

Ascom i63

Cisco

Catalyst 9800 controller platform

Cisco IOS XE v. 17.3.3

Ascom i63 v. 3.0.0

Morrisville, NC, USA

June 2021

Contents

Introduction.....	3
About Ascom.....	3
About Cisco	3
Site Information.....	4
Verification site.....	4
Participants	4
Verification topology.....	4
Summary	5
General conclusions	5
Compatibility information	5
Verification overview	6
Known limitations.....	7
Appendix A: Validation Configurations	8
Cisco Catalyst 9800 platform Version 17.3.3.....	8
Ascom i63	23
Appendix B: Interoperability Validation Records.....	25
Document History	25

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

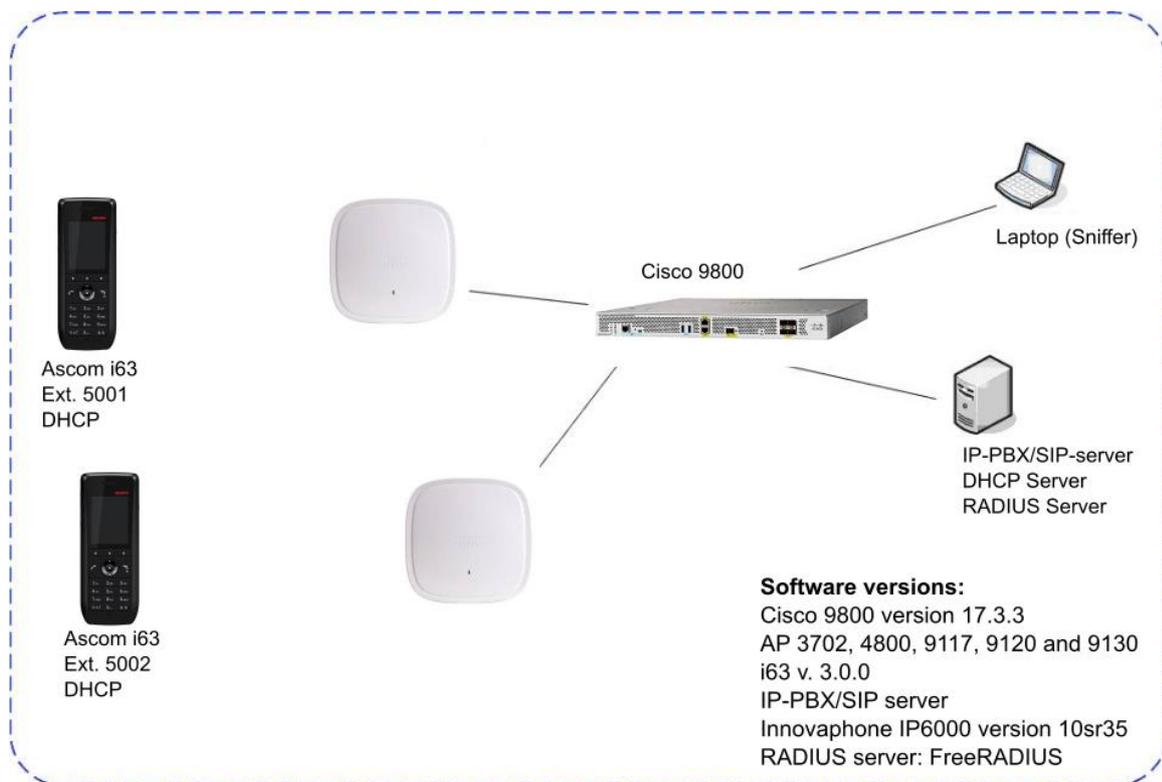
Verification site

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 mostly good results with regards to all test areas including authentication, stability, roaming, QoS and power save related areas. It was however noted that roaming with WPA3 (PSK and Enterprise) did not work to our satisfaction. Refer to Known limitation sections for details.

To maintain roaming performance with WPA2, it is necessary to enable Fast Roaming (FT) both when using PSK and 802.1X based Authentication.

