

Ascom i63

Cisco

Catalyst 9800 controller platform

Cisco IOS XE v. 17.9.3

Ascom i63 v. 4.0.0

Utrecht, The Netherlands

June 2023

# Contents

<b>Introduction</b> .....	<b>3</b>
<b>Site Information</b> .....	<b>4</b>
Test site .....	4
Participants .....	4
Test topology .....	4
<b>Summary</b> .....	<b>5</b>
General conclusions .....	5
Compatibility information .....	5
Verification overview .....	6
Known limitations.....	7
<b>Appendix A: Validation Configurations</b> .....	<b>8</b>
Cisco Catalyst 9800 platform Version 17.9.3.....	8
Ascom i63 .....	23
<b>Appendix B: Interoperability Validation Records</b> .....	<b>25</b>
<b>Document History</b> .....	<b>25</b>

# Introduction

This document describes a summary of the interoperability validation results of the Ascom and Cisco platform, furthermore it provides the necessary steps and guidelines to optimally configure the respective platforms. This report should be used in conjunction with configuration guides from both Cisco and Ascom.

## 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](https://thenetwork.cisco.com) and follow us on Twitter at @Cisco.

# Site Information

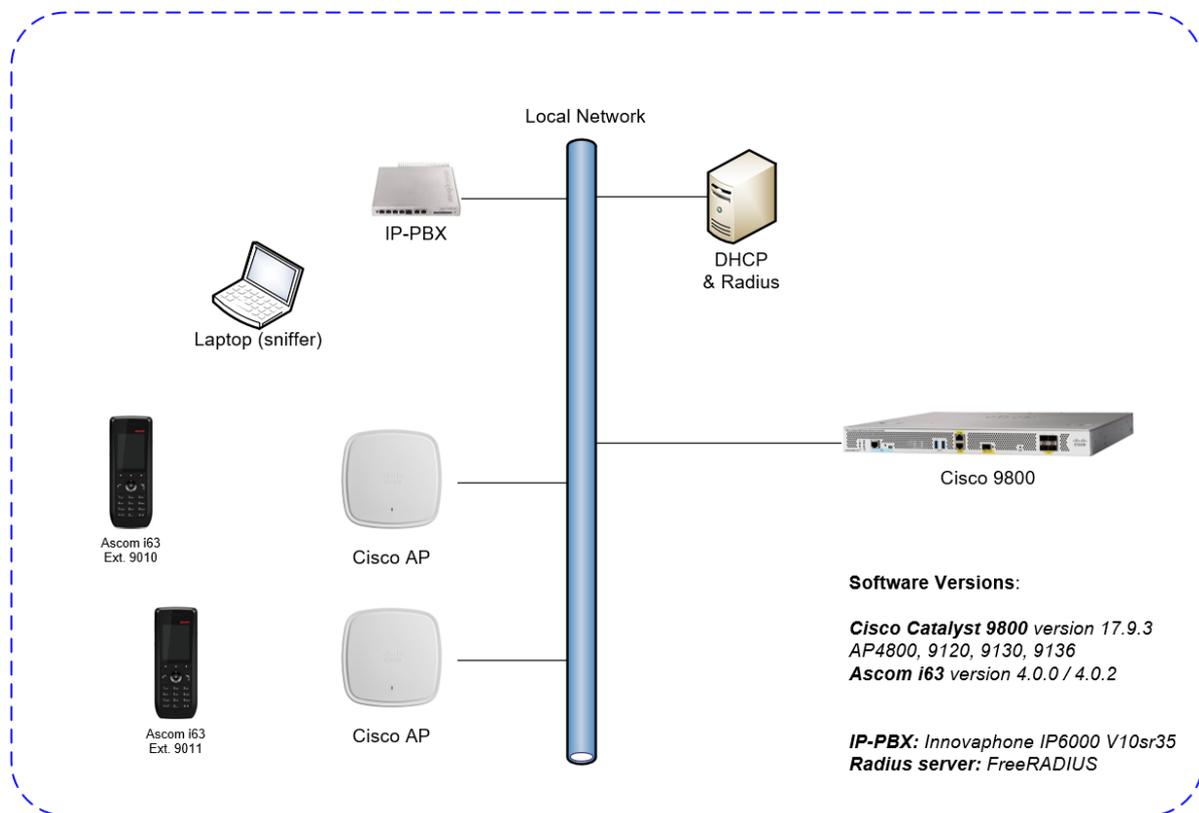
## Test site

Ascom Nederland  
Orteliuslaan 982  
3528 BD Utrecht  
The Netherlands

## Participants

Remco van den Pangaart, Ascom, Nederland

## Test topology



# Summary

## General conclusions

This Ascom interoperability validation produced good results with regard to the tested areas of authentication, stability, roaming, QoS and power save. WPA3 (Personal and Enterprise) was left out of the test due to known issues.

