INTEROPERABILITY REPORT

Ascom i62 Cisco 9800

Catalyst 9800 controller platform Cisco ISO XE v. 17.3.1 Ascom i62 v. 6.2.0 Morrisville, NC, USA November 2020

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 Catalyst 9800 platform Version 17.3.1	. 8
Ascom i62	23
Appendix B: Interoperability Validation Records2	26
Document History2	26

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 very good results with regards to all test areas including authentication, stability, roaming, QoS and power save related areas.

Issues with OKC basically prevents all other Auth methods than PSK from being viable options. Refer to Known Issues section for details.

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 17.3.1:

AP1702, 2702, 3702 AP1832, 1852 AP2802, 3802, 4800 AP 9115, 9117, 9120, 9130

Supported Partner Controller Platforms with SW version 17.3.1:

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	NOK	
WPA2-opportunistic/proactive Key Caching	OK	
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 *	Typical roaming time 50 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	NOK	Issue with OKC
Roaming, EAP-FAST, CCKM	OK	40ms

*) Average roaming times are measured using 802.11a/n. Refer to Appendix B for detailed test results

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
OKC not working. Roaming with 802.1X authentication methods always results in full EAP key exchange. Depending on infrastructure (RADIUS server etc.) roaming times could be above 1 second with significant loss of voice as result. Only viable authentication method supported until resolved is PSK	Use PSK	Contact Ascom interop team or Cisco Tac.
CAC/TSPEC problem. Significant voice gap during roaming when using CAC/TSPEC. Under investigation.	Make sure CAC is disabled in the 9800 system as well as in the i62 device	

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

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

Appendix A: Validation Configurations

Cisco Catalyst 9800 platform Version 17.3.1

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 i62. Please note that security settings were modified according to requirements in individual test cases.

WLAN settings

Q, Search Menu Items		Configuration * > Tags & Profiles * > WLANs							
Dashboard		+ /	Add	×D	lelete Enable WLAN Disable WLAN				
		Number	r of WLAI	Ns selec	ted : 0				
Monitoring	>	0	Statu	s v	Name	~	ID	SSID ~	Security
		0	G	•	CiscoIntopPSK9800	•	1	CiscoIntopPSK9800	[WPA2][PSK][AES]
	^	0	G)	CiscoIntop1X9800	•	2	CiscoIntop1X9800	[WPA2][802.1x][AES]
So Administration	>	0	C	•	CiscoIntopOPEN9800	•	3	CiscoIntopOPEN9800	[open]
~~		0	G		CiscoIntopEAPFAST	•	4	CiscoIntopEAPFAST	[WPA2][CCKM][AES]
C Licensing		14 -	∈ 1	\vdash	H 10 v items per page				
X Troubleshooting									

