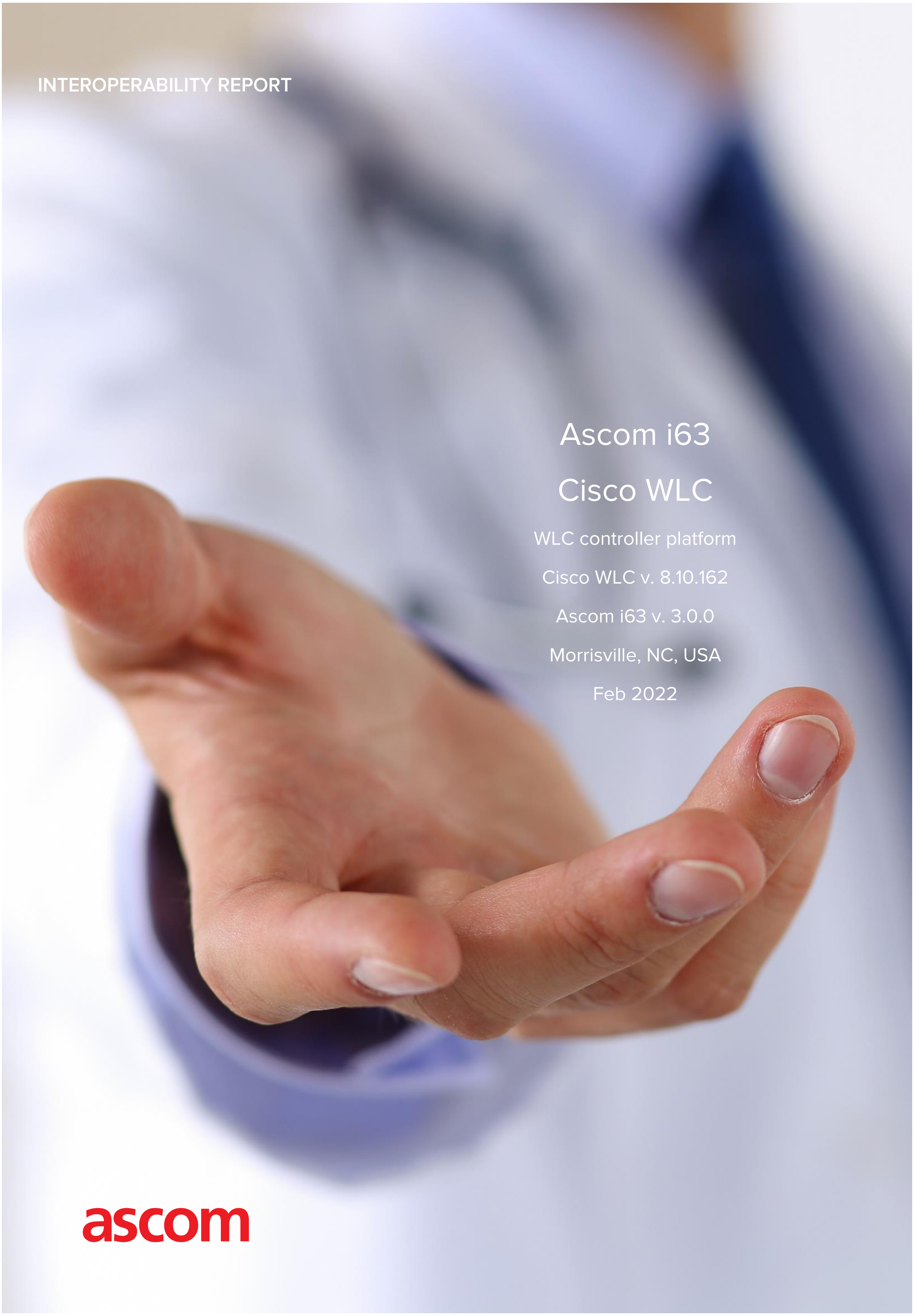


INTEROPERABILITY REPORT

Ascom i63

Cisco WLC

WLC controller platform

Cisco WLC v. 8.10.162

Ascom i63 v. 3.0.0

Morrisville, NC, USA

Feb 2022

ascom

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 WLC platform Version 8.10.162 8

Ascom i63 18

Appendix B: Interoperability Validation Records 20

Document History 20

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

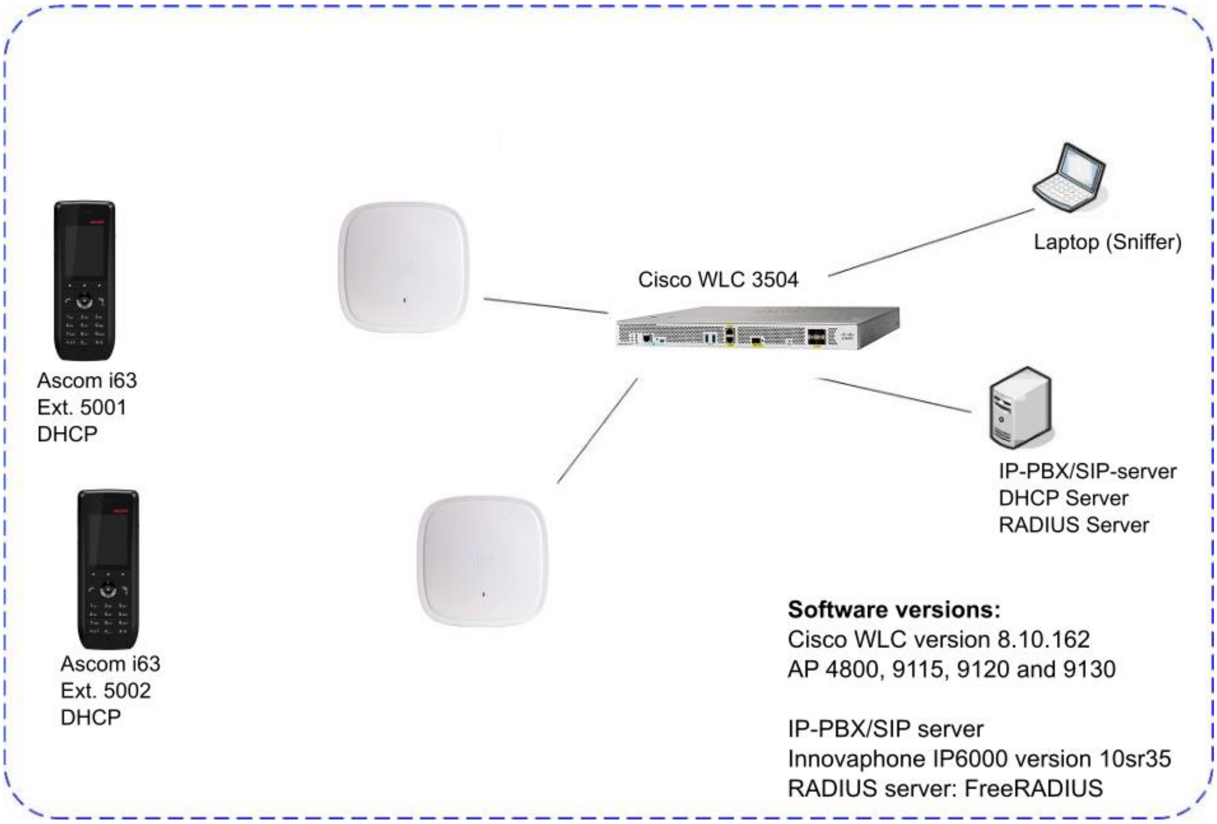
Verification site

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

Participants

Karl-Magnus Olsson, Ascom, Morrisville

Verification topology



Software versions:
Cisco WLC version 8.10.162
AP 4800, 9115, 9120 and 9130

IP-PBX/SIP server
Innovaphone IP6000 version 10sr35
RADIUS server: FreeRADIUS

Summary

General conclusions

The Ascom interoperability verification produced very good results with regards to authentication, stability and roaming.

This test is considered a regression test and some test cases that has previously been tested on the 8.10.x track has been left out. Test cases left out includes for example battery measurements and capacity tests.

OKC is no longer being tested and it is mandatory to use 11r/FT together with EAP based authentication. Also for PSK it its strongly recommended to use 11r/FT

Compatibility information

One Access point model from every product generation has been selected as a representation (4800, 9115, 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 8.10.162:

AP1832, 1852

AP2802, 3802, 4800

AP 9105, 9115, 9117, 9120, 9130

Supported Partner Controller Platforms with SW version 8.10.162:

Cisco 3504 Wireless Controller

Cisco 5520 Wireless Controller

Cisco 8540 Wireless Controller

Cisco Virtual Wireless Controller (vWLC)

Cisco Wireless Controllers for High Availability for Cisco 3504 WLC, Cisco 5520 WLC, and Cisco 8540 WLC.