To maintain optimal 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 4800, 9120, 9130 and 9136). By testing these access points we are considered to cover all supported major Cisco access points based on chipset compatibility listed below.

### Supported Partner Access Points with SW version 17.9.3:

AP1832, 1852

AP2802, 3802, 4800

AP 9115, 9117, 9120, 9130, 9136

### Supported Partner Controller Platforms with SW version 17.9.3:

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, 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 51ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 26ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 40ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 36ms
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

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 Validation Records.

# Appendix A: Validation Configurations

## Cisco Catalyst 9800 platform Version 17.9.3

In the following chapter you will find screenshots and explanations of basic settings 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 x 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]

1 - 3 of 3 items

10 items per page

### 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.

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

## WLAN 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

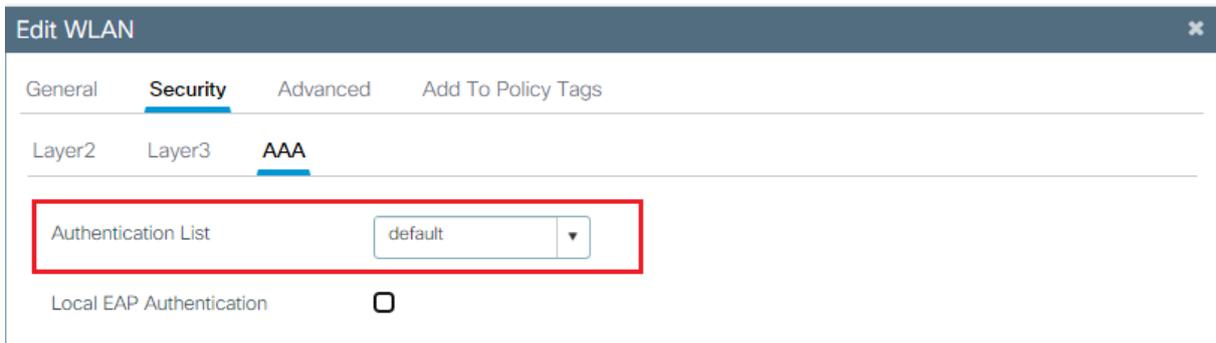
MPSK

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

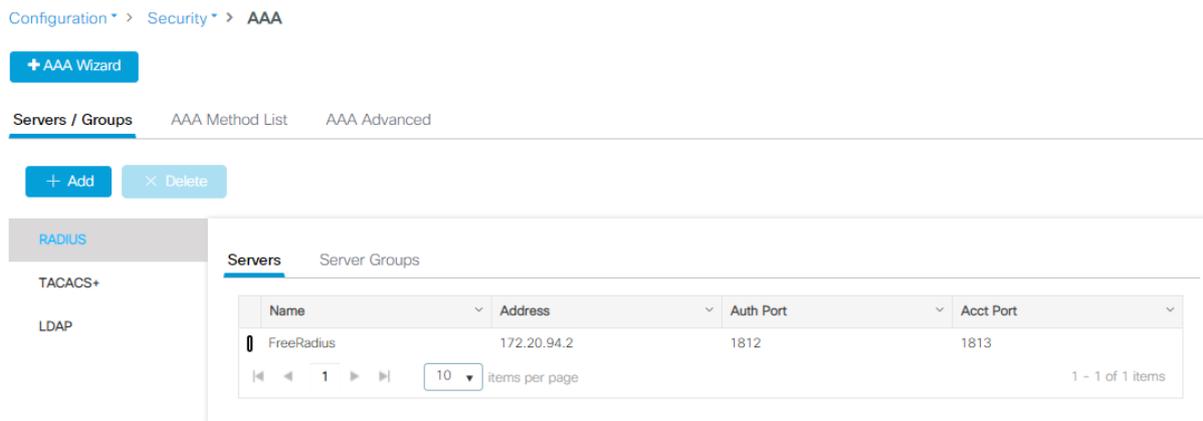
Configuration of authentication using external Radius server, 802.1X. In this example is WPA2-AES used. Select 802.1X as Authentication Key Management.