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 17.3.3:

AP1702, 2702, 3702

AP1832, 1852

AP2802, 3802, 4800

AP 9115, 9117, 9120, 9130

Supported Partner Controller Platforms with SW version 17.3.3:

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 with WPA3 SAE (PSK) authentication	OK	Note. problem with roaming
Association with WPA3 Enterprise authentication	OK	Note. problem with roaming
Association, Multiple ESSIDs	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	Typical roaming time 40ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 32ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	NOK	Problem with OKC. 802.11r required.
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 40ms
Roaming, WPA3-PSK Authentication	NOK	Refer to known issues
Roaming, WPA3-Enterprise Authentication	NOK	Refer to known issues
Channel usage controlled by 802.11k	OK	

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
OKC not working as intended resulting in full EAP exchange when roaming.	Use 802.11r/FT with EAP Auth.	
WPA3-PSK and WPA3-Enterprise. Problem with roaming resulting on poor connectivity and audio gaps.	WPA3 is not supported. Use other authentication method such as WPA2.	WH2-3388
Call Admission Control not working in conjunction with 802.11w (Protected Management Frames)	Disable Protected Management Frames in the Cisco WLC if CAC is being used	WH2-2363

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 17.3.3

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 i63. Please note that security settings were modified according to requirements in individual test cases.

WLAN settings

Configuration > Tags & Profiles > WLANs

+ Add × Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID	SSID	Security
<input type="checkbox"/>	+	CiscoIntopPSK9800	1	CiscoIntopPSK9800	[WPA2][PSK][FT + PSK][AES],[FT Enabled]
<input type="checkbox"/>	+	CiscoIntop1X9800	2	CiscoIntop1X9800	[WPA2][802.1x][FT + 802.1x][AES],[FT Enabled]
<input type="checkbox"/>	-	CiscoIntopOPEN9800	3	CiscoIntopOPEN9800	[open]

10 items per page 1 - 3 of 3 items

WLAN overview

WLAN PSK configuration

Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

PSK Format

PSK Type

Pre-Shared Key*

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

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)
- It is strongly recommended to use Fast Transition (802.11r) for enhanced roaming performance
- Select both PSK and FT+PSK for compatibility with i62 and Myco 1 & 2 on the same SSID.

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.

802.1X authentication (PEAP-MSCHAPv2).

Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

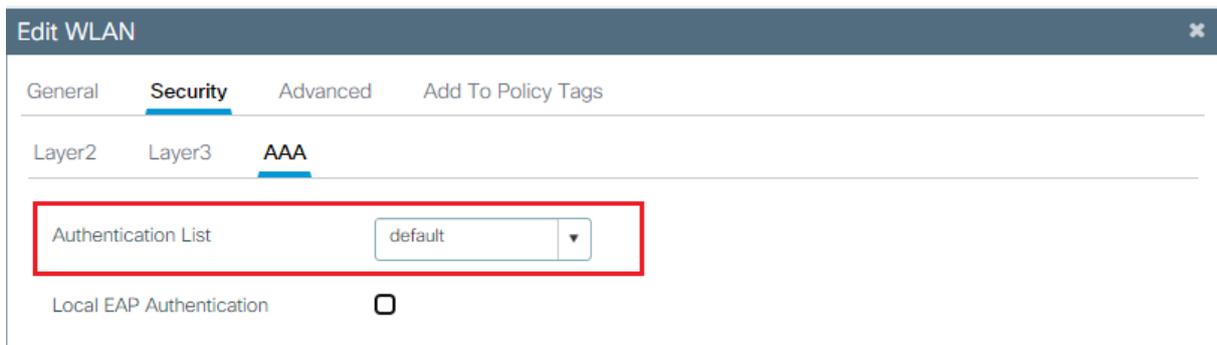
MPSK

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

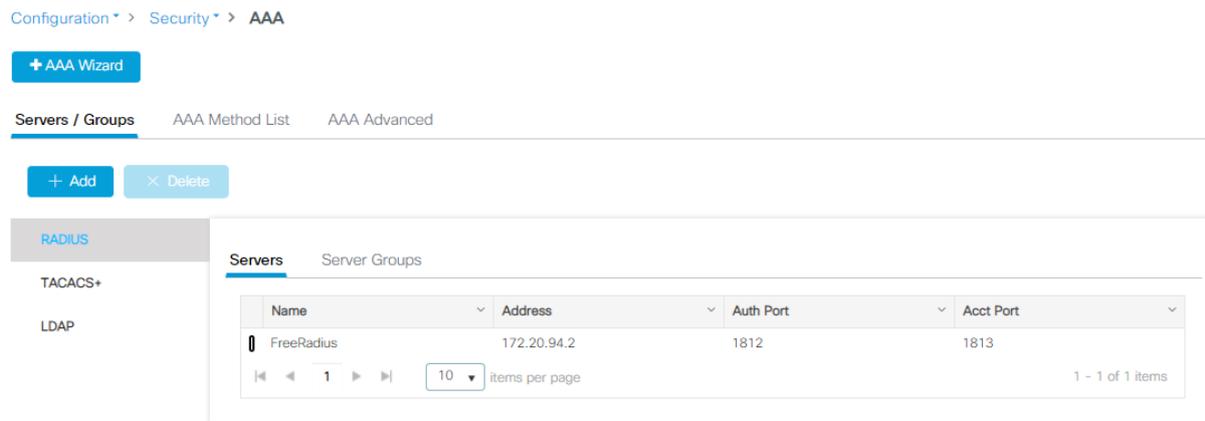
Configuration of authentication using external Radius server, 802.1X. In this example is WPA2-AES used. Select 802.1X as Authentication Key Management.

- Select WPA2 Policy with AES encryption.
- It is mandatory use Fast Transition (802.11r) for acceptable performance when using EAP authentication. See known limitations regarding OKC problem.
- Select both 802.1X and FT + 802.1X for compatibility with i62 and Myco 1 and 2 on the same SSID.

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.



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

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Adva

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Gro

Name

FreeRadius

Edit AAA Radius Server

Name*	FreeRadius
Server Address*	172.20.94.2
PAC Key	<input type="checkbox"/>
Key Type	Clear Text
Key*
Confirm Key*
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

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.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name

default

Type

dot1x

Quick Setup: AAA Authentication

Method List Name*	default
Type*	dot1x
Group Type	group
Fallback to local	<input type="checkbox"/>
Available Server Groups	ldap tacacs+
Assigned Server Groups	radius

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

Per AP Per WLAN

Per AP Radio Per WLAN

11v BSS Transition Support

BSS Transition

Disassociation Imminent(0 to 3000 TBTT)

Optimized Roaming Disassociation Timer(0 to 40 TBTT)

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

Assisted Roaming (11k)

Prediction Optimization

Neighbor List

Dual Band Neighbor List

DTIM Period (in beacon intervals)

5 GHz Band (1-255)

2.4 GHz Band (1-255)

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.
- Make sure 11k – Neighbor list is enabled. (Default settings)
- 11v BSS Transition Support is not supported by Ascom i63 but can be left enabled per default configuration.

Policy and general settings (QoS, Radio)

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add - Delete

Policy Tag Name
<input type="checkbox"/> default-policy-tag

10 items per page

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* default-policy-tag

Description default policy-tag

WLAN-POLICY Maps: 3

+ Add - Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> CiscoIntop1X9800	default-policy-profile
<input type="checkbox"/> CiscoIntopPSK9800	default-policy-profile
<input type="checkbox"/> CiscoIntopOPEN9800	default-policy-profile

10 items per page 1 - 3 of 3 items

Map WLAN and Policy

WLAN Profile* CiscoIntop1X9800 Policy Profile* default-policy-profile

- ✓

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

Configuration > Tags & Profiles > Policy

+ Add - Delete

Status	Policy Profile Name	Description
<input type="checkbox"/> ✓	default-policy-profile	default policy profile

10 items per page 1 - 1 of 1 items

Policy overview

Edit Policy Profile

General Access Policies **QoS and AVC** Mobility Advanced

Auto QoS	None ▼
QoS SSID Policy	
Egress	platinum x ▼
Ingress	platinum-up x ▼
QoS Client Policy	
Egress	AutoQos-4.0-wlan-ET-SSID-Output-policy x ▼
Ingress	AutoQos-4.0-wlan-ET-SSID-Input-AVC-policy x ▼
SIP-CAC	
Call Snooping	<input type="checkbox"/>
Send Disassociate	<input type="checkbox"/>
Send 486 Busy	<input type="checkbox"/>