Cisco Mobility Express Solution

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 (Personal) authentication	N/A	Not tested due to know issues
Association with WPA3 Enterprise authentication	N/A	Not tested due to know issues
Association, Multiple ESSIDs	OK	
Beacon Interval and DTIM Period	OK	
PMKSA Caching	N/T	Not tested
WPA2-opportunistic/proactive Key Caching	N/T	Not tested
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 30ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	N/T *	802.11r required
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 30-40ms
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

*) 802.11r / FT is generally recommended to enhance roaming performance.

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
WPA3-Personal 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
It's now mandatory to use 802.11r/FT with EAP authentication. OKC is no longer tested.		

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

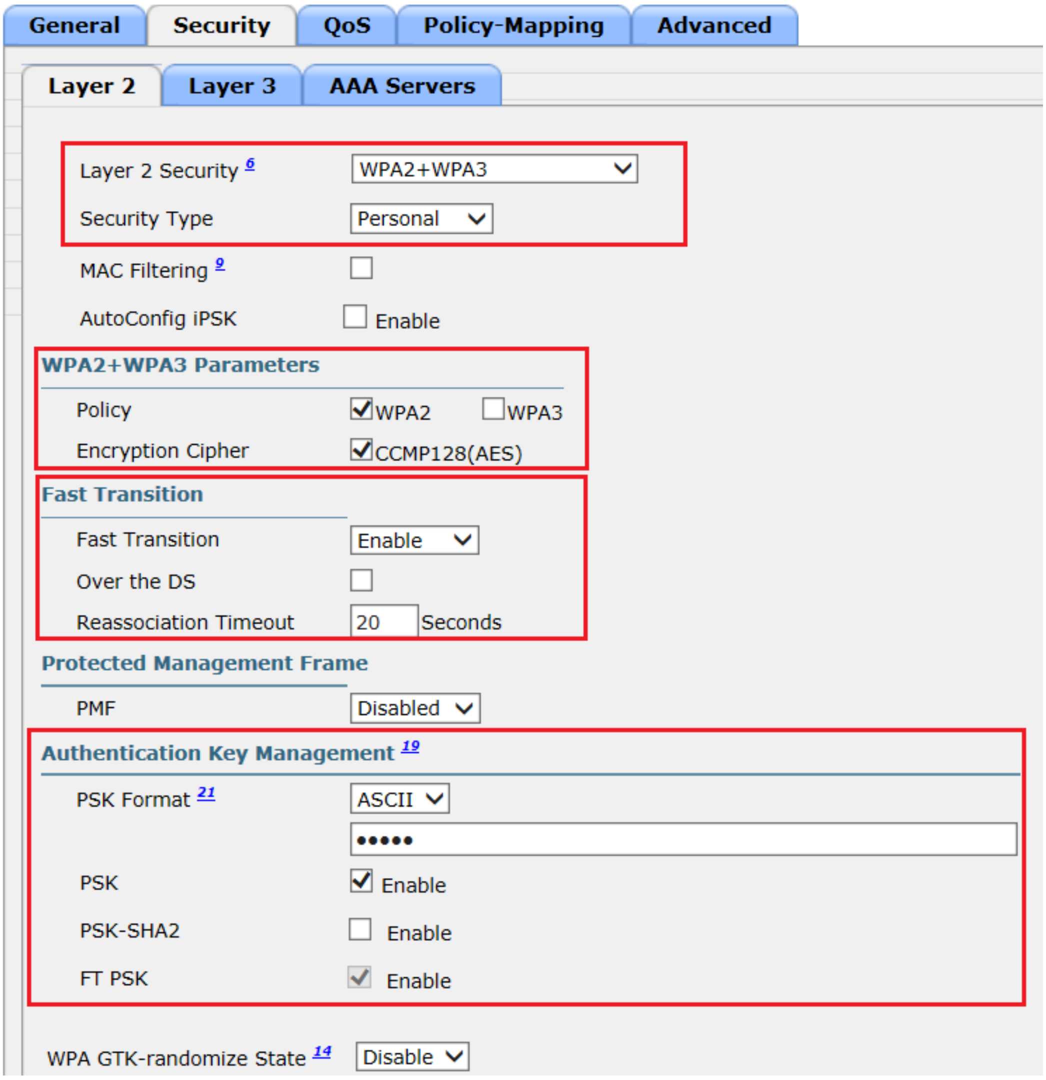
For detailed verification results, refer to Appendix B: Interoperability Validation Records.

Appendix A: Validation Configurations

Cisco WLC platform Version 8.10.162

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

Security settings (PSK)



Layer 2 Security 6: WPA2+WPA3

Security Type: Personal

MAC Filtering 9: □

AutoConfig iPSK: □ Enable

WPA2+WPA3 Parameters

Policy: ☑ WPA2 □ WPA3

Encryption Cipher: ☑ CCMP128(AES)

Fast Transition

Fast Transition: Enable

Over the DS: □

Reassociation Timeout: 20 Seconds

Protected Management Frame

PMF: Disabled

Authentication Key Management 19

PSK Format 21: ASCII

●●●●●

PSK: ☑ Enable

PSK-SHA2: □ Enable

FT PSK: ☑ Enable

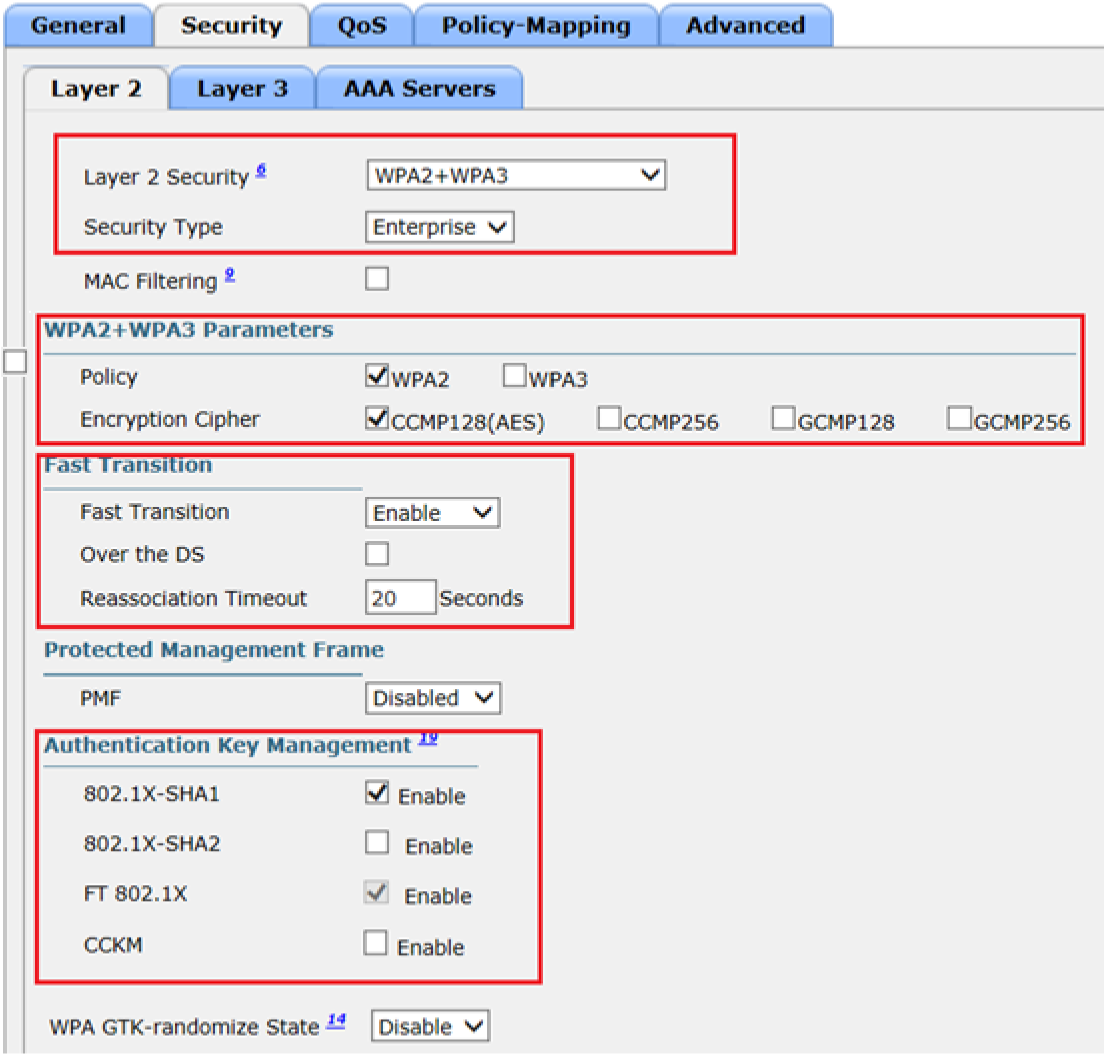
WPA GTK-randomize State 14: Disable

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 were 802.11r (FT) is advertised in conjunction with a legacy method.



