INTEROPERABILITY REPORT

Ascom i63 Juniper Mist

Cloud-Managed Wi-Fi platform Ascom i63 v. 5.0.2 Utrecht, The Netherlands February 2024

ascom

Contents

ntroduction	. 3
Test site	4
Participants	4
Test topology	4
General conclusions	5
Compatibility information	5
Verification overview	. 6
Appendix A: Validation Configurations	. 8
Mist Cloud-Managed Wi-Fi platform	. 8
Appendix B: Interoperability Validation Records	14
Document History	14

Introduction

This document summarizes interoperability test results relating to the validation of Ascom's and the Partner's platform. It also describes recommended steps and guidelines to configure these respective platforms and provides a point of contact for inquiries. The report should be used in conjunction with configuration guides from Ascom and the Partner.

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 Mist

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Juniper Networks (NYSE: JNPR), founded in 1996 and headquartered in Sunnyvale, CA, is a global leader in Al Networking, Cloud and Connected Security Solutions.

Site Information

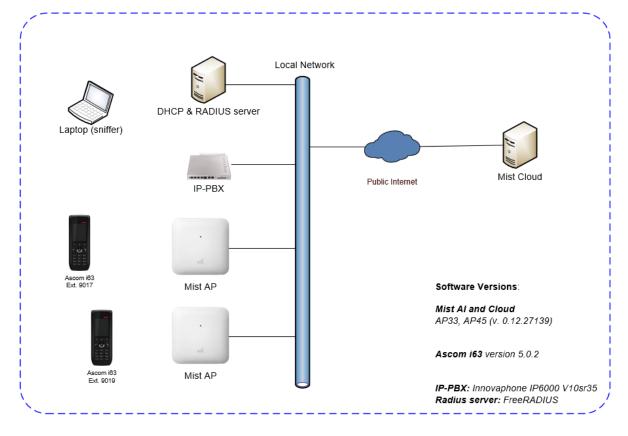
Test site

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 regards to the tested areas of authentication, stability, roaming, QoS and power save.

This test is considered a regression test and some test cases that have previously been tested on the 0.10.x track have been left out. Test cases left out includes for example battery measurement and capacity tests.

To maintain optimal roaming performance, it is recommended to enable Fast Roaming (802.11r/FT) both when using PSK or 802.1X based Authentication.

Compatibility information

One Access point model from every product generation has been selected as a representation (AP33 and AP45). By testing these access points, we are considered to cover all supported major Juniper Mist access points based on chipset compatibility listed below.

Supported Partner Access Points with SW version 0.12.27139:

AP12 AP32 AP33 AP41 AP43 AP45 AP61

AP63

Interoperability Report Ascom i63 – Juniper Mist

Verification overview

WLAN Compatibility and Performance

High Level Functionality	Result	Comments
Association, Open with No Encryption	ОК	
Association, WPA2-PSK / AES Encryption	ОК	
Association, PEAP-MSCHAPv2 Auth, AES Encryption	ОК	
Association with EAP-TLS authentication	ОК	
Association, Multiple ESSIDs	ОК	
Beacon Interval and DTIM Period	ОК	DTIM Period = 2, Option to change this value in the GUI can be activated by Juniper Mist Support if required/requested
PMKSA Caching	ОК	
WPA2-opportunistic/proactive Key Caching	ОК	
WMM Prioritization	ОК	
802.11 Power-save mode	ОК	
802.11e U-APSD	ОК	
Roaming, WPA2-PSK, AES Encryption	ОК	Typical roaming time 46ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	ОК	Typical roaming time 39ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	ОК	Typical roaming time 50ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	ОК	Typical roaming time 40ms
Channel usage controlled by 802.11k	ОК	

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 **<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

Mist Cloud-Managed Wi-Fi platform

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

General settings (SSID, Authentication, Radio and QoS)

