

INTEROPERABILITY REPORT

Ascom Myco 3

Juniper Mist

Cloud-Managed Wi-Fi platform

Ascom Myco 3 v. 3.5.8

Utrecht, The Netherlands

February 2024

ascom

Contents

Introduction.....	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.....	15
Document History	15

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 AI Networking, Cloud and Connected Security Solutions.

Site Information

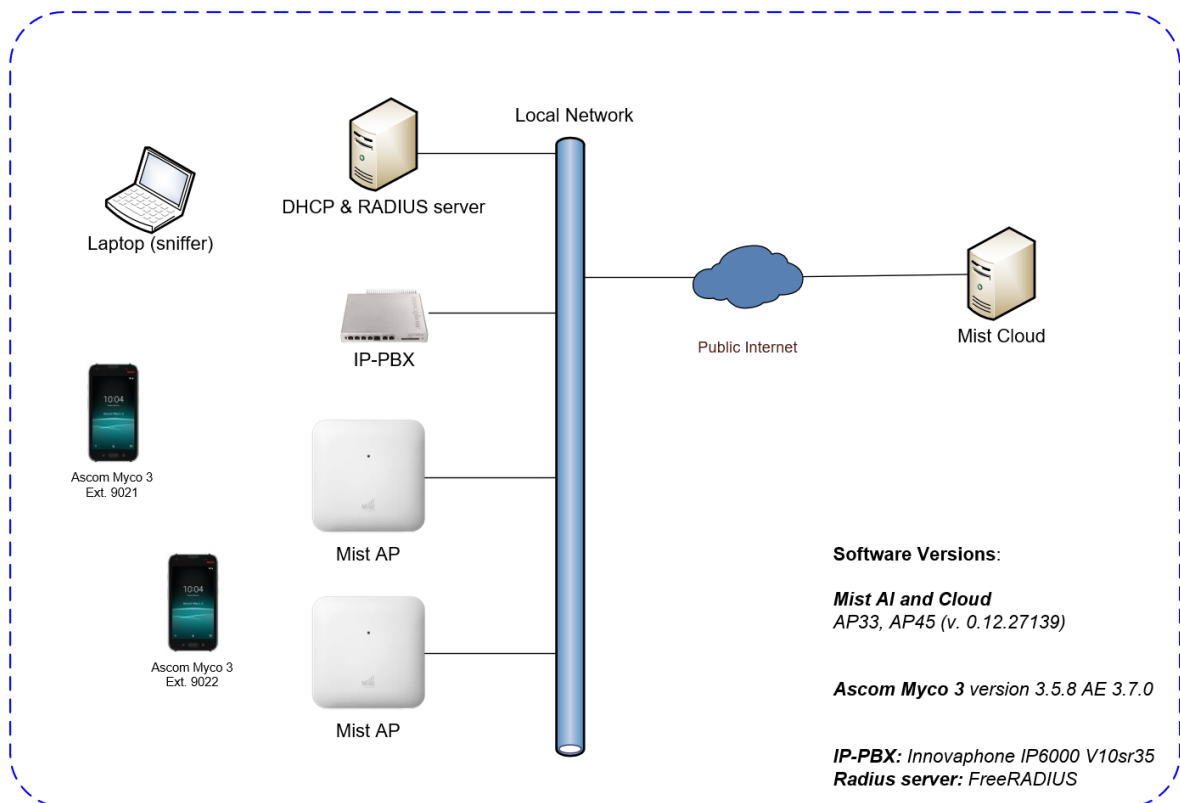
Test site

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 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 (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

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	DTIM Period = 2, <i>Option to change this value in the GUI can be activated by Juniper Mist Support if required/requested</i>
PMKSA Caching	OK	
WPA2-opportunistic/proactive Key Caching	OK	802.11/FT-roaming strongly recommended
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	N/T	Myco 3 is not using U-APSD
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 81ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 75ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 116ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 78ms
Channel usage controlled by 802.11k	OK	
Network features controlled by 802.11v	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 or support@ascom.com.

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

Appendix A: Validation Configurations

Juniper 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 Myco 3 handset. Please note that security settings were modified according to requirements in individual test cases.

General settings (SSID, Authentication, Radio and QoS)

The screenshot shows the 'Site Configuration' page for a site named 'Mist-Certification'. The page is divided into several sections:

- Information:** Site Name (Mist-Certification), Site ID (0ca9f30d-79a8-49b5-9248-01585227c96a), Country (Netherlands), Time Zone (Europe/Amsterdam (GMT +01:00/+02:00)).
- Location:** Location Search (or click on the map), Street address or latitude, longitude. A map of Utrecht, Netherlands, is shown with a red box highlighting the location details.
- Notes:** Add Notes.
- RF Template:** Ascom-4-channel.
- Site Groups:** Add Site Group.
- AP Firmware Upgrade:** Enable Auto Update, Upgrade Version (Auto upgrade to production firmware, Auto upgrade to rc2 firmware, Auto upgrade to custom firmware Select Version), Upgrade Schedule (Scheduling for the first time must be done 2 hours prior to scheduled time), Time of Day (2:00 am), Day of Week (Daily).
- Engagement Analytics:** Enable, Dwell Time Categories (value in seconds between 0 and 24 hours), Categories (Passerby, Customer, Associate, Asset), Min dwell, Max dwell, Active Hours (Day, Start, End).
- Mist Tunnels:** Add Tunnel, VLAN IDs, Protocol, AP Subnets, Primary Cluster, Secondary.
- Radius Proxy:** Enabled, Disabled.
- Upstream Resource Monitoring:** Enabled, Disabled.
- Site Variables:** Add Variable, Variables, Values.

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.

WLANs : MistIntopPSK

SSID
MistIntopPSK

WLAN ID
641f5422-fc58-4484-ad89-044cd209d9c3

WLAN Status
☒ Enabled ☐ Disabled
☐ Hide SSID
☐ Broadcast AP Name

Radio Band
☒ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

Band Steering
☐ Enable

Client Inactivity
 Drop inactive clients after seconds: 1800

Geofence
☐ Minimum client RSSI (2.4G) 0
☐ Minimum client RSSI (5G) 0
☐ Minimum client RSSI (6G) 0
 Block clients having RSSI below the minimum

Data Rates
☐ Compatible (allow all connections)
☐ No Legacy (2.4G, no 11b)
☐ High Density (disable all lower rates)
☒ Custom Rates

2.4G Custom Rates
 1 2 5.5
 6 9 11
 12 Mandatory 18 Supported 24 Supported
 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 Mbps

Application Rate Limit
☐ Enabled ☒ Disabled

Security
 Security Type
 WPA3 WPA2 **OWE** Open Access
 Enterprise (802.1X) **Personal (PSK)**
☒ Passphrase ***