Layer 2 Security [6] WPA2+WPA3

Security Type Enterprise

MAC Filtering [9] □

WPA2+WPA3 Parameters

Policy ☑WPA2 □WPA3

Encryption Cipher ☑CCMP128(AES) □CCMP256 □GCMP128 □GCMP256

Fast Transition

Fast Transition Enable

Over the DS □

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

Authentication Key Management [19]

802.1X-SHA1 ☑ Enable

802.1X-SHA2 □ Enable

FT 802.1X ☑ Enable

CCKM □ Enable

WPA GTK-randomize State [14] Disable

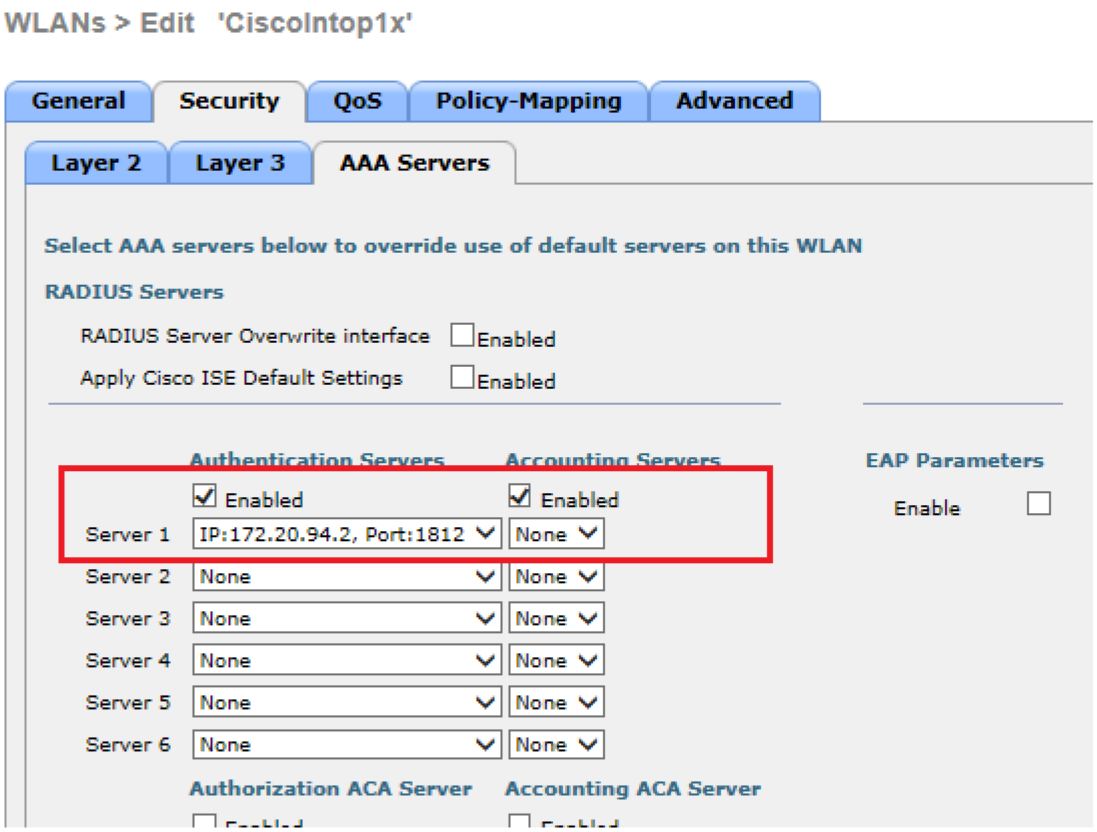
802.1X authentication (PEAP-MSCHAPv2).
Example of how to configure the system for .1X authentication

Configuration of authentication using external Radius server, 802.1X (Step 1). In this example is WPA2-AES used. Select 802.1X as Authentication Key Management.

- It is mandatory use Fast Transition (802.11r). OKC is no longer tested
- Select WPA2 Policy with AES encryption.
- Select both 802.1X and FT 802.1X for compatibility with i62 and Myco 1 and 2 on the same SSID.

  In cases were i62 and Myco 1 & 2 using CCKM, select both CCKM and FT 802.1X for compatibility.

Compatibility 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.



WLANs > Edit 'CiscoIntop1x'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □Enabled

Apply Cisco ISE Default Settings □Enabled

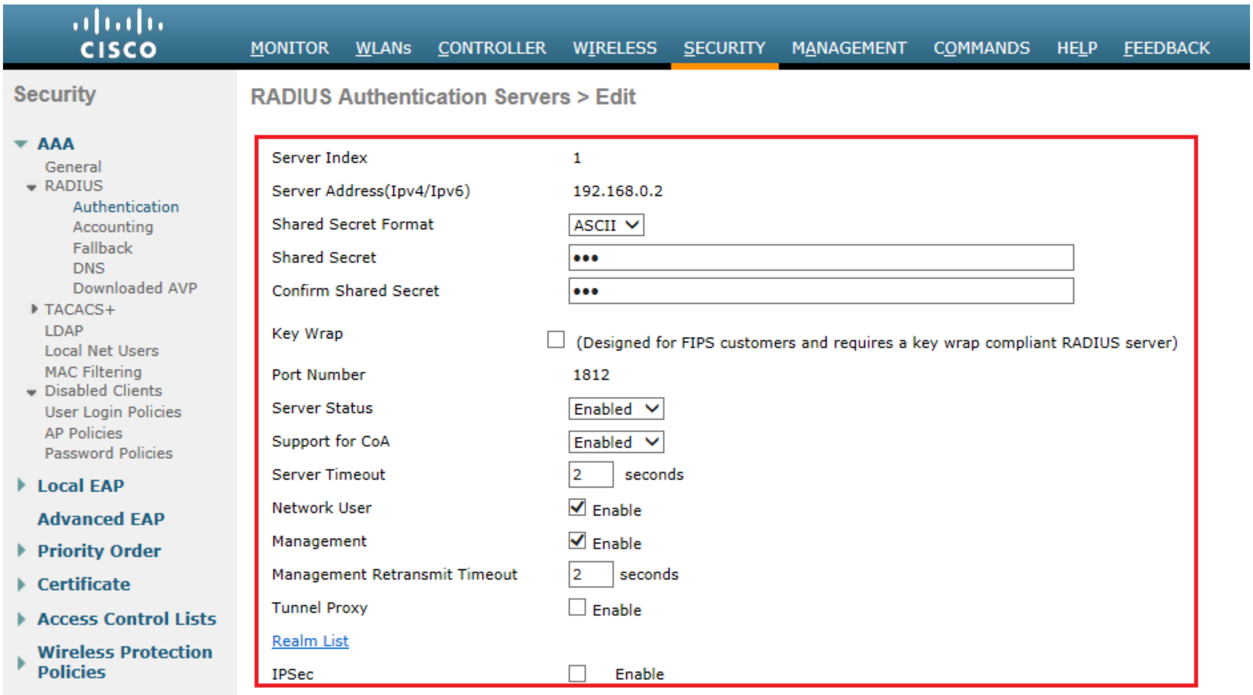
	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:172.20.94.2, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable □

Authorization ACA Server	Accounting ACA Server
□ Enabled	□ Enabled

Example of authentication configuration using external Radius server (Step 2). Select the server to use. The server is configured under tab Security/Radius. See configuration of server below.