- Select WPA2 Policy with AES encryption.
- It is strongly recommended to use Fast Transition (802.11r) for enhanced roaming performance.
- Select both 802.1X and FT + 802.1X for compatibility with i62 and Myco 1 and 2 on the same SSID.

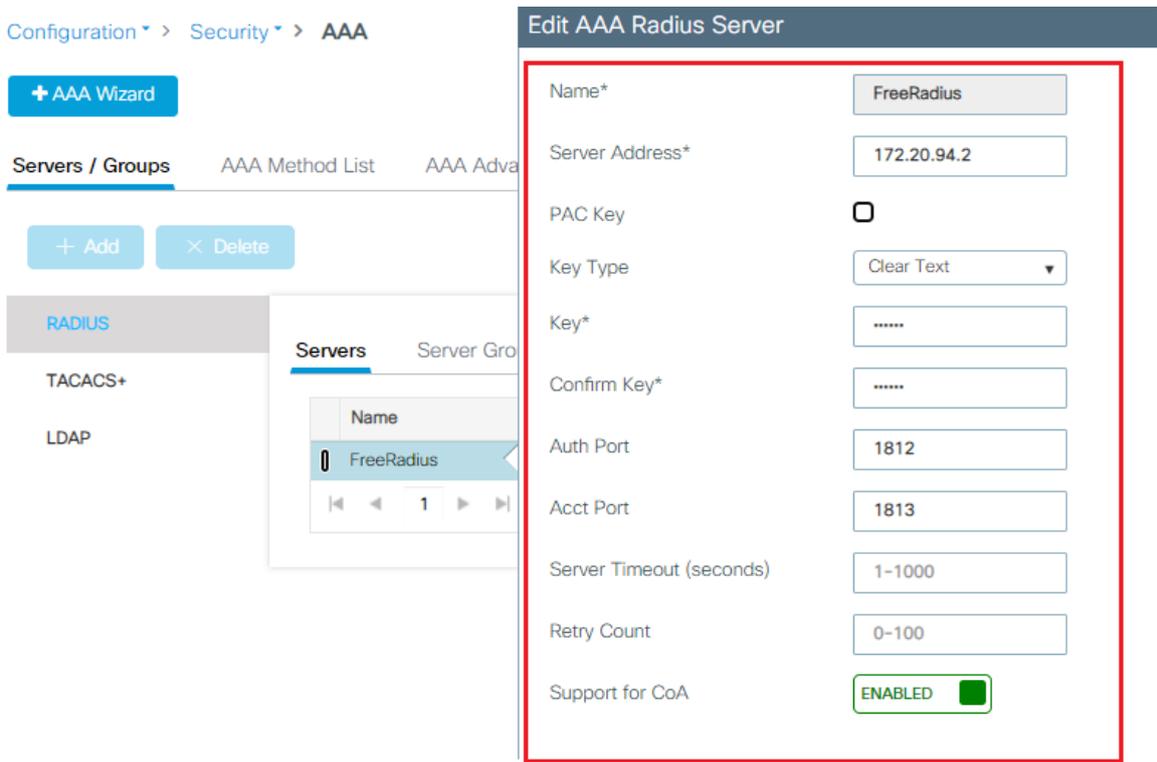
Compatibility Note: 802.11r is not supported by Ascom i62 and Myco 1 & 2 but the devices have no problem operating on a SSIDs where 802.11r (FT) is advertised in conjunction with a legacy method.