WLAN overview

General Security Advanced Add To Policy Tags Layer2 Layer3 AAA Layer2 Security Mode WPA + WPA2 • Fast Transition Disabled MAC Fittering 0 Fast Transition Disabled Portected Management Frame Disabled • Over the DS 0 PMF Disabled • MPSK Configuration 20 WPA Parameters 0 MPSK 0 WPA Policy 0 MPSK 0 GKR Randomize 0 AES(CMP128) NESK NESK QPA2 Encrypton 0 AES(CMP128) NESK NESK NESK Auth Key Mgmt 0 S02.1x PSK PSK NESK NESK PSK Format ASCI PSK PSK-SHA256 PSK-SHA256 PSK-SHA256 PSK Type Unencrypted • Unencrypted • Nesk NESK Nesk	dit WLA	N				
Layer3 AAA Layer 2 Security Mode WPA + WPA2 • MAC Fittering Image: Comparison of the Disabled Protected Management Frame Disabled • WPA Parameters Disabled • WPA Policy Image: Comparison of the Disabled WPA Policy Image: Comparison of the Disabled WPA Policy Image: Comparison of the Disabled WPA2 Encryption Action (Comparison of the Disabled) Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the Disabled Image: Comparison of the	General	Security	Advanced	Add To Policy Tags		
Layer 2 Security Mode WPA + WPA2 MAC Filtering Protected Management Frame PMF Disabled WPA Parameters WPA Parameters WPA Policy GAR Configuration GARC WPA2 Policy GARC GARD GARD GARD GARD GARD GARD GARD GARD GARD GARD GARD GARD	Layer2	Layer3	AAA			
Protected Management Frame Over the DS Image: Comparison of the DS PMF Disabiled Reassociation Timeout 20 VPA Parameters MPSK Configuration MPSK Image: Comparison of the DS Image	Layer 2 Se MAC Filter	ecurity Mode		WPA + WPA2	Lobby Admin Access Fast Transition	Disabled v
PMF Disabled MPSK MPSK WPA Parameters MPSK MPSK MPSK WPA Policy I MPSK I WPA Policy I MPSK I WPA Policy I I I GTK Randomize I I I OSEN Policy I I I WPA2 Encryption A AES(CCMP128) I I I CCMP256 I I I I I I Auth Key Mgmt I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I <td>Protected</td> <td>d Managemer</td> <td>nt Frame</td> <td></td> <td>Over the DS</td> <td>0</td>	Protected	d Managemer	nt Frame		Over the DS	0
MPSK Configuration WPA Parameters MPSK WPA Policy Impsk WPA 2 Policy Impsk GTK Randomize Impsk OSEN Policy Impsk WPA2 Encryption AES(CCMP128) CCMP256 GMP128 Impsk Impsk WPA2 Encryption AES(CCMP128) Impsk Impsk Impsk <thimpsk< th=""> Impsk</thimpsk<>	PMF			Disabled v	Reassociation Timeout	20
MPSK Crmat PSK Type	WPA Par	ameters			MPSK Configuration	
WPA Policy I WPA2 Policy I GTK Randomize I OSEN Policy I WPA2 Encryption AES(CCMP128) CCMP256 GCMP256 GCMP256 GCMP256 I GCMP256 I S02.1x I PSK I PSK I S02.1x I PSK I S02.1x I PSK I S02.1x I PSK I PSK I S02.1x I PSK I PSK SPinzet PSK Type Unencrypted	WI A Full				MPSK	Ο
WPA2 Policy I GTK Randomize I OSEN Policy I WPA2 Encryption I AES(CCMP128) CCMP256 GCMP128 GCMP256 GCMP256 Auth Key Mgmt I 802.1x PSK CCKM FT + 802.1x FT + 802.1x FT + PSK 802.1x-SHA256 PSK-SHA256 PSK-SHA256 PSK Format ASCII PSK Type Unencrypted Pre-Shared Key* IIII	WPA Polic	зy		0		
GTK Randomize I OSEN Policy I WPA2 Encryption AES(CCMP128) CCMP256 GCMP128 GCMP256 GCMP256 Auth Key Mgmt 802.1x PSK CCKM FT + 802.1x FT + 802.1x FT + PSK 802.1x-SHA256 PSK Format ASCII PSK Type Unencrypted Pre-Shared Key* Immini	WPA2 Poli	icy		Ø		
OSEN Policy OSEN P	GTK Rande	omize		0		
WPA2 Encryption AES(CCMP128) CCMP256 GCMP128 GCMP256 Auth Key Mgmt 802.1x PSK CCKM FT + 802.1x FT + 802.1x FT + 802.1x FT + 802.1x FT + PSK 802.1x-SHA256 PSK-SHA256 PSK Format ASCI VInencrypted Pre-Shared Key*	OSEN Poli	су		0		
□ CCMP256 □ GCMP128 □ GCMP256 Auth Key Mgmt □ 802.1x ☑ PSK □ CCKM □ FT + 802.1x □ PSK-SHA256 □ PSK - SHA256 □ PSK - SHA256 □ PSK Type □ Unencrypted ▼ Pre-Shared Key*	WPA2 End	cryption		AES(CCMP128)		
GCMP128 GCMP256 Auth Key Mgmt □ 802.1x Ø PSK CCKM FT + 802.1x FT + 802.1x FT + PSK 802.1x-SHA256 Ø PSK-SHA256 PSK Format ASCII ▼ PSK Type Unencrypted ▼				CCMP256		
Auth Key Mgmt B 802.1x PSK S FOrmat PSK Type Auth Key Mgmt B 802.1x S FT + 802.1x FT + 802.1x FT + PSK B 802.1x-SHA256 PSK-SHA256 VUnencrypted Pre-Shared Key* S S S S S S S S S S S S S S S S S S S				GCMP128		
CCKM FT + 802.1x FT + PSK 802.1x-SHA256 PSK-SHA256 PSK Format ASCII PSK Type Unencrypted Pre-Shared Key*	Auth Key M	Mgmt		 ■ 802.1x Ø PSK 		
□ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 PSK Format ASCII PSK Type Unencrypted Pre-Shared Key*				С ССКМ		
□ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 □ PSK-SHA256 □ PSK Type □ Unencrypted □ Pre-Shared Key*				F T + 802.1x		
B02.1x-SHA256 PSK-Format ASCII PSK Type Unencrypted Pre-Shared Key*				FT + PSK		
PSK Format ASCII PSK Type Unencrypted Pre-Shared Key*				 PSK-SHA256 		
PSK Type Unencrypted Pre-Shared Key*	PSK Forma	at		ASCII		
Pre-Shared Key*	PSK Type			Unencrypted •		
	Pre-Share	ed Key*				