RADIUS Authentication Servers > Edit

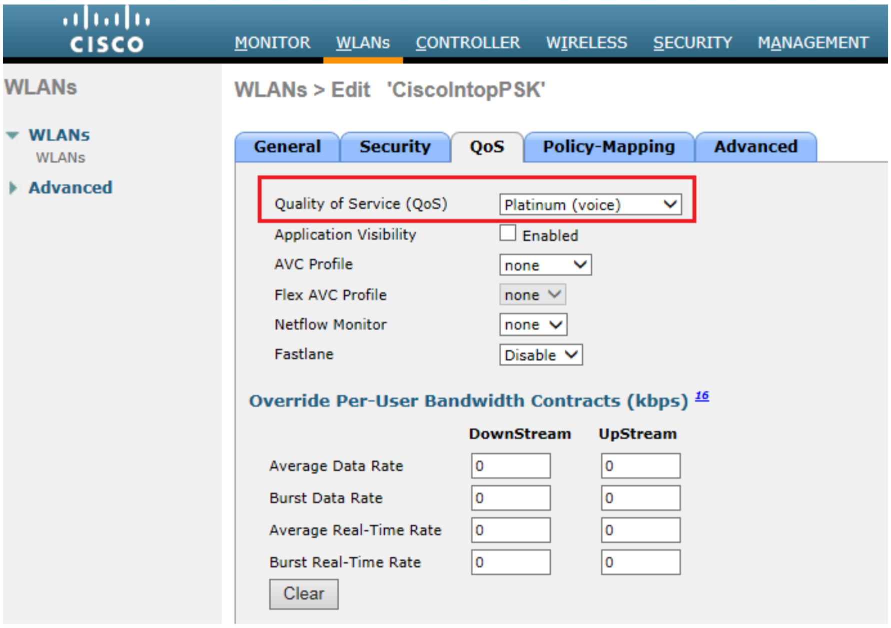
Server Index	1
Server Address(Ipv4/Ipv6)	192.168.0.2
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	2 seconds
Tunnel Proxy	□ Enable
Realm List	
IPSec	□ Enable

Configuration of authentication using external Radius server (Step 3). 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.

Note. Depending on authentication method used it might be necessary to add a certificate into the i63. PEAP-MSCHAPv2 requires a CA certificate and EAP-TLS requires both a CA certificate and a client certificate.

Note. Refer to the i63 section in for matching handset configurations.

General settings (QoS, Radio)



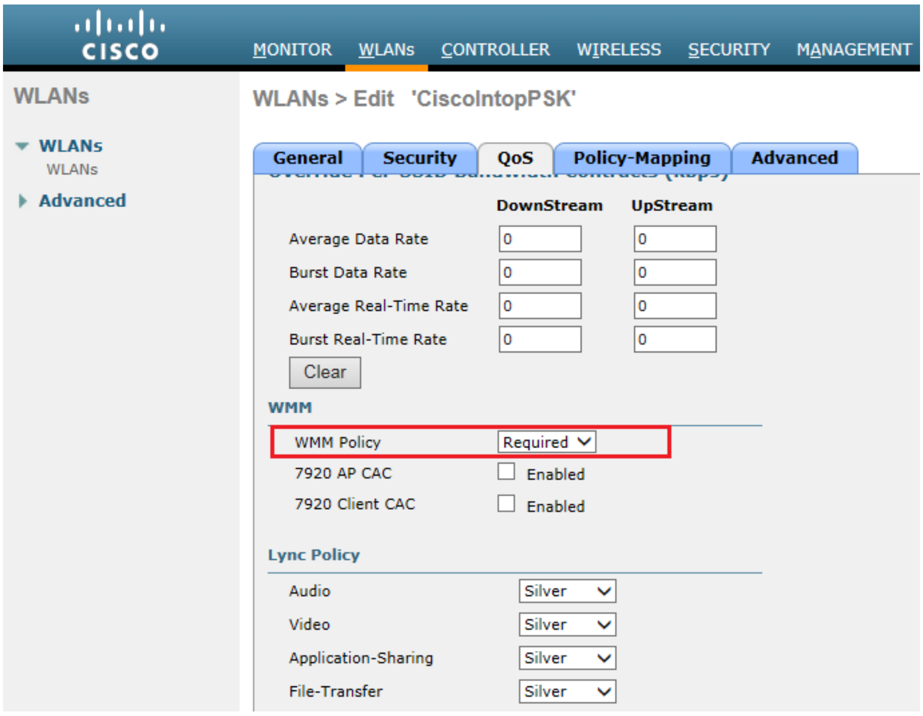
WLANs > Edit 'CiscoIntopPSK'

Quality of Service (QoS)	Platinum (voice)
Application Visibility	□ Enabled
AVC Profile	none
Flex AVC Profile	none
Netflow Monitor	none
Fastlane	Disable

Override Per-User Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Set QoS to “Platinum (Voice)”



WLANs > Edit 'CiscoIntopPSK'

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

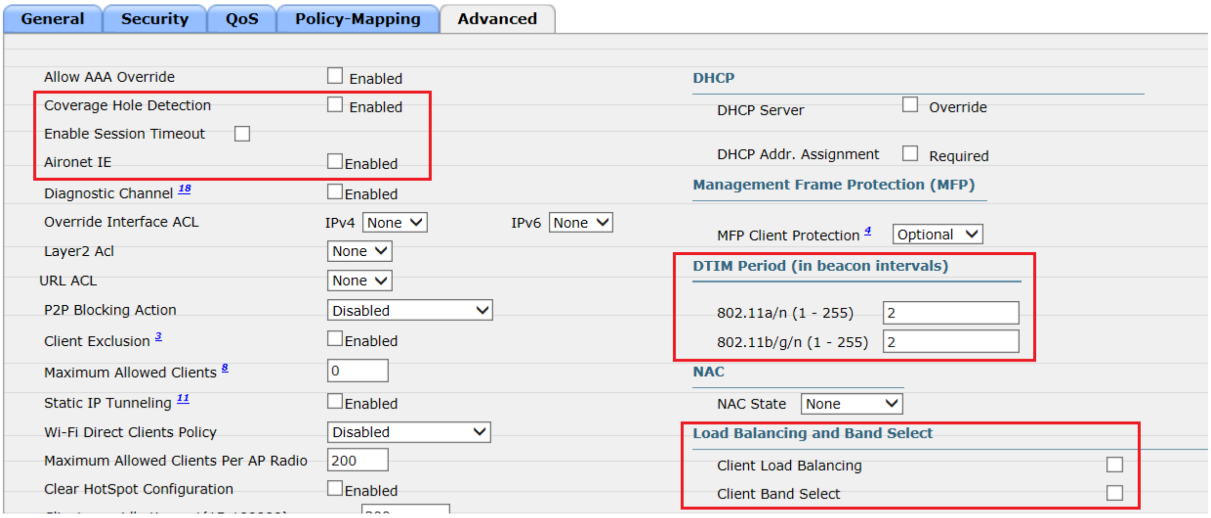
WMM

WMM Policy	Required
7920 AP CAC	□ Enabled
7920 Client CAC	□ Enabled

Lync Policy

Audio	Silver
Video	Silver
Application-Sharing	Silver
File-Transfer	Silver

Make sure that WMM policy is set to “Required” or “Allowed”



Allow AAA Override □ Enabled
Coverage Hole Detection □ Enabled
Enable Session Timeout □
Aironet IE □ Enabled
Diagnostic Channel [18] □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion [3] □ Enabled
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

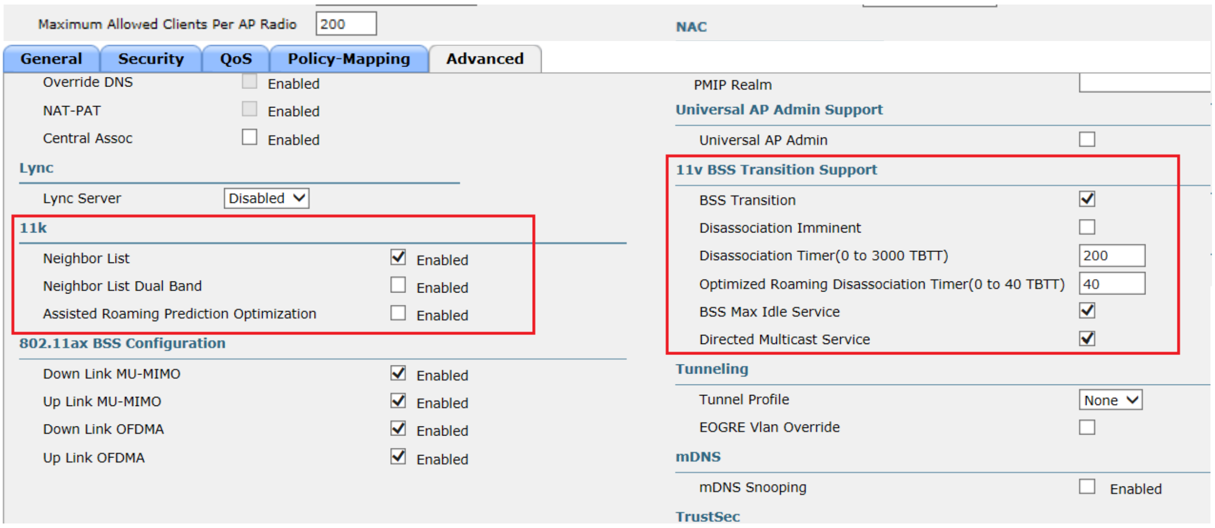
Management Frame Protection (MFP)
MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 2
802.11b/g/n (1 - 255) 2

NAC
NAC State None

Load Balancing and Band Select
Client Load Balancing □
Client Band Select □

- Make sure "Session timeout" is disabled or set to a very large value.
- Coverage Hole Detection can be left enabled if RRM is used in the system.
- Aironet IE is not needed for i63
- 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.