Flow Monitor IPv4	
Egress	Search or Select ▼
Ingress	Search or Select ▼
Flow Monitor IPv6	
Egress	Search or Select ▼
Ingress	Search or Select ▼

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”

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Fabric Profile

mDNS Service Policy

[Clear](#)

Hotspot Server

User Private Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map

[Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

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

Network Settings and

Configuration > Radio Configurations > Network

5 GHz Band 2.4 GHz Band

General

5 GHz Network Status

⚠ 5 GHz Network is operational. Configuring Beacon Interval, Fragmentation Threshold, DTPC Support will result in loss of connectivity of clients.

Beacon Interval*

Fragmentation Threshold(bytes)*

DTPC Support

Tri-Radio Mode

CCX Location Measurement

Mode

Data Rates

⚠ 5 GHz Network is operational. Configuring Data Rates will result in loss of connectivity of clients.

6 Mbps	Disabled	9 Mbps	Disabled	12 Mbps	Mandatory
18 Mbps	Supported	24 Mbps	Mandatory	36 Mbps	Supported
48 Mbps	Supported	54 Mbps	Supported		

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.

5 GHz Band **2.4 GHz Band**

General

2.4 GHz Network Status

⚠ 2.4 GHz Network is operational. Configuring 802.11g Network Status, Beacon Interval, Short Preamble, Fragmentation Threshold, DTPC Support will result in loss of connectivity of clients.

802.11g Network Status

Beacon Interval*

Short Preamble

Fragmentation Threshold(bytes)*

DTPC Support

CCX Location Measurement

Mode

Data Rates

⚠ 2.4 GHz Network is operational. Configuring Data Rates will result in loss of connectivity of clients.

1 Mbps	Disabled ▼	2 Mbps	Disabled ▼	5.5 Mbps	Disabled ▼
6 Mbps	Disabled ▼	9 Mbps	Disabled ▼	11 Mbps	Disabled ▼
12 Mbps	Mandatory ▼	18 Mbps	Supported ▼	24 Mbps	Supported ▼
36 Mbps	Supported ▼	48 Mbps	Supported ▼	54 Mbps	Supported ▼

Data rates 2.4GHz. The default data rate set will work just fine, however Ascom recommends disabling the lowest data rates and have 12Mbps as lowest data rate.

5 GHz Band 2.4 GHz Band

⚠ 5 GHz Network is operational. Configuring EDCA Profile and DFS Channel Switch Announcement Mode will result in loss of connectivity of clients.

<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">EDCA Parameters</div> <div style="border: 2px solid red; padding: 5px; margin-bottom: 10px;"> EDCA Profile <input type="text" value="optimized-voice"/> </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">DFS (802.11h)</div> <div style="background-color: #fff9c4; padding: 5px; margin-bottom: 10px;"> ⚠ DTPC Support is enabled. Please disable it at Network to configure Power Constraint </div> <div style="border: 2px solid red; padding: 5px; margin-bottom: 10px;"> Power Constraint* <input type="text" value="0"/> Channel Switch Status <input checked="" type="checkbox"/> Channel Switch Announcement Mode <input type="text" value="Loud"/> </div> Smart DFS <input checked="" type="checkbox"/>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">11ax Parameters</div> Target Wakeup Time <input checked="" type="checkbox"/> Target Wakeup Time Broadcast <input checked="" type="checkbox"/> Multiple Bssid <input checked="" type="checkbox"/> BSS Color <input checked="" type="checkbox"/>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 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.

▼ All Access Points

Number of AP(s): 2

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location
AP00A6.CA36.210E	AIR-AP3802I-B-K9	2	✔	172.20.94.86	006b.f155.1820	Local	Registered	default-policy-tag	default-site-tag	default-rf-tag	Default	default location
AP0CD0.F894.1350	C9117AXI-B	2	✔	172.20.94.58	0cd0.f895.00e0	Local	Registered	default-policy-tag	default-site-tag	default-rf-tag	Default	default location