WLAN PSK configuration

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)

Note. Select both PSK and FT+PSK for compatibility with i63 and Myco 3 on the same SSID.

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 WLA	N				
General	Security	Advanced	Add To Policy Tags		
Layer2	Layer3	AAA			
Layer 2 Se	ecurity Mode		WPA + WPA2	Lobby Admin Access	0
MAC Filter	ing		0	Fast Transition	Disabled
Protected	Managemer	nt Frame		Over the DS	0
				Reassociation Timeout	20
PMF			Disabled	MPSK Configuration	
WPA Para	ameters			MPSK	Ο
					0
WPA Polic	у		0		
WPA2 Poli	icy		Ø		
GTK Rando	omize		0		
OSEN Poli	су		0		
WPA2 Enc	ryption		AES(CCMP128)		
			CCMP256		
			GCMP128		
			GCMP256		
Auth Key N	Ngmt		🕢 802.1x		
			O PSK		
			ССКМ		
			FT + 802.1x		
			FT + PSK		
			0 802.1x-SHA256		
			PSK-SHA256		

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

Not recommended until OKC issue is resolved

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.

Note. Select both 802.1X and FT + 802.1X for compatibility with i63 and Myco 3 on the same SSID.

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.

Edit WLA	N		
General	Security	Advanced	Add To Policy Tags
Layer2	Layer3	AAA	
Authenti	cation List	d	lefault 🔻
Local EA	AP Authenticat	ion 🖸	

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.

Configuration * > Securi	ty* > AAA				
+ AAA Wizard					
Servers / Groups AA	A Method List AAA Advanc	ced			
+ Add × Dele	te				
RADIUS	Servers Server Group	21			
TACACS+					
I DAP	Name	 Address 	 Auth Port 	 Acct Port 	~
	FreeRadius	172.20.94.2	1812	1813	
		10 🔻 items per page		1	- 1 of 1 items

AAA overview

Configuration * > Sec	surity* > AAA	Edit AAA Radius Server	
+ AAA Wizard		Name*	FreeRadius
Servers / Groups	AAA Method List AAA Adva	Server Address*	172.20.94.2
		PAC Key	Ο
+ Add × D	elete	Кеу Туре	Clear Text 🔹
RADIUS	Servers Server Gro	Key*	
TACACS+		Confirm Key*	
LDAP	Name	Auth Port	1812
	⊲ ⊲ 1 ⊩ ⊮	Acct Port	1813
		Server Timeout (seconds)	1-1000
		Retry Count	0-100
		Support for CoA	ENABLED

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 Method List Name* default	
Servers / Groups AAA Method List AAA Advanced Type*	
Authentication Fallback to local	
Authorization + Add × Delete Available Server Groups Assigned Server Groups	
Accounting Name Type Idap tacacs+	