Maximum Allowed Clients Per AP Radio 200
NAC

Override DNS □ Enabled
NAT-PAT □ Enabled
Central Assoc □ Enabled

Lync
Lync Server Disabled

11k
Neighbor List ☑ Enabled
Neighbor List Dual Band □ Enabled
Assisted Roaming Prediction Optimization □ Enabled

802.11ax BSS Configuration
Down Link MU-MIMO ☑ Enabled
Up Link MU-MIMO ☑ Enabled
Down Link OFDMA ☑ Enabled
Up Link OFDMA ☑ Enabled

PMIP Realm

Universal AP Admin Support
Universal AP Admin □

11v BSS Transition Support
BSS Transition ☑
Disassociation Imminent □
Disassociation Timer(0 to 3000 TBTT) 200
Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40
BSS Max Idle Service ☑
Directed Multicast Service ☑

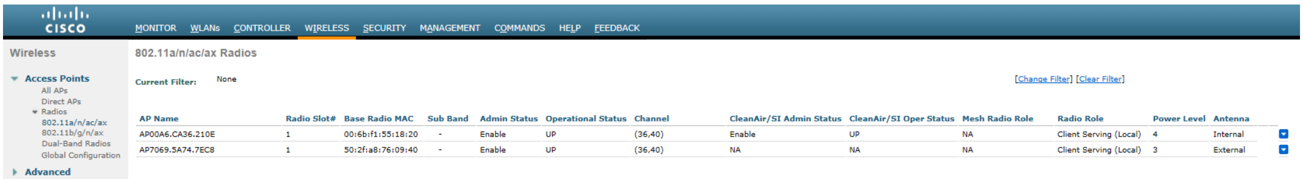
Tunneling
Tunnel Profile None
EOGRE Vlan Override □

mDNS
mDNS Snooping □ Enabled

TrustSec

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

Note for mixed device installation. Ascom i62 and Myco 1 & 2 do not support 11k but have no problem operating on an SSID were these settings are enabled. (Assuming i62 version 6.0.0 and later)

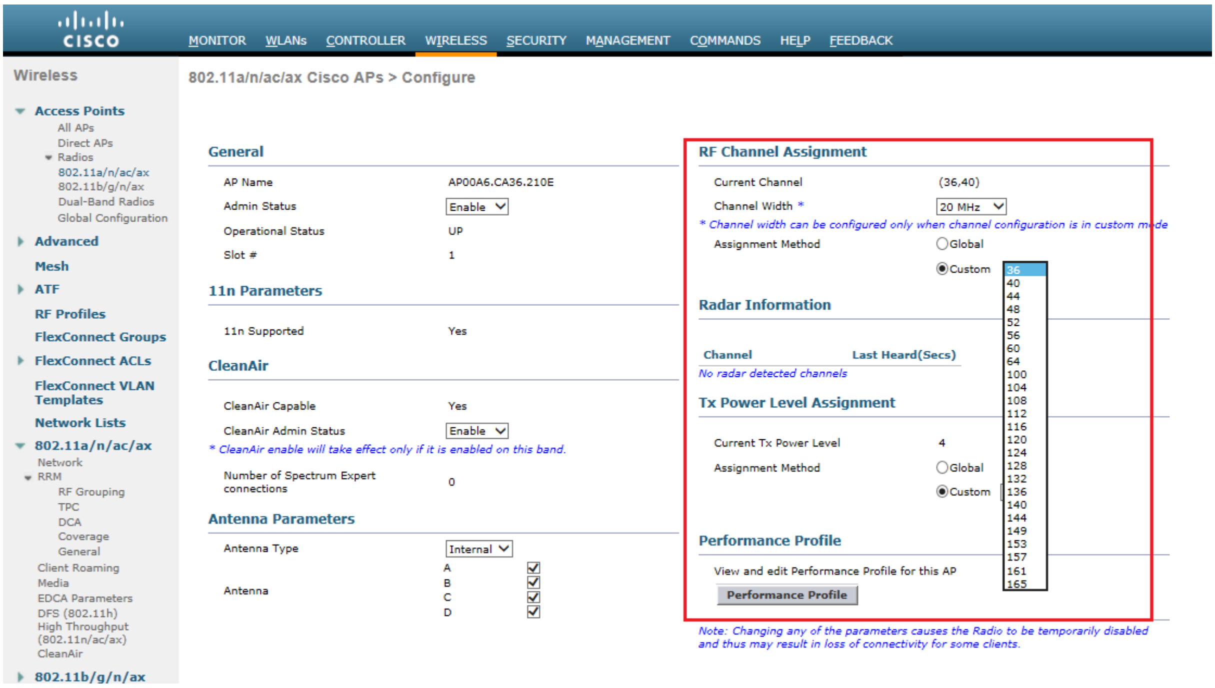


802.11a/n/ac/ax Radios

Current Filter: None

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanAir/SI Admin Status	CleanAir/SI Oper Status	Mesh Radio Role	Radio Role	Power Level	Antenna
AP00A6.CA36.210E	1	00:6b:f1:55:18:20	-	Enable	UP	(36,40)	Enable	UP	NA	Client Serving (Local)	4	Internal
AP7069.5A74.7EC8	1	50:2f:a8:76:09:40	-	Enable	UP	(36,40)	NA	NA	NA	Client Serving (Local)	3	External

Channel configuration. See next picture for additional information.



802.11a/n/ac/ax Cisco APs > Configure

General

AP Name AP00A6.CA36.210E

Admin Status Enable

Operational Status UP

Slot # 1

11n Parameters

11n Supported Yes

CleanAir

CleanAir Capable Yes

CleanAir Admin Status Enable

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections 0

Antenna Parameters

Antenna Type Internal

Antenna A ☑ B ☑ C ☑ D ☑

RF Channel Assignment

Current Channel (36,40)

Channel Width * 20 MHz

* Channel width can be configured only when channel configuration is in custom mode

Assignment Method ○Global ●Custom 36

Radar Information

Channel	Last Heard(Secs)

No radar detected channels

Tx Power Level Assignment

Current Tx Power Level 4

Assignment Method ○Global ●Custom

Performance Profile

View and edit Performance Profile for this AP

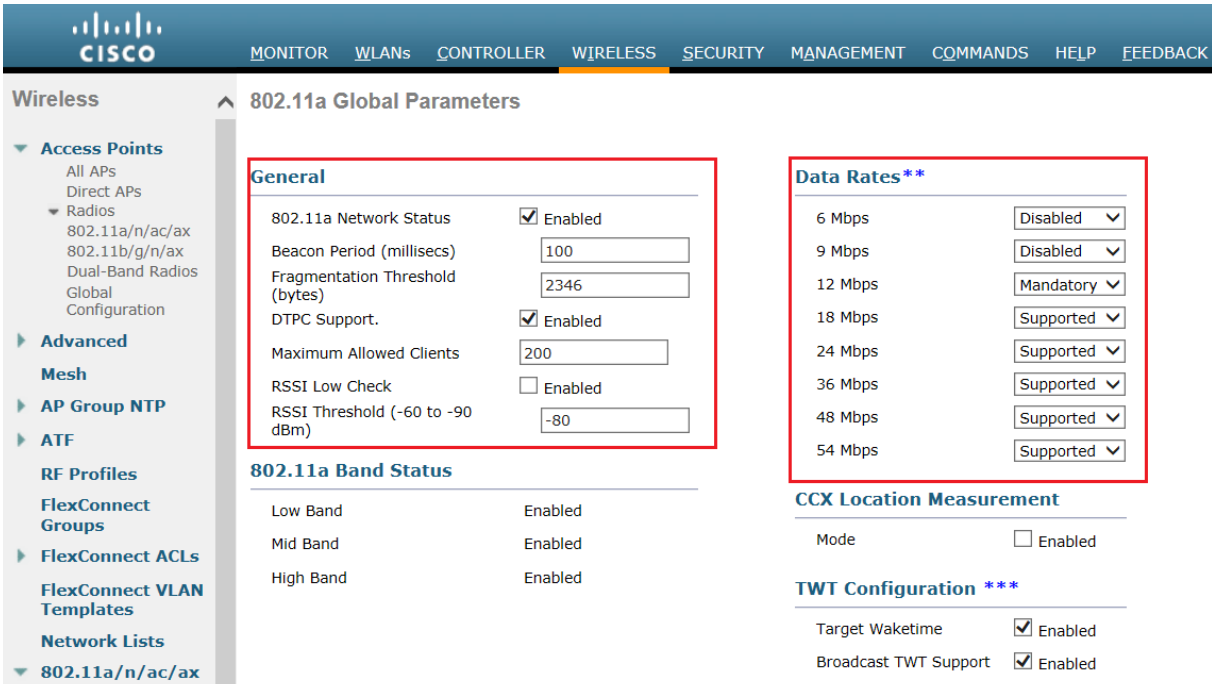
Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