Mist	••• ASCOMNL					FRI, 10:06 AM 🖉 💡 🅐
Monitor	 Site Configuration : Mist-Certification 					Clone Site Save Cancel
Marvis™						
Clients	Information	Location		required	Mist Tunnels Add Tunnel	
• Access Points	Site Name required		(or click on the map)	- Counco	WISC TOTILES	
	Mist-Certification	Street address	or latitude, longitude		VLAN ID(s) Protocol AP Subnets Primary Cluster Secondary	
Switches	Site ID		NZ30	DIU		
+ WAN Edges	0ca9f30d-79a8-49b5-9248-01585227c96a	Maar	oud-Zuilen	Groenekan		
Mist Edges	Country required	VL.	EUTEN	De Bilt		
	Netherlands 🗸	armelen N198	EIDSCHE RIJN	trecht		
✓ Location	Time Zone	A12		Gi		
DO Analytics	Europe/Amsterdam (GMT +01:00/+02:00)	Achthoven-West	1228 A2 A12	Netti Bunnik	Radius Proxy O Enabled Disabled	
🔒 Site		+		1408 N421		
	Notes		Jutphaas	Houten	Upstream Resource Monitoring	
Organization	Add Notes	-	Nieuwegein Man Catallit		O Enabled Disabled	
		Crossbills	Map Satellit	e Iap data ©2023 Terms of Use		
		Street Address			Site Variables Add Variable	
	RF Template		982, 3528 BD Utrecht, Ne		Variables Values	
	Ascom-4-channel	Latitude 52.067973		gitude 5.082844		
	Site Groups	Engagement	Analytics			
	+	Enable				
		Dwell Time Cate	gories (value in seconds l	between 0 and 24 hours)		
		Categories	Min dwell	Max dwell		
	AP Firmware Upgrade	Passerby	1	300		
	Enable Auto Update	Customer	301	14400		
	Upgrade Version	Associate	14401	28800		
	 Auto upgrade to production firmware 	Asset	28801	42000		
	 Auto upgrade to rc2 firmware 	Active Hours				
	Auto upgrade to custom firmware <u>Select Version</u>	David	61	T = 1		
	Upgrade Schedule	Day Sunday	Start	End		
	(Scheduling for the first time must be done 2 hours prior to scheduled time)	Monday	12:00 AM •	12:00 AM •		
	Time of Day required Day of Week	Tuesday	12:00 AM 🔻	12:00 AM 👻		
	2:00 am 👻 Day: Daily 👻	Wednesday	12:00 AM 🔻	12:00 AM 🔻		
		Thursday	12:00 AM 🔻	12:00 AM 👻		

Organization > Admin > Site Configuration

- Define Site Name.
- Select Country (Regulatory Domain inferred from this setting).
- Select Time Zone.
- Select location.

Please refer to Mist's documentation on how to create a Mist account, organization, sites, templates, networks and the claiming of access points to an organization. Only after the latter can devices be assigned to a site.

Mišt	ascomnl			FRI, 11:02 AM 🖉 🖓 🕐
	-			Delete WLAN Save Cancel
	WLANS : MistintopPSK A This is a Template WLAN. To view or make any changes to this	r WI AN places visit WI AN Tamplata - MictintonDCK		
000 Marvis™	A This is a remplate work. To view of make any changes to the	s work please visit <u>work reinplate, wistintop, sk</u>		
Clients	SSID	Security	Apply to Access Points	
• Access Points	MistIntopPSK	Security Type	All APs AP Labels Specific APs	
Switches	WLAN ID	WPA3 WPA2 OWE Open Access		
+ WAN Edges	641f5422-fc58-4484-ad89-044cd209d9c3	Enterprise (802.1X) Personal (PSK)		
Mist Edges		Passphrase Reveal		
	WLAN Status	O Multiple passphrases	Isolation	
✓ Location	Enabled Disabled Hide SSID	MAC address authentication by RADIUS lookup	Prohibit peer to peer communication	
00 Analytics	Broadcast AP name	Prevent banned clients from associating	Disabled Same AP Same Subnet	
Site	Radio Band	Edit banned clients in Network Security Page	Filtering (Wireless)	
Organization	🖾 2.4 GHz 🖾 5 GHz 🗌 6 GHz	Fast Roaming	Broadcast/Multicast	
W	Band Steering	Default	Allow mDNS	
	Enable	.11r	Allow SSDP	
		L	Allow IPv6 Neighbor Discovery	
	Client Inactivity	VLAN	Ignore Broadcast SSID Probe Requests	
	Drop inactive clients after seconds: 1800	Untagged Tagged Pool Dynamic		
			Custom Forwarding	
	Geofence	Guest Portal	Custom Forwarding will be disabled for Untagged VLAN	
	Minimum client RSSI (2.4G)		Custom Forwarding to Eth0 + PoE *	
	Minimum client RSSI (5G)	 No portal (go directly to internet) Custom guest portal 		
	Minimum client RSSI (6G)	Custom guest portai Forward to external portai	SSID Scheduling	
	Block clients having RSSI below the minimum	SSO with Identity Provider	Enabled Disabled	
		Bypass guest/external portal in case of exception		
	Data Datas		QoS Priority	
	Data Rates		Override QoS	
	 Compatible (allow all connections) No Legacy (2.4G, no 11b) 		Covernue gus	
	High Density (disable all lower rates)			
	Custom Rates		AirWatch	
	2.4G Custom Rates		 Enabled Disabled 	
	1 • 2 • 5.5 •			
	6 • 9 • 11 •		Bonjour Gateway	
	12 Mandatory 18 Supported 24 Supported		O Enabled Disabled	
	36 Supported 👻 48 Supported 👻 54 Supported 👻			
	5G Custom Rates			
	6 • 9 • 12 Mandatory •			
	18 Supported + 24 Mandatory + 36 Supported +			
	48 Supported 👻 54 Supported 👻			
	WiFi Protocols			
	WiFi-6 Enabled Disabled			
	WLAN Rate Limit			
	Limit uplink to 10 Mbps *			
	Limit downlink to 20 Mbps *			
	Per-Client Rate Limit			
	Limit uplink to 512 Kbps -			
	Limit downlink to 1			
	Application Rate Limit			
	 Enabled			—
				-