1 - 2 of 2 access points

▼ 5 GHz Radios

Number of AP(s): 2

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Channel	Power Level
AP00A6.CA36.210E	1	006b.f155.1820	✔	✔	default-policy-tag	default-site-tag	default-rf-tag	(149,153)	5/7 (7 dBm)
AP0CD0.F894.1350	1	0cd0.f895.00e0	✔	✔	default-policy-tag	default-site-tag	default-rf-tag	(149,153)	6/8 (8 dBm)

1 - 2 of 2 items

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

Edit Radios 5 GHz Band

Configure Detail

General

AP Name: AP00A6.CA36.210E

Admin Status: **ENABLED**

CleanAir Admin Status: **ENABLED**

Antenna Parameters

Antenna Type: Internal

Antenna Mode: Omni

Antenna A:

Antenna B:

Antenna C:

Antenna D:

Antenna Gain: 10

RF Channel Assignment

Current Channel: 149

Channel Width: 20 MHz

Assignment Method: Custom

Channel Number: 149

Tx Power Level Assignment

Current Tx Power Level: 5

Assignment Method: Custom

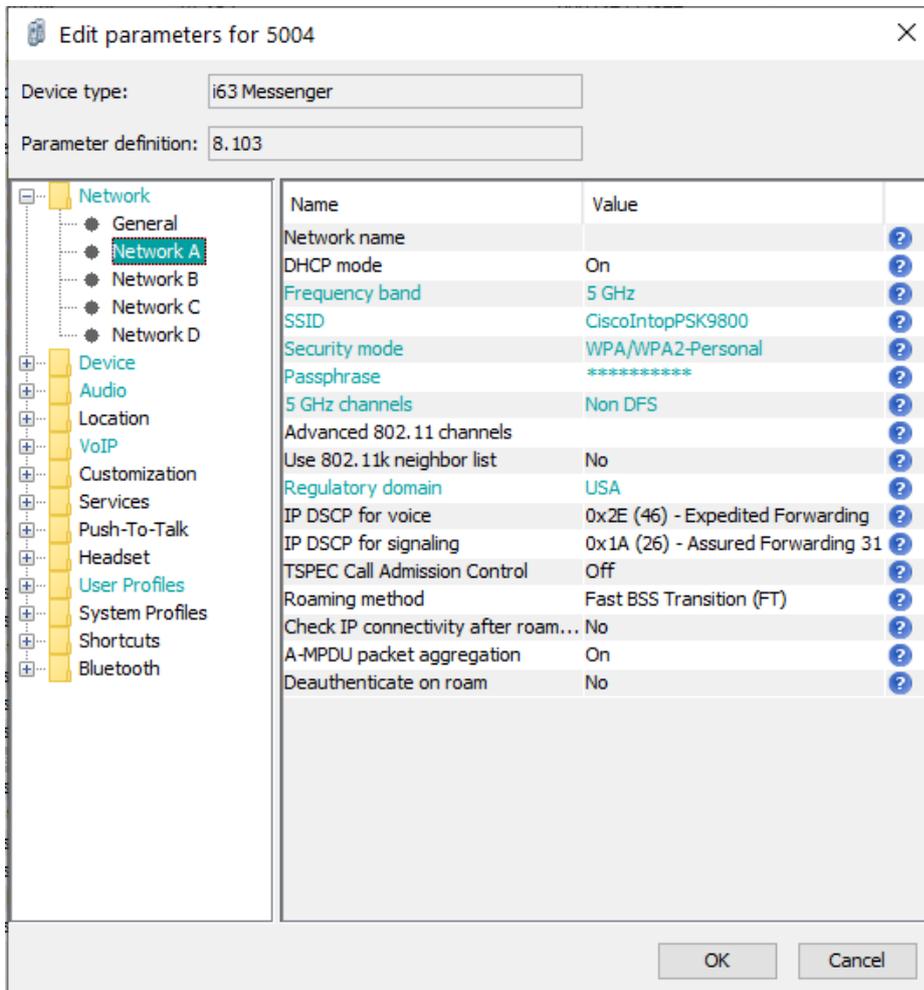
Transmit Power: 5

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.