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.**



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200
RSSI Low Check	□ Enabled
RSSI Threshold (-60 to -90 dBm)	-80

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

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

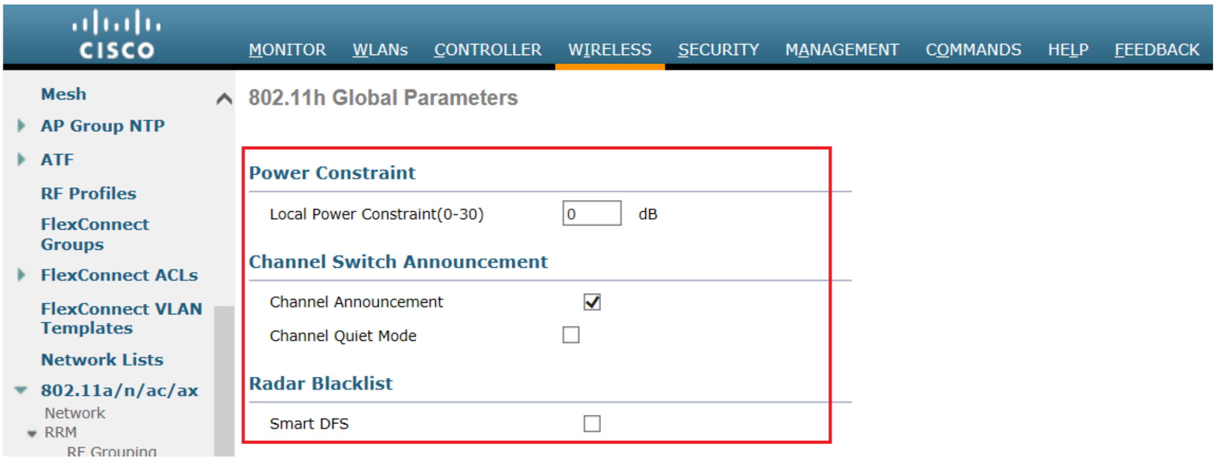
CCX Location Measurement

Mode	□ Enabled

TWT Configuration ***

Target Waketime	☑ Enabled
Broadcast TWT Support	☑ Enabled

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



802.11h Global Parameters

Power Constraint

Local Power Constraint(0-30)	0 dB

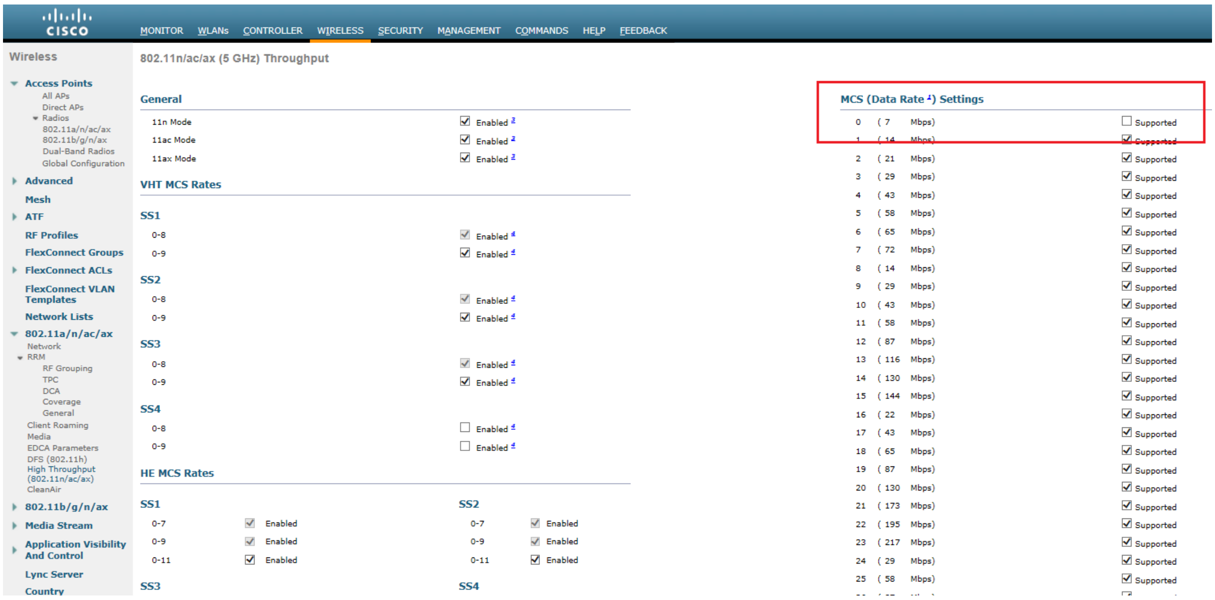
Channel Switch Announcement

Channel Announcement	☑
Channel Quiet Mode	□

Radar Blacklist

Smart DFS	□

As Ascom i63 do support Channel Switch Announcement it's recommended to have this setting enabled in the system (only applicable when DFS channels are used)



802.11n/ac/ax (5 GHz) Throughput

General

11n Mode	☑ Enabled [3]
11ac Mode	☑ Enabled [3]
11ax Mode	☑ Enabled [3]

VHT MCS Rates

SS1	
0-8	☑ Enabled [4]
0-9	☑ Enabled [4]
SS2	
0-8	☑ Enabled [4]
0-9	☑ Enabled [4]
SS3	
0-8	☑ Enabled [4]
0-9	☑ Enabled [4]
SS4	
0-8	□ Enabled [4]
0-9	□ Enabled [4]

HE MCS Rates

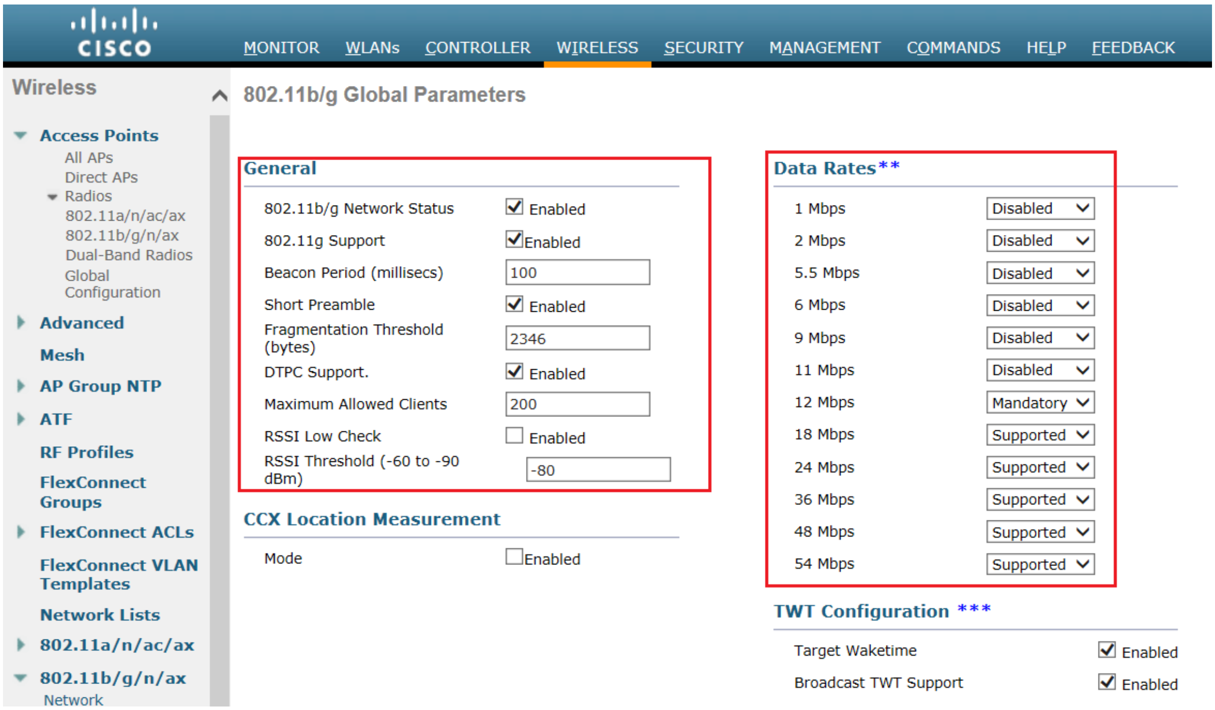
SS1		SS2	
0-7	☑ Enabled	0-7	☑ Enabled
0-9	☑ Enabled	0-9	☑ Enabled
0-11	☑ Enabled	0-11	☑ Enabled
SS3		SS4	