Assign radius server to Method List (default)

dit WLAN		
General Security Ad	vanced Add To Polic	icy Tags
Coverage Hole Detection	Ø	Universal Admin
Aironet IE	0	Load Balance
P2P Blocking Action	Disabled •	Band Select
Multicast Buffer	DISABLED	IP Source Guard
Media Stream Multicast-	0	WMM Policy Required
11ac MU-MIMO	Ø	mDNS Mode Bridging v
Max Client Connections		Off Channel Scanning Defer
Der WI AN		Defer O 0 O 1 O 2
	0	
Per AP Per WLAN	0	
Per AP Radio Per WLAN	200	Scan Defer 100
11v BSS Transition Support	:	Time
		Assisted Roaming (11k)
BSS Transition		Production
Disassociation Imminent(0 to 3000 TBTT)	200	Optimization
Optimized Roaming Disassociation Timer(0 to 40 TBTT)	40	Neighbor List
BSS Max Idle Service		List
BSS Max Idle Protected	0	DTIM Period (in beacon intervals)
Directed Multicast Service	Ø	5 GHz Band (1-255) 2
11ax		2 4 GHz Band (1-255)
Downlink OFDMA		Device Analytics
Uplink OFDMA		Advertise Support
Downlink MU-MIMO		Share Data with Client
Uplink MU-MIMO		11k Reacon Dadio Messurament
BSS Target Wake Up Time		Client Scan Report
		Un 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.
- Even though 11k features are not supported by Ascom i62 it can coexist in a network were it is enabled.

Policy and general settings (QoS, Radio)

Configuration > Tags & Profiles > Tags	Edit Policy Tag	×			
Policy Site RF AP	Changes may result in lo	ss of connectivity for some clients that are associated to APs with this Policy Tag.			
+ Add × Delete	Name* default-	policy-tag			
Policy Tag Name	Description default p	policy-tag			
default-policy-tag					
◀ ◀ 1 ▶ ▶ 10 ▼ items per page	WLAN-POLICY Maps:	3			
	+ Add × Delete				
	WLAN Profile	V Policy Profile			
	CiscoIntop1X9800	default-policy-profile			
	CiscoIntopPSK9800	default-policy-profile			
	CiscoIntopOPEN9800	default-policy-profile			
	⊲ ⊲ 1 ⊳ ⊳ 10	▼ items per page 1 - 3 of 3 items			
	Map WLAN and Policy				
	WLAN Profile* Ciscolnt	op1X9800 ▼ Policy Profile* default-policy-profile ▼			
		× •			

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

Cor	figuration * >	> Tags & Profiles * > Policy			
-	⊢ Add	× Delete			
	Status 🖂	Policy Profile Name	~	Description	×.
Ο	0	default-policy-profile		default policy profile	
4	≪ 1 ⊨	▶ ► 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		Flow Monitor	IPv4
QoS SSID Policy			Egress	Search or Select
Egress	platinum x v		Ingress	Search or Select
Ingress	platinum-up 🗙 🔻		Flow Monitor	IPv6
QoS Client Policy			Egress	Search or Select
Egress	AutoQos-4.0-wlan		Ingress	Search or Select
Ingress	AutoQos-4.0-wlan			
SIP-CAC				
Call Snooping	Ο			
Send Disassociate	Ο			
Send 486 Busy	Ο			

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"

dit Policy	Profile				
General	Access Policies	QOS and AVC	Mobility	Advanced	
WLAN T	imeout			Fabric Profile	Search or Select
Session T	ïmeout (sec)	0		mDNS Service Policy	default-mdns-service Clear
Idle Time	out (sec)	43200		Hotspot Server	Search or Select 🔹
Idle Thres	hold (bytes)	0		User Private Netwo	ork
Client Exc	lusion Timeout (sec)	D 60		Status	0
Guest LA	N Session Timeout	0		Drop Unicast	0
DHCP				Umbrella	
IPv4 DHC DHCP Se	P Required	0		Umbrella Parameter Map	Not Configured
now more	>>>			Flex DHCP Option for DNS	ENABLED
AAA Pol	icy			DNS Traffic Redirect	IGNORE
Allow AA	A Override	0		WLAN Flex Policy	
NAC Stat	e	0		VLAN Central Switch	ning 🖸
Policy Na	me	default-aaa-policy x	•	Split MAC ACL	Search or Select
Accountir	ng List	Search or Select	•	Air Time Fairness I	Policies
				2.4 GHz Policy	Search or Select
				5 GHz Policy	Search or Select 🔹