General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac environments:

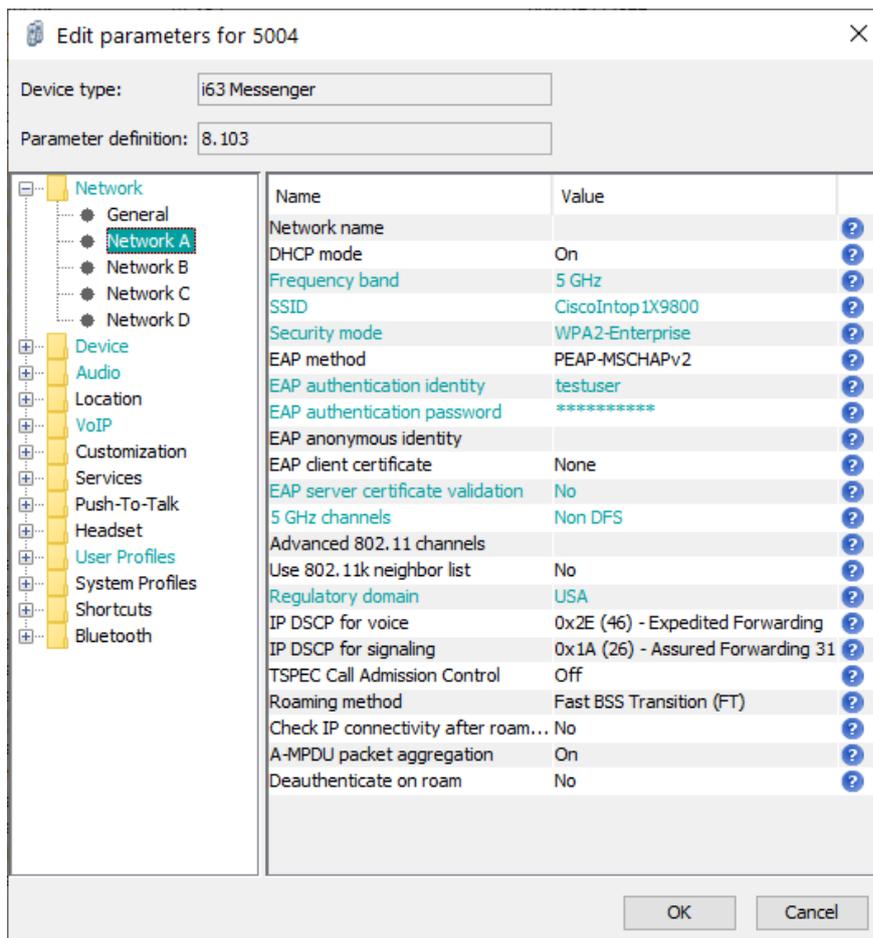
- 1. For environments not utilizing 802.11k Neighbor Report - Enabling more than 8 channels will degrade roaming performance. (In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed) Ascom does not recommend exceeding this limit unless 802.11k is in use.**
- 2. Ascom 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.**



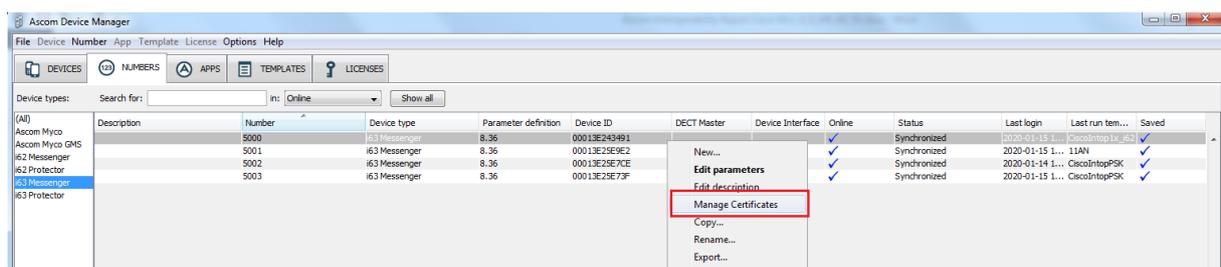
Network settings for WPA2-PSK

Note. Make sure that the enabled channels in the i63 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.

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

Appendix B: Interoperability Validation Records

Pass	22
Fail	3
Comments	3
Not verified	2
Total	30

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	01-June-2021	SEKMO	Draft
R1	15-June-2021	SEKMO	Adjustments after review. Revision R1