MCS (Data Rate [1]) Settings

0	(7 Mbps)	□ Supported
1	(14 Mbps)	☑ Supported
2	(21 Mbps)	☑ Supported
3	(29 Mbps)	☑ Supported
4	(43 Mbps)	☑ Supported
5	(58 Mbps)	☑ Supported
6	(65 Mbps)	☑ Supported
7	(72 Mbps)	☑ Supported
8	(14 Mbps)	☑ Supported
9	(29 Mbps)	☑ Supported
10	(43 Mbps)	☑ Supported
11	(58 Mbps)	☑ Supported
12	(87 Mbps)	☑ Supported
13	(116 Mbps)	☑ Supported
14	(130 Mbps)	☑ Supported
15	(144 Mbps)	☑ Supported
16	(22 Mbps)	☑ Supported
17	(43 Mbps)	☑ Supported
18	(65 Mbps)	☑ Supported
19	(87 Mbps)	☑ Supported
20	(130 Mbps)	☑ Supported
21	(173 Mbps)	☑ Supported
22	(195 Mbps)	☑ Supported
23	(217 Mbps)	☑ Supported
24	(29 Mbps)	☑ Supported
25	(58 Mbps)	☑ Supported

Ascom does support both usage of “11n Mode” and “11ac Mode” including 40 MHz and 80MHz channels. Its possible to also disable the lowest MCS data rates for optimal performance.

Follow the recommendations “General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac environments“



802.11b/g Global Parameters

General

802.11b/g Network Status	☑ Enabled
802.11g Support	☑ Enabled
Beacon Period (millisecs)	100
Short Preamble	☑ Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200
RSSI Low Check	□ Enabled
RSSI Threshold (-60 to -90 dBm)	-80

CCX Location Measurement

Mode	□ Enabled

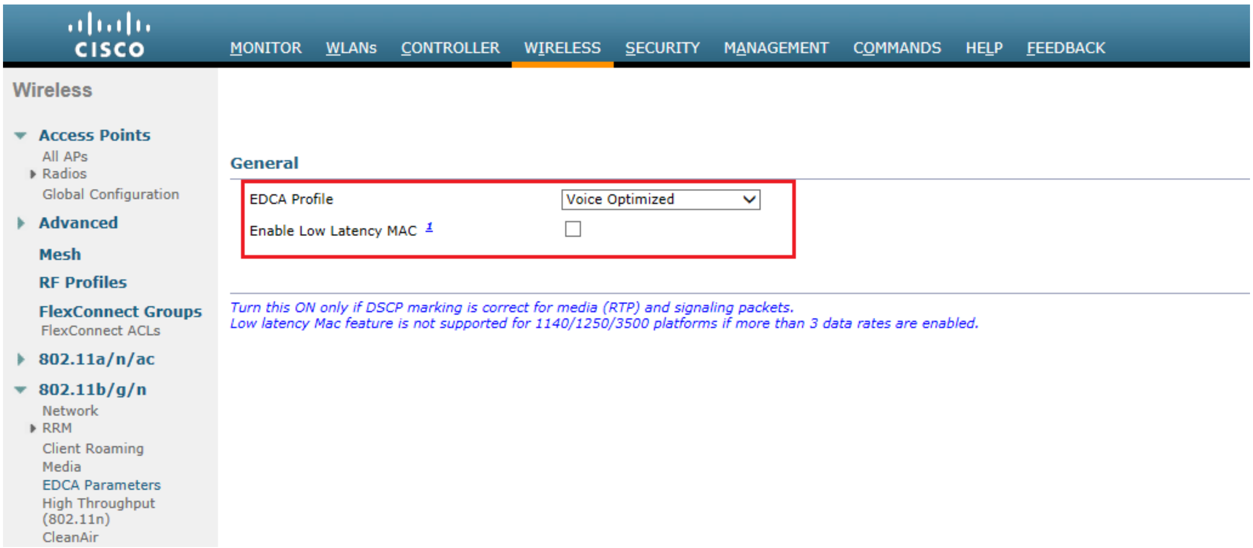
Data Rates**

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

TWT Configuration ***

Target Waketime	☑ Enabled
Broadcast TWT Support	☑ Enabled

The default data rate set will work fine, however for optimization Ascom recommends disabling the lowest data rates and have 12Mbps as lowest mandatory rate.



General

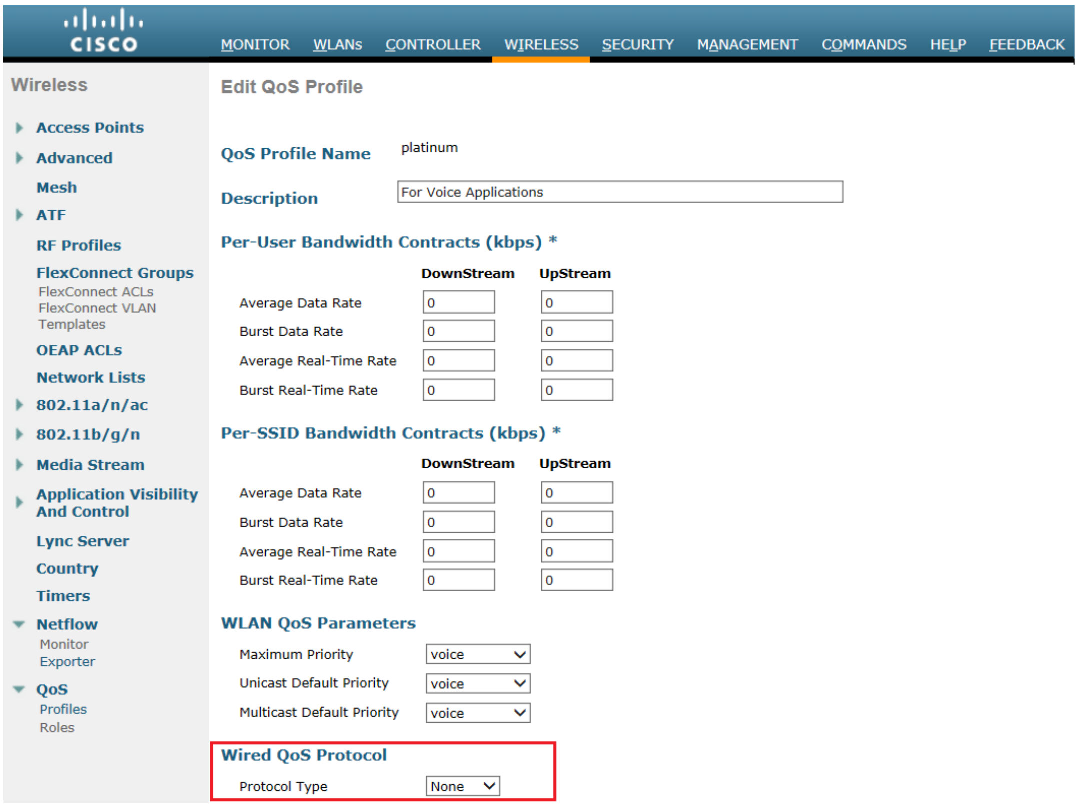
EDCA Profile	Voice Optimized
Enable Low Latency MAC [1]	□

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets.
Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled.

Ascom recommends “EDCA Profile”: Voice Optimized

Make sure Low Latency MAC is disabled. (Both 802.11a/n/ac and 802.11b/g/n)

Note. Using EDCA Profile “WMM” is acceptable but “Voice Optimized” is to prefer when voice clients are present in the system.