Example of how to configure the system for WPA2-PSK authentication.

Site > Wireless > WLANs

- Define SSID
- Select Security Type (WPA2 Personal (PSK)
- Enter WPA2 Pre-shared key (passphrase)

Mist	ascomnl			FRI, 11:29 AM 🖉 🖗 🕐
Monitor	- Mictiptop1V			Delete WLAN Save Cancel
Marvis™	 WLANS : Mistintop1X A This is a Template WLAN. To view or make any changes to thi 	s WLAN please visit <u>WLAN Template : MistIntop1X</u>		
്റ്റ Clients				
	SSID	Security	Apply to Access Points	
Access Points	MistIntop1X	Security Type	All APs AP Labels Specific APs	
Switches	WLAN ID	WPA3 WPA2 OWE Open Access		
+ WAN Edges	70519279-6460-4ab0-87ee-6b1aa65322f9	Enterprise (802.1X) Personal (PSK)		
		MAC address authentication by RADIUS lookup		
Mist Edges	WLAN Status	Prevent banned clients from associating	Isolation	
✓ Location	Enabled O Disabled	Edit banned clients in <u>Network Security Page</u>	Prohibit peer to peer communication	
00 Analytics	Hide SSID	Fast Roaming	Disabled O Same AP O Same Subnet	
	Broadcast AP name		Filtering (Wireless)	
Site	Radio Band	Opportunistic Key Caching (OKC)	ARP	
Organization	🖾 2.4 GHz 🖾 5 GHz 🗌 6 GHz	.11r	Broadcast/Multicast	
	Band Steering		Allow mDNS Allow SSDP	
	Enable	802.1X Web Redirect	Allow SSDP Allow IPv6 Neighbor Discovery	
	Client Inactivity	Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect AVP	Ignore Broadcast SSID Probe Requests	
	Drop inactive clients after seconds: 1800	O Enabled Disabled		
			Custom Forwarding	
	Geofence	Hotspot 2.0	Custom Forwarding will be disabled for Untagged VLAN	
	Minimum client RSSI (2.4G)	Enabled Disabled	Custom Forwarding to Eth0 + PoE -	
	Minimum client RSSI (5G) 0			
	Minimum client RSSI (6G) 0	Authentication Servers	SSID Scheduling	
	Block clients having RSSI below the minimum	RADIUS	Enabled Disabled	
		DADUUS Authoritien Comun		
	Data Rates	RADIUS Authentication Servers	QoS Priority	
	 Compatible (allow all connections) 	10.30.174.5 : 1812 primary 🛩	Override QoS	
	 No Legacy (2.4G, no 11b) 	Add Server		
	High Density (disable all lower rates) Custom Rates	RADIUS Accounting Servers	AirWatch	
	2.4G Custom Rates	Enable Interim Accounting	Enabled Disabled	
		No accounting servers defined		
	1 • 2 • 5.5 • 6 • 9 • 11 •	Add Server	Bonjour Gateway	
	12 Mandatory 18 Supported 24 Supported	Randomize authentication and accounting server per		
	36 Supported → 48 Supported → 54 Supported →		Enabled Disabled	
	5G Custom Rates	NAS Identifier		
	6 • 9 • 12 Mandatory •			
	18 Supported 24 Mandatory 36 Supported	NAS IP Address		
	48 Supported 👻 54 Supported 👻			
	WiFi Protocols	CoA/DM Server		
	WiFi-6 Enabled Disabled	 Enabled Disabled 		
	WLAN Rate Limit	VLAN		
	Limit uplink to 10 Mbps *	Untagged O Tagged O Pool O Dynamic		
	Limit downlink to 20 Mbps *			
		Guest Portal		
	Per-Client Rate Limit	No portal (go directly to internet)		
	Limit uplink to 512 Kbps *	Custom guest portal		
	Limit downlink to 1 Mbps *	Forward to external portal		
	Application Rate Limit	 SSO with Identity Provider Bypass guest/external portal in case of exception 		
	 Enabled Disabled 	Jees one and a provide of exception		_