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

Network Settings and

Configuration * > Radio Configurations * > Network

General					
5 GHz Netwo	ork Status				
5 GHz Netwo Threshold,	ork is operational. Co DTPC Support will n	onfiguring Beaco esult in loss of co	n Interval, Fragme	entation hts.	
Beacon Inter	val*	100			
Fragmentatic Threshold(by	on /tes)*	2346			
DTPC Suppo	ort				
Tri-Radio Mo	ode	Ο			
CCX Locati	on Measurement				
Mode		0			
Data Rates					
🛕 5 GHz Ne	etwork is operationa loss of conr	I. Configuring Date the clients	ata Rates will resu ₃.	lt in	
6 Mbps	Disabled	9 Mbps	Disabled	 12 Mbps 	Mandatory v
18 Mbps	Supported	24 Mbps	Mandatory	▼ 36 Mbps	Supported 🔻
48	Supported	54	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.

Configuration * > Radio Configurations * > Network

GHz Band	2.4 GHz Band						
General							
2.4 GHz Netv	vork Status						
A 2.4 GH Status, Beacor Su	z Network is operation n Interval, Short Pream oport will result in loss	nal. Configurin nble, Fragmen of connectivi	g 802.11g Netw tation Threshold, ty of clients.	ork DTPC			
802.11g Net	work Status						
Beacon Inter	/al*	100					
Short Preamb	ble						
Fragmentatio Threshold(by	n tes)*	2346					
DTPC Suppo	rt						
CCX Locatio	on Measurement						
Mode		O					
Data Rates							
A 2.4 GHz N	etwork is operational. loss of connec	Configuring D tivity of clients	Data Rates will re s.	sult in			
1 Mbps	Disabled 🔻	2 Mbps	Disabled	•	5.5 Mbps	Disabled	•
6 Mbps	Disabled 🔻	9 Mbps	Disabled	•	11 Mbps	Disabled	•
12 Mbps	Mandatory v	18 Mbps	Supported	¥	24 Mbps	Supported	•
36 Mbps	Supported v	48 Mbps	Supported	¥	54 Mbps	Supported	•

Ascom recommends disabling the lowest data rates and have 12Mbps as lowest data rate.

Configuration * > Radio Configurations * > Parameters

5 GHz Band 2.4 GHz B	Band			
▲ 5 GHz Network is operat	ional. Configuring EDCA Profile and D connectivity o	FS Channel Switch of clients.	Announcement Mode will re	esult in loss of
EDCA Parameters			11ax Parameters	
EDCA Profile	optimized-voice		Target Wakeup Time	
DFS (802.11h)			Target Wakeup Time Broadcast	
A DTPC Support is ena to configu	bled. Please disable it at Network re Power Constraint		Multiple Bssid	
Power Constraint*	0		BSS Color	
Channel Switch Status	Ø			
Channel Switch Announcement Mode	Loud			
Smart DFS				

- 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.