Edit QoS Profile

QoS Profile Name platinum

Description For Voice Applications

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

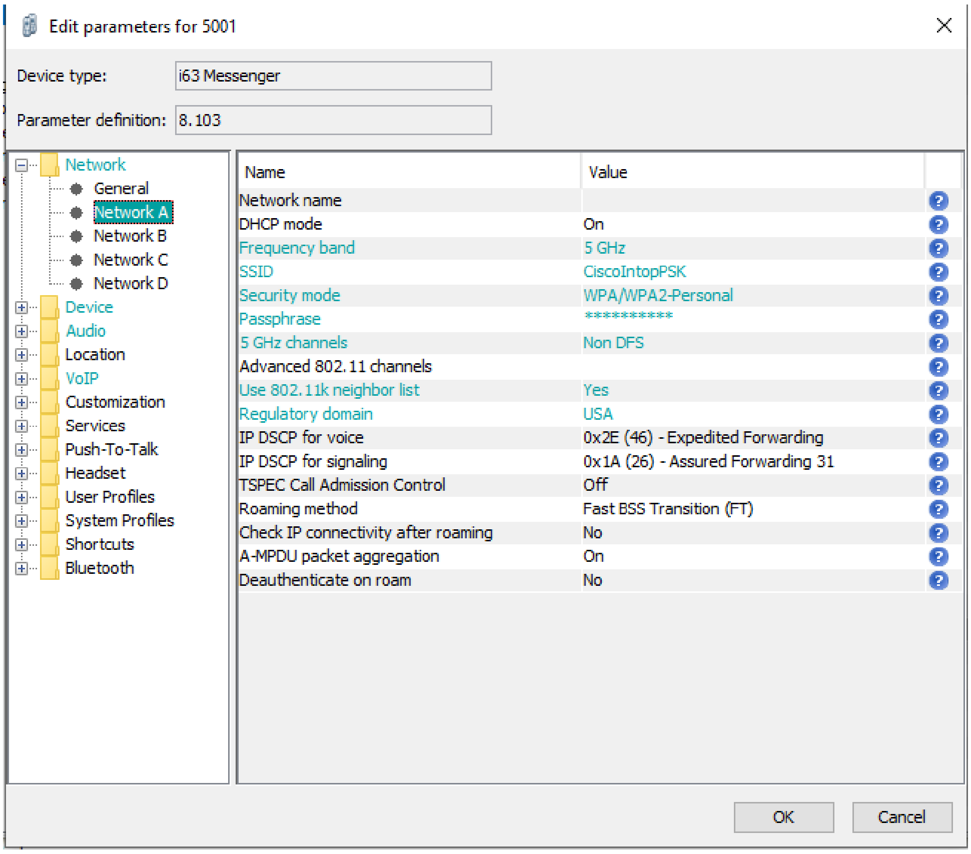
Maximum Priority	voice
Unicast Default Priority	voice
Multicast Default Priority	voice

Wired QoS Protocol

Protocol Type	None

Depending on the infrastructure (switches) ”Protocol Type” may have to be disabled.

Ascom i63



Device type: i63 Messenger

Parameter definition: 8.103

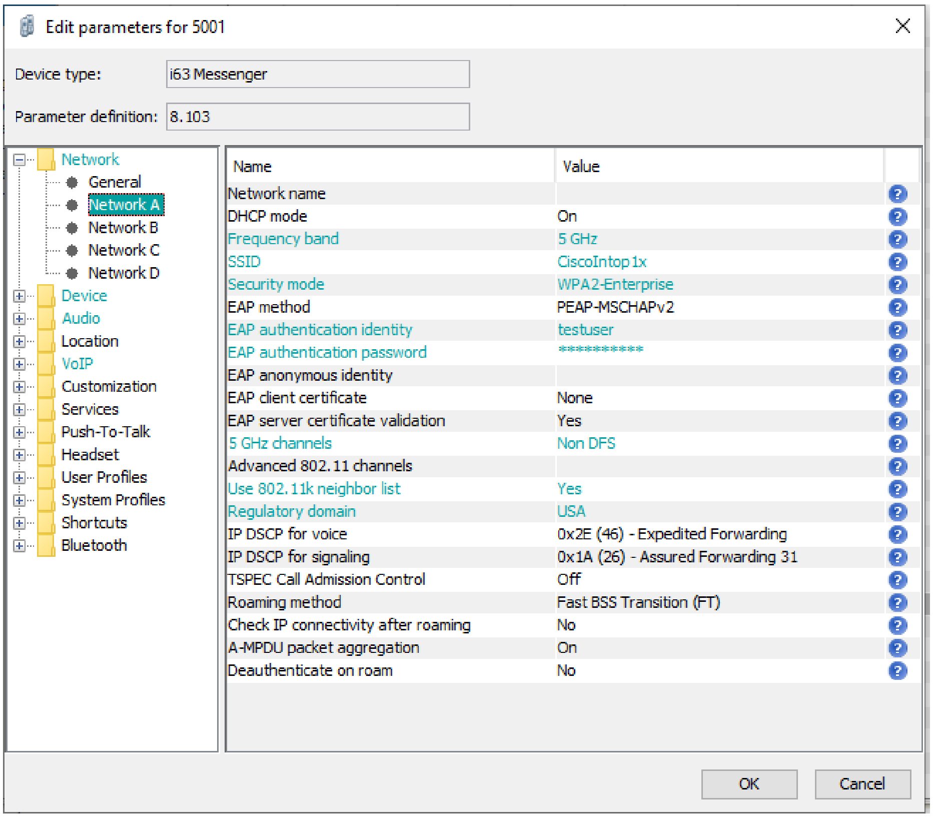
Name	Value
Network name	
DHCP mode	On
Frequency band	5 GHz
SSID	CiscoIntopPSK
Security mode	WPA/WPA2-Personal
Passphrase	***********
5 GHz channels	Non DFS
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	USA
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
Roaming method	Fast BSS Transition (FT)
Check IP connectivity after roaming	No
A-MPDU packet aggregation	On
Deauthenticate on roam	No

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 exceed the 9 non-DFS channels .

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



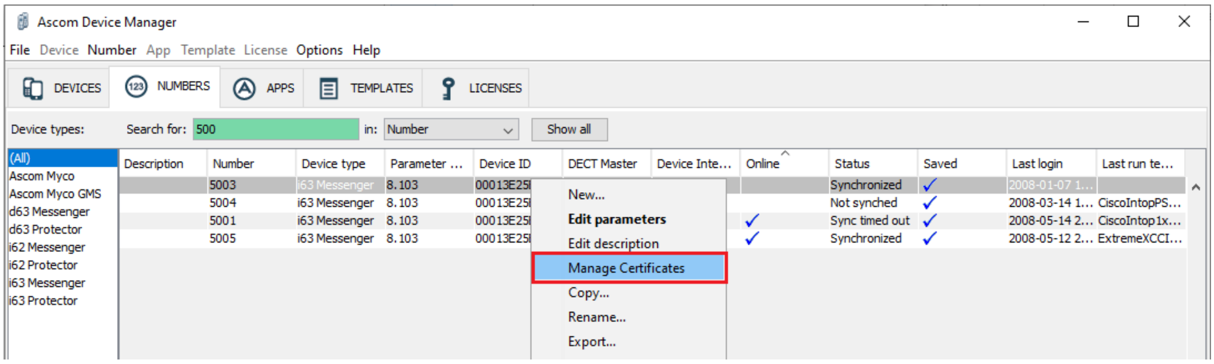
Device type: i63 Messenger

Parameter definition: 8.103

Name	Value
Network name	
DHCP mode	On
Frequency band	5 GHz
SSID	CiscoIntop1x
Security mode	WPA2-Enterprise
EAP method	PEAP-MSCHAPv2
EAP authentication identity	testuser
EAP authentication password	***********
EAP anonymous identity	
EAP client certificate	None
EAP server certificate validation	Yes
5 GHz channels	Non DFS
Advanced 802.11 channels	
Use 802.11k neighbor list	Yes
Regulatory domain	USA
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
TSPEC Call Admission Control	Off
Roaming method	Fast BSS Transition (FT)
Check IP connectivity after roaming	No
A-MPDU packet aggregation	On
Deauthenticate on roam	No

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

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



Device types: Search for: 500 in: Number

Description	Number	Device type	Parameter ...	Device ID	DECT Master	Device Inte...	Online	Status	Saved	Last login	Last run te...
	5003	i63 Messenger	8.103	00013E25I				Synchronized	✓	2008-01-07 1...	
	5004	i63 Messenger	8.103	00013E25I				Not synched	✓	2008-03-14 1...	CiscoIntopPS...
	5001	i63 Messenger	8.103	00013E25I			✓	Sync timed out	✓	2008-05-14 2...	CiscoIntop1x...
	5005	i63 Messenger	8.103	00013E25I			✓	Synchronized	✓	2008-05-12 2...	ExtremeXCCI...

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	17
Fail	0
Comments	2
Not verified	9
Total	28

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	4-Feb-20	SEKMO	Draft
R1	10-Feb-2022	SEKMO	Minor corrections after internal review.