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

Site > Wireless > WLANs

- Define SSID
- Select Security Type (WPA2 Enterprise (802.1X)
- Define a RADIUS server.

NOTE: To accomplish optimal roaming performance with WPA2, it is recommended to enable Fast Roaming (802.11r/FT) when using PSK or 802.1X authentication.

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

Ascom recommends only using channels 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:

- For environments not utilizing 802.11k Neighbor Report Enabling more than 8 channels in the system will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels in the system can be allowed. Ascom does not recommend exceeding these limits unless 802.11k is in use.
- 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 nonoverlapping 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.

vice type: i63 Messenger			
Network Name Image: Second state	and e e 2.11 channels neighbor list omain roice ignaling dmission Control hod et aggregation	Value PSK On 5 GHz MistIntopPSK WPA/WPA2-Personal ************************************	

Network settings for WPA2-PSK

- Make sure that the enabled channels in the i63 handset match the channel plan used by the WLAN 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".

Edit parameters for 90	011		×
Device type: i63 Messenge	r		
Image: Network Image: Network Image: Network B Image: Network B Image: Network B Image: Network B Image: Network C Image: Network D Image: Network D <th>Name Network name DHCP mode Frequency band SSID Security mode EAP method EAP authentication identity EAP authentication password EAP authentication password EAP authentication password EAP authentication identity EAP authentication password EAP authentication identity EAP authentication password EAP authentication identity EAP authenticate on roam</th> <th>Value MSCHAP On 5 GHz MistIntop 1X WPA2-Enterprise PEAP-MSCHAPv2 testuser ************************************</th> <th>8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8</th>	Name Network name DHCP mode Frequency band SSID Security mode EAP method EAP authentication identity EAP authentication password EAP authentication password EAP authentication password EAP authentication identity EAP authentication password EAP authentication identity EAP authentication password EAP authentication identity EAP authenticate on roam	Value MSCHAP On 5 GHz MistIntop 1X WPA2-Enterprise PEAP-MSCHAPv2 testuser ************************************	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8
		OK	Cancel

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

- Make sure that the enabled channels in the i63 handset match the channel plan used by the WLAN 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".

🎒 Ascom Devic	e Manager											-		×
File Device Num	nber App Templa	ate License O	ptions Help											
DEVICES	123 NUMBERS	APPS	TEMPLATES											
Device types:	Search for:		in: Descrip	tion v	Show a	1								
(All)	Description	Number	Device type	Parameter defin	nition	Device ID	DECT Mas	Device Int	Online	Status	Saved	Last login	Last ru	
i63 Messenger		9010	i63 Messenger	OK		000125055007			\checkmark	Synchronized	\checkmark	2023-06	CiscoInt	
i63 Protector		9011	i63 Messenger	ок	N	ew			1	Synchronized	1	2023-06	CiscoInt	
		9012	i63 Messenger	OK	Ed	lit parameters			1	Synchronized	1	2023-06	CiscoInt	
		9013	i63 Messenger	OK					1	Synchronized	1	2023-06	CiscoInt	
		9014	i63 Messenger	OK	Ec	lit description	_		1	Synchronized	1	2023-06	CiscoInt	
		9015	i63 Messenger	OK	M	anage Certificates			1	Synchronized	1	2023-06	CiscoInt	
		9016	i63 Messenger	OK	C	opy	-			Not synched	×	2023-06	CiscoInt	

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	12
Fail	0
Comments	9
Not verified	9
Total	30

Refer to the attached file for detailed verification results.

Document History

Rev	Date	Author	Description
D1	01-February-2024	NLRPa	Initial draft
P1	15-February-2024	NLRPa	Minor adjustment after internal review