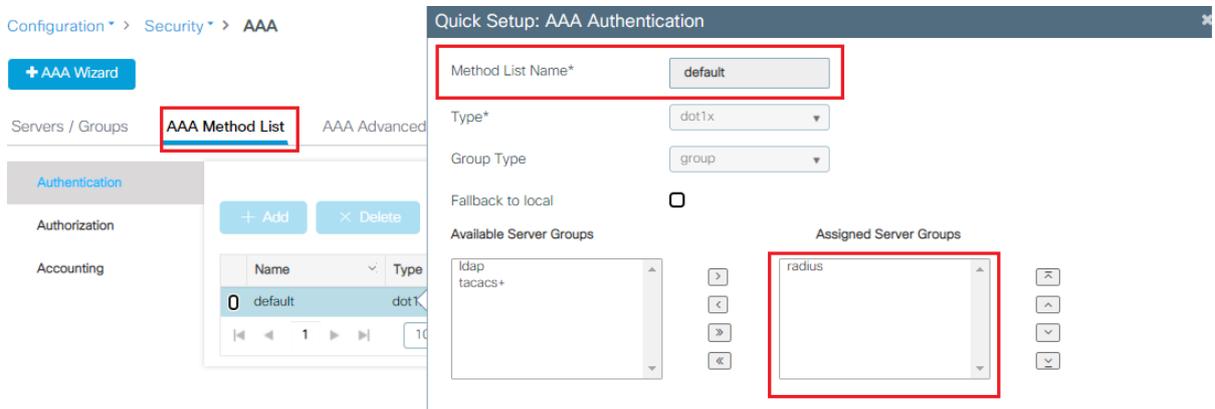
Example of authentication configuration using external Radius server. Select the Authentication list. The server is configured under tab Security/Radius. See configuration of server below.



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 <input checked="" type="checkbox"/>	Universal Admin <input type="checkbox"/>
Aironet IE <input type="checkbox"/>	OKC <input checked="" type="checkbox"/>
Advertise AP Name <input type="checkbox"/>	Load Balance <input type="checkbox"/>
P2P Blocking Action <input type="text" value="Disabled"/>	Band Select <input type="checkbox"/>
Multicast Buffer <input type="text" value="DISABLED"/>	IP Source Guard <input type="checkbox"/>
Media Stream Multicast-direct <input type="checkbox"/>	WMM Policy <input type="text" value="Required"/>
11ac MU-MIMO <input checked="" type="checkbox"/>	mDNS Mode <input type="text" value="Bridging"/>
WiFi to Cellular Steering <input type="checkbox"/>	<b>Off Channel Scanning Defer</b>
Fastlane+ (ASR) <input checked="" type="checkbox"/>	Defer Priority <input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2
Deny LAA (RCM) clients <input type="checkbox"/>	<input type="checkbox"/> 3 <input type="checkbox"/> 4 <input checked="" type="checkbox"/> 5
6 GHz Client Steering <input type="checkbox"/>	<input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7
<b>Max Client Connections</b>	Scan Defer Time <input type="text" value="100"/>
Per WLAN <input type="text" value="0"/>	<b>Assisted Roaming (11k)</b>
Per AP Per WLAN <input type="text" value="0"/>	Prediction Optimization <input type="checkbox"/>
Per AP Radio Per WLAN <input type="text" value="200"/>	Neighbor List <input checked="" type="checkbox"/>
<b>11v BSS Transition Support</b>	Dual Band Neighbor List <input type="checkbox"/>
BSS Transition <input checked="" type="checkbox"/>	<b>DTIM Period (in beacon intervals)</b>
Dual Neighbor List <input type="checkbox"/>	5 GHz Band (1-255) <input type="text" value="2"/>
BSS Max Idle Service <input checked="" type="checkbox"/>	2.4 GHz Band (1-255) <input type="text" value="2"/>
BSS Max Idle Protected <input type="checkbox"/>	<b>Device Analytics</b>
Directed Multicast Service <input checked="" type="checkbox"/>	Advertise Support <input checked="" type="checkbox"/>
<i>Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only</i>	Advertise PC Analytics Support <input checked="" type="checkbox"/>
<b>11ax</b>	Share Data with Client <input type="checkbox"/>
Enable 11ax <input checked="" type="checkbox"/>	<b>11k Beacon Radio Measurement</b> <i>Client Scan Report</i>
Downlink OFDMA <input checked="" type="checkbox"/>	On Association <input type="checkbox"/>
Uplink OFDMA <input checked="" type="checkbox"/>	On Roam <input type="checkbox"/>
Downlink MU-MIMO <input checked="" type="checkbox"/>	
Uplink MU-MIMO <input checked="" type="checkbox"/>	
BSS Target Wake Up Time <input type="checkbox"/>	

- 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

1 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

1 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

1 10 items per page 1 - 1 of 1 items

Policy overview

## Edit Policy Profile

General

Access Policies

**QoS and AVC**

Mobility

Advanced

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

<b>Flow Monitor IPv4</b>	
Egress	Search or Select ▼
Ingress	Search or Select ▼
<b>Flow Monitor IPv6</b>	
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”.

