc1550@172

- Monitor
- Configuration
  - System Config
  - Security
  - Wireless
    - Radio
    - ARRP
    - Hotspot 2.0
    - ESS**
    - Load Balance
    - Mesh
  - Wired
  - Policies
  - Devices
  - Access Control
  - WIPS

SSID Number: 2  
 ESS Profile: MerulntopPSK

Enable/Disable: **Enable**  
 SSID: MerulntopPSK (Enter 0-32 chars.)  
 Security Profile: **WPA2PSK**

ESSID TYPE

Essid Type: Regular  
 Backup ESS Profile: No Backup ESS  
 Timer Profile: No Data for Timer Profile  
 Primary RADIUS Accounting Server: No RADIUS  
 Secondary RADIUS Accounting Server: No RADIUS  
 Accounting Interim Interval (seconds): 3600 (Valid range: [0, 60-36000])  
 Reconnect Primary Server (minutes): 10 (Valid range: [5-60])  
 IPv6 Forwarding:

Enterprise Mobility

802.11r: Off  
 802.11r Group: 7 (Valid range: [1-65535])  
 802.11k: Off  
 BSS Transition: Off  
 Max Idle Period: Off  
 Client Idle Timeout: 400 (Valid range: [60-3600])  
 Direct Mcast Service: Off

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.

The screenshot displays the Fortinet FortiWLC configuration interface. The left-hand navigation menu is expanded to show the 'ESS' (Essential Service Set) settings under the 'Wireless' category. The main configuration area is divided into three sections: 'DATAPLANE MODE', 'VIRTUALIZATION MODE', and 'GENERAL SETTINGS'. In the 'VIRTUALIZATION MODE' section, 'RF Virtualization Mode' is set to 'Virtual Cell'. In the 'GENERAL SETTINGS' section, 'APSD Support' is set to 'On', 'Multicast-to-Unicast Conversion' is set to 'On', and 'Band Steering Mode' is set to 'Band Steering Disable'. Other settings include 'Dataplane Mode' (Tunneled), 'IP Prefix Validation' (On), 'Tunnel Interface Type' (No Tunnel), 'ACM Support' (ACM Voice and ACM Video are unchecked), and 'Hotspot Profile Name' (No Data for Hotspot Profile Name).

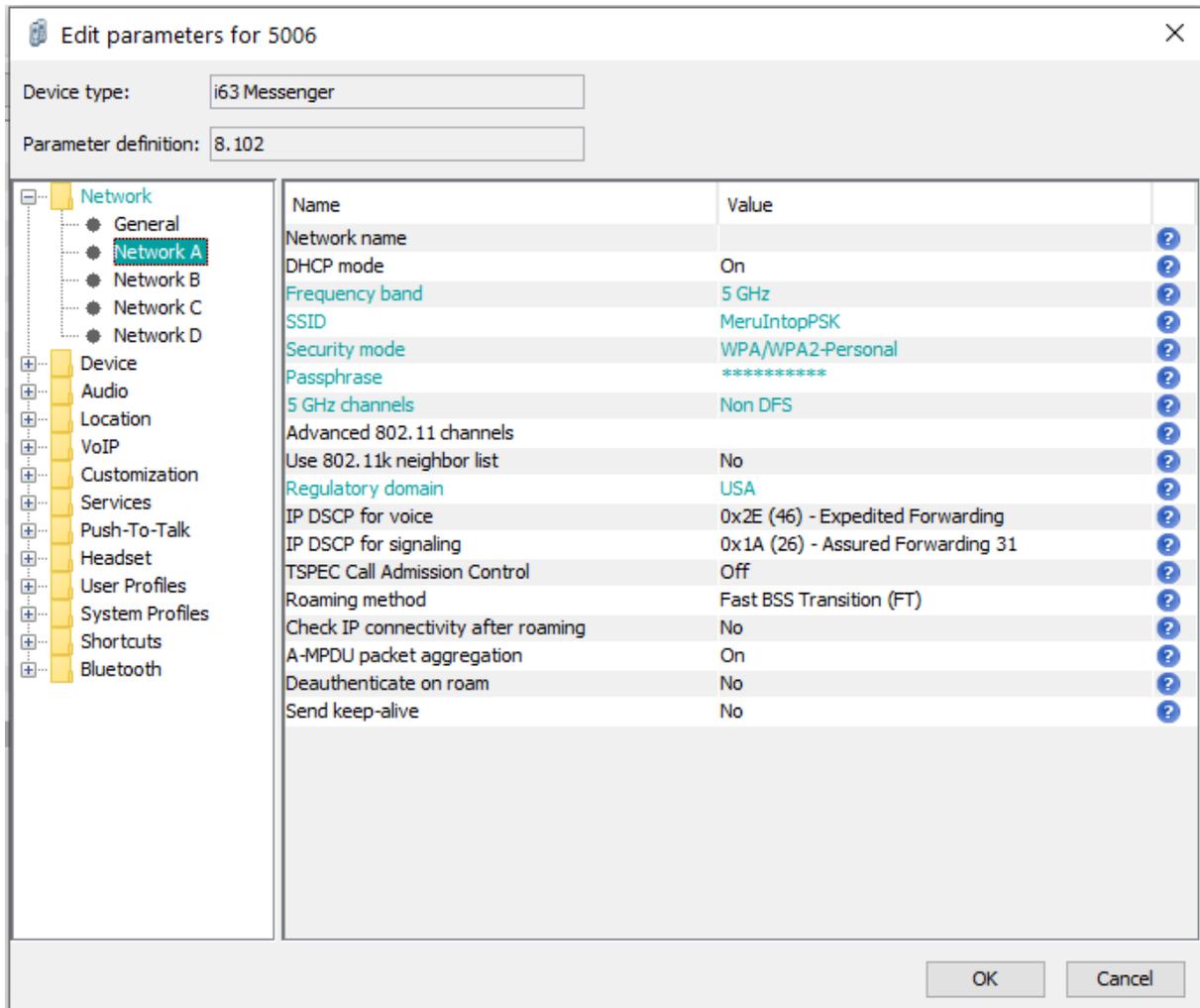
ESS settings (continued).