Configuration * > Wireless * > Access Points

✓ All Access Points

Number of AP(s): 2

AP Name	AP × Model	Slots 🖂	Admin Status	IP v Address	Base Radio MAC	AP ⊻ Mode	Operation Status	Policy Y Tag	Site 🗹 Tag	RF × Tag	Tag Source	Location	n × c
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	U
AP0CD0.F894.1350	C9117AXI- B	2	0	172.20.94.58	0cd0.f895.00e0	Local	Registered	default- policy-tag	default- site-tag	default- rf-tag	Default	default location	U
⊲ ⊲ 1 ⊩	10 🔻 it	tems per pa	ge								1 - 2 of 2	access point	s C
4													×.
5 GHz Radios	\$												
Number of AP(s): 2													
Number of AP(s): 2 AP Name	Slot No	Base Ra	idio MAC	Admin Status	 Operation Status 	Policy Tag	∽ Site	Tag 🖂	RF Tag	~ c	hannel		vel O
AP Name	Slot No	Base Ra	dio MAC	Admin Status	 Operation Status 	Policy Tag	✓ Site icy-tag defa	Tag ∽ ult-site-tag	RF Tag default-rf	✓ C	hannel 49,153)	Power Le 5/7 (7 dB	wel 0 m)
Number of AP(s): 2 AP Name AP00A6.CA36.210E AP0CD0.F894.1350	Slot No	Base Ra 006b.f1 0cd0.f8	dio MAC 55.1820 95.00e0	 Admin Status O O 	 Operation Status O 	Policy Tag default-pol default-pol	 Site icy-tag defa icy-tag defa 	Tag ∽ ult-site-tag ult-site-tag	RF Tag default-rf default-rf	→ C -tag (1 -tag (1	hannel 49,153) 49,153)	Power Le 5/7 (7 dB 6/8 (8 dB	wel 1 m) m)

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

Edit Radios 5 GHz Ban	d		
Configure Detail			
General		RF Channel Assignment	1
AP Name	AP00A6.CA36.210E	Current Channel	149
Admin Status	ENABLED	Channel Width	20 MHz 🔹
CleanAir Admin Status	ENABLED	Assignment Method	Custom 🔻
Antenna Parameters		Channel Number	149 🔻
Antenna Type	Internal 🔻	Tx Power Level Assignm	nent
Antenna Mode	Omni	Current Tx Power Level	5
Antenna A		Assignment Method	Custom 🔻
Antenna B		Transmit Power	5 🔹
Antenna C	\square		
Antenna D	Ø		
Antenna Gain	10		

¢°

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.

- 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.
- Using 40 MHz channels (or "channel-bonding") will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 20MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.
- 3. Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.
- 4. 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.

*) Dynamic Frequency Selection (radar detection)

Edit parameters for 1	001	ACRES OF THE	X
Device type: i62	Protector		
Parameter definition: 14.	350		
	Name	Value	
General	Network name		0
Network A	DHCP mode	On	0
Network B	802.11 protocol	802.11a/n	0
Network D	SSID	CiscoIntopPSK	0
Pevice	Security mode	WPA-PSK & WPA2-PSK	0
	WPA-PSK passphrase	******	•
	Voice power save mode	U-APSD	0
	802.11a/n channels	Non DFS	•
	Advanced: 802.11 channels		2
	World mode regulatory domain	World mode (802.11d)	2
	Transmission power	Automatic	2
	IP DSCP for voice	0x2E (46) - Expedited Forwarding	2
Push-To-Talk	IP DSCP for signaling	0x1A (26) - Assured Forwarding 31	2
Headset	TSPEC Call Admission Control	Off	2
User Profiles	Transmit gratuitous ARP	Yes	•
System Profiles	Deauthenticate on roam	No	•
	Roaming methodology	802.11 roaming	•
	Maximum transfer unit	1400	•
	Aruba 800 controller compability	No	•
	Check IP connectivity after roaming	No	•
		ОК	Cancel

Network settings for WPA2-PSK

Note. Make sure that the enabled channels in the i62 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)

👸 Ascom Device	Manager							
File Device Num	ber App Templa	te License Option	ns Help					
DEVICES	123 NUMBERS	APPS	TEMPLATES	3	LICENSES			
Device types:	Search for: 1012		in: Numb	ber	✓ Show all			
(All)	Description	Number	Device type		Parameter defi Device	e ID	DECT Master	Device Interface
Ascom Myco Back Charger		1012	i62 Protector		14 330 000138	1178FF		
i62 Messenger				N	lew			
i62 Protector				E	dit parameters			
				E	dit description			
			[N	1anage Certificates			
				C	ору			
				R	ename			
				E	xport			
				S	ave			

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	13
Fail	3
Comments	1
Not validated	5
Total	20

Refer to the attached file for detailed validation results.

Refer to the validation specification for explicit information regarding each validation case. The specification can be found here (requires login): <u>https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability/Templates/</u>

Document History

Rev	Date	Author	Description	
P1	3-Nov-20	SEKMO	Draft	
R1	9-Nov-20	SEKMO	Internal review. R1	