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

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

**WLAN Timeout**

Session Timeout (sec)	<input type="text" value="86400"/>	ⓘ
Idle Timeout (sec)	<input type="text" value="43200"/>	
Idle Threshold (bytes)	<input type="text" value="0"/>	
Client Exclusion Timeout (sec)	<input type="checkbox"/> <input type="text" value="60"/>	
Guest LAN Session Timeout	<input type="checkbox"/>	

**DHCP**

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

Show more >>>

**AAA Policy**

Allow AAA Override	<input type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input type="text" value="default-aaa-policy x"/>
Accounting List	<input type="text" value="Search or Select"/>

**WGB Parameters**

Broadcast Tagging	<input type="checkbox"/>
WGB VLAN	<input type="checkbox"/>

**Policy Proxy Settings**

ARP Proxy	<input type="checkbox"/> DISABLED
IPv6 Proxy	<input type="text" value="None"/>

Fabric Profile	<input type="checkbox"/> <input type="text" value="Search or Select"/>
Link-Local Bridging	<input type="checkbox"/>
mDNS Service Policy	<input type="text" value="default-mdns-ser..."/>
Hotspot Server	<input type="text" value="Search or Select"/>

**User Defined (Private) Network**

Status	<input type="checkbox"/>
Drop Unicast	<input type="checkbox"/>

**DNS Layer Security**

DNS Layer Security Parameter Map	<input type="text" value="Not Configured"/>
Flex DHCP Option for DNS	<input checked="" type="checkbox"/> ENABLED
Flex DNS Traffic Redirect	<input type="checkbox"/> IGNORE

**WLAN Flex Policy**

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input type="text" value="Search or Select"/>

**Air Time Fairness Policies**

2.4 GHz Policy	<input type="text" value="Search or Select"/>
5 GHz Policy	<input type="text" value="Search or Select"/>

**EoGRE Tunnel Profiles**

Tunnel Profile	<input type="text" value="Search or Select"/>
----------------	---

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

## 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	<input type="text" value="Disabled"/>	9 Mbps	<input type="text" value="Disabled"/>	12 Mbps	<input type="text" value="Mandatory"/>
18 Mbps	<input type="text" value="Supported"/>	24 Mbps	<input type="text" value="Mandatory"/>	36 Mbps	<input type="text" value="Supported"/>
48 Mbps	<input type="text" value="Supported"/>	54 Mbps	<input type="text" value="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 having 12Mbps as lowest data rate.

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

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p><b>EDCA Parameters</b></p> <p>EDCA Profile <span style="border: 1px solid red; padding: 2px;">optimized-voice ▼</span></p> <p>Client Load Based Configuration <span style="border: 1px solid green; padding: 2px;">ENABLED <input checked="" type="checkbox"/></span></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p><b>DFS (802.11h)</b></p> <p>⚠ DTPC Support is enabled. Please disable it at <a href="#">Network</a> to configure Power Constraint</p> </div> <div style="border: 1px solid red; padding: 5px;"> <p>Power Constraint* <span style="border: 1px solid #ccc; padding: 2px;">0</span></p> <p>Channel Switch Status <input checked="" type="checkbox"/></p> <p>Channel Switch Announcement Mode <span style="border: 1px solid #ccc; padding: 2px;">Loud ▼</span></p> </div> <p>Smart DFS <input checked="" type="checkbox"/></p>	<div style="border: 1px solid #ccc; padding: 5px;"> <p><b>11ax Parameters</b></p> <p>Target Wakeup Time <input type="checkbox"/></p> <p>Target Wakeup Time Broadcast <input type="checkbox"/></p> <p>Multiple Bssid <input checked="" type="checkbox"/></p> <p>BSS Color <input type="checkbox"/></p> <p>OBSS PD <input type="checkbox"/></p> <p>Non-SRG OBSS PD Max Threshold (dBm)* <span style="border: 1px solid #ccc; padding: 2px;">-62</span></p> <p>SRG OBSS PD <input type="checkbox"/></p> <p>SRG OBSS PD Min Threshold (dBm)* <span style="border: 1px solid #ccc; padding: 2px;">-82</span></p> <p>SRG OBSS PD Max Threshold (dBm)* <span style="border: 1px solid #ccc; padding: 2px;">-62</span></p> </div>
---	---

- 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

Misconfigured APs  
Tag : 0    Country Code : 0    LSC Fallback : 0

Total APs : 2

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Operation Status	Cont Stat
AP4C77.6D9E.61FA	AIR-AP4800-B-K9	3	✔	0 days 1 hrs 12 mins 3 secs	172.20.94.82	7069.5a51.5840	4c77.6d9e.61fa	Local	Registered	Heal
APD4E8.8019.5228	C9120AXI-B	2	✔	0 days 20 hrs 16 mins 15 secs	172.20.94.69	d4e8.8019.bd40	d4e8.8019.5228	Local	Registered	Heal

10 items per page

> 6 GHz Radios

▼ 5 GHz Radios

Total 5 GHz radios : 2

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Channel	Power Level
AP4C77.6D9E.61FA	1	7069.5a51.5840	✔	✔	default-policy-tag	default-site-tag	default-rf-tag	(149,153)	6/8 (8 dBm)
APD4E8.8019.5228	1	d4e8.8019.bd40	✔	✔	default-policy-tag	default-site-tag	default-rf-tag	(44,48)	5/8 (10 dBm)

Access points and channel overview. See the 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

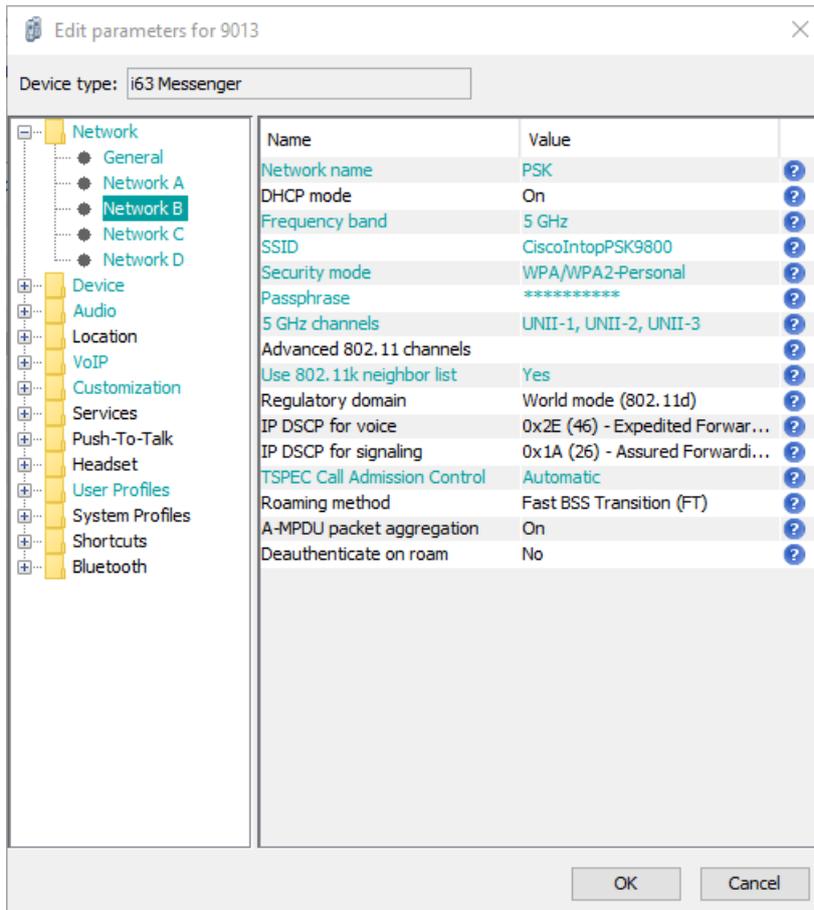
Transmit Power: 5

Ascom recommends only use channel 1, 6 and 11 for 802.11b/g/n. 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 these limits unless 802.11k is in use.**
- 2. Ascom does support and can coexist in 80MHz channel bonding environments. The recommendation 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 channels 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 VoWi-Fi deployments.**

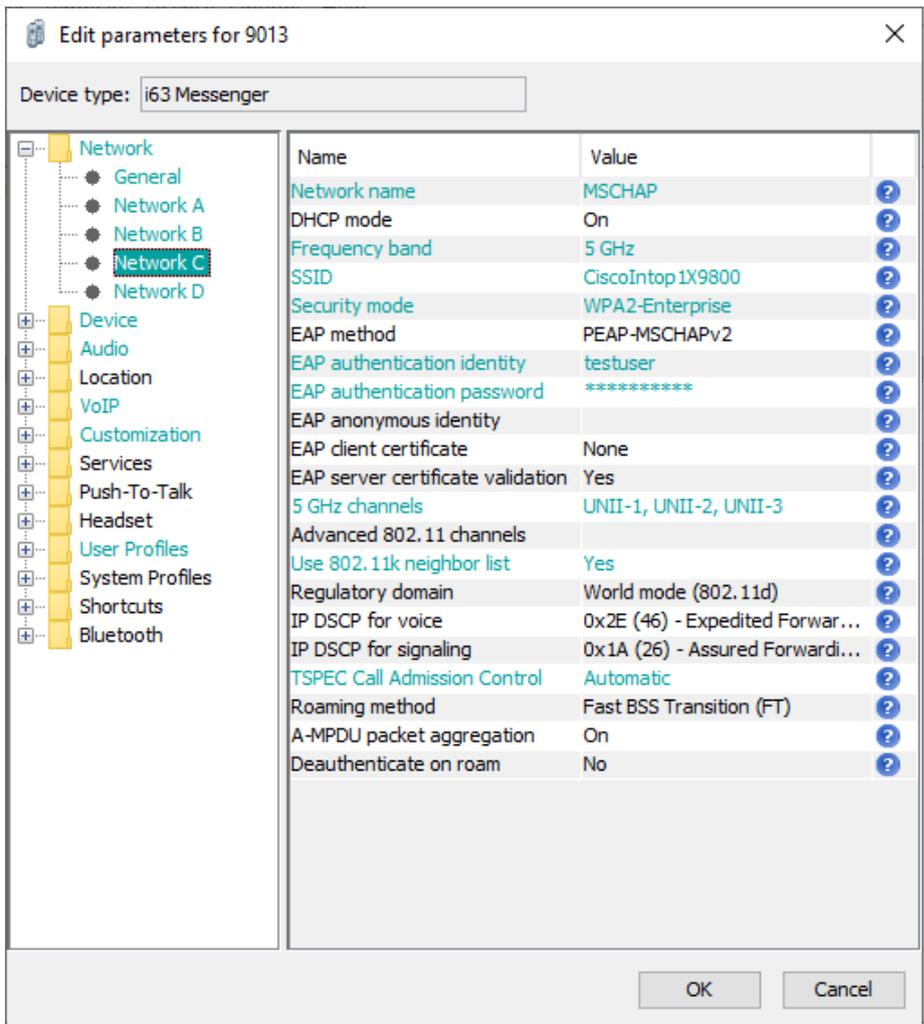


Network settings for WPA2-PSK

Make sure that the enabled channels in the i63 handset match the channel plan used in the system.

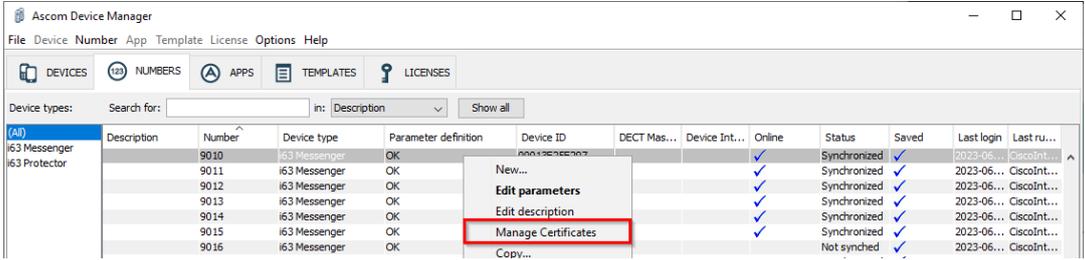
802.11k neighbor list will improve roaming performance especially when the number of channels in the system exceeds the 9 non-DFS channels.

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



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

802.11k neighbor list will improve roaming performance especially when the number of channels in the system exceeds the 9 non-DFS channels.



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	21
Fail	0
Comments	5
Not verified	4
Total	30

Refer to the attached file for detailed verification results.

## Document History

Rev	Date	Author	Description
D1	20-June-2023	NLRPa	Initial draft
P1	17-July-2023	NLRPa	Minor adjustments after peer review