- 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

The screenshot displays the Fortinet FortiWLC configuration interface, specifically the 'ADVANCED SETTINGS' section for ESS. The left-hand navigation menu is expanded to show the 'ESS' settings. The main configuration area is a light blue panel with several settings: 'Expedited Forward Override' is set to 'On'; 'Beacon Interval (msec)' is set to '100' with a valid range of [20-1000]; 'Isolate Wireless To Wireless traffic' is set to 'Off'; 'SSID Broadcast' is set to 'On'; 'Multicast MAC Transparency' is set to 'Off'; 'DTIM Period (number of beacons)' is set to '2' with a valid range of [1-255]; 'Countermeasure' is set to 'Off'; 'Voice Client Type' is set to 'ascom'; and 'Force DHCP' is set to 'Off'.

ESS advanced settings

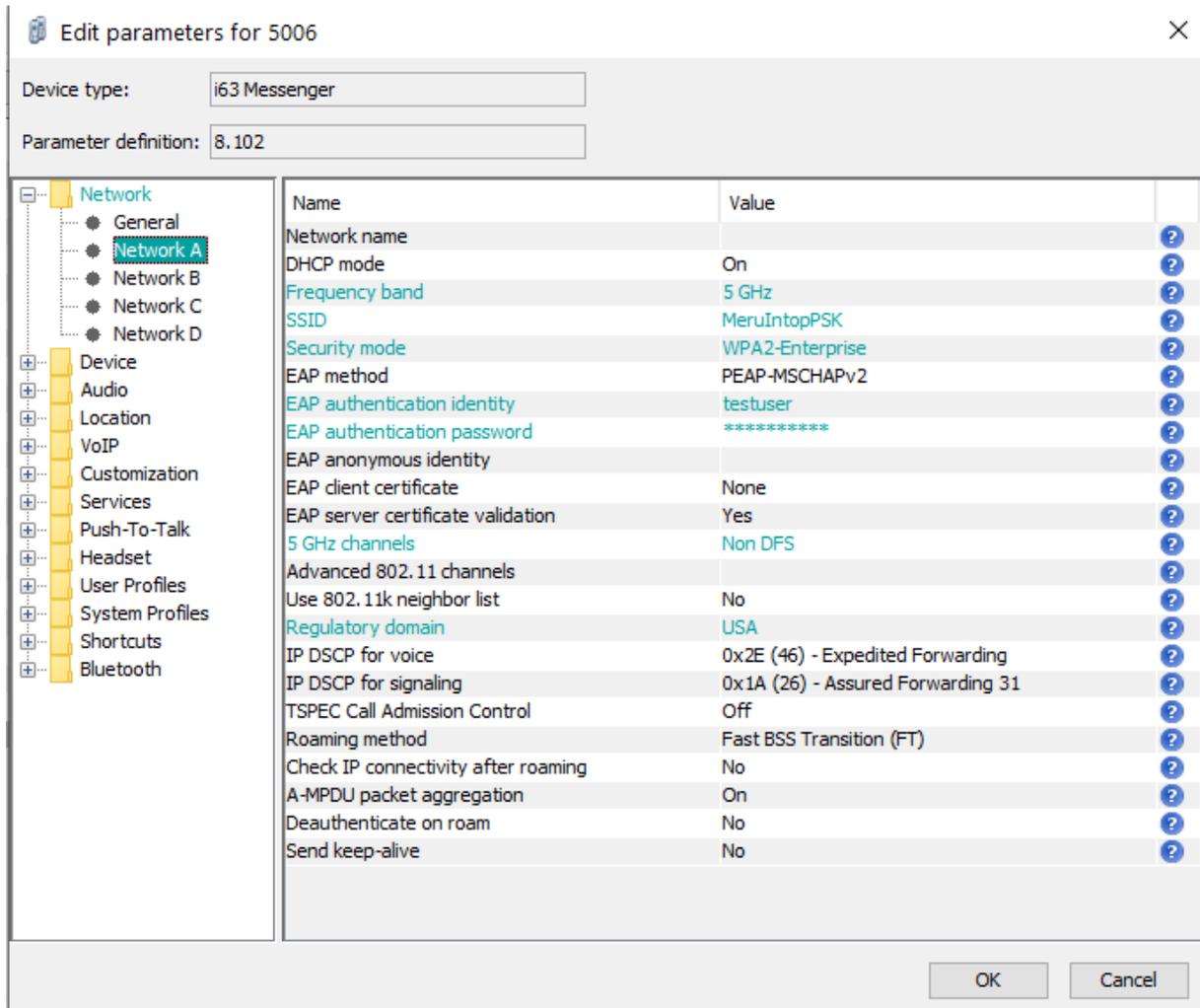
- Ascom recommends a DTIM period of at least 2 but no higher than 5 and a DTIM interval of 100ms. These values are recommended in order to allow maximum battery conservation without impacting the quality.
- Expedited Forwarding Override will map DSCP 46 (EF) to the AC\_VO.
- Select Voice Client Type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



Network settings for WPA2-PSK

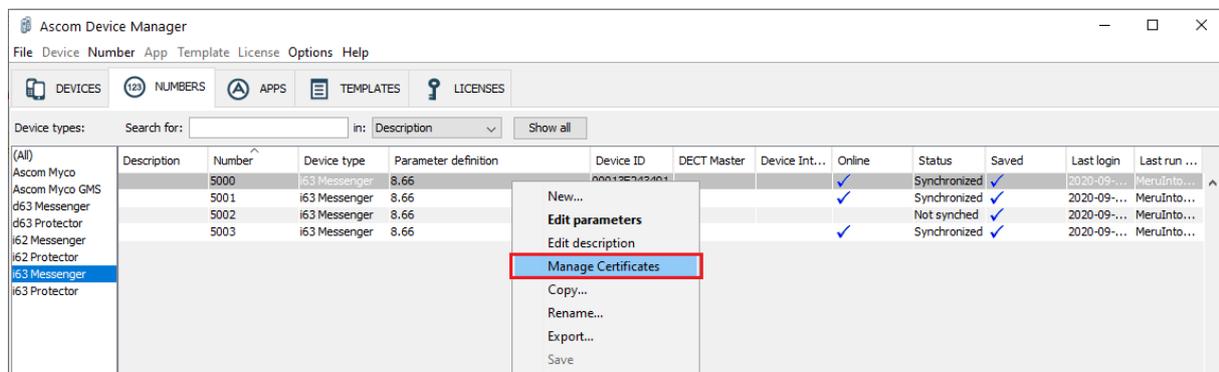
Make sure that the enabled channels in the i63 handset match the channel plan used in the system. For Virtual Cell/Single channel deployments it might only be necessary to specify 1 channel in the i63

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
<b>Total</b>	<b>25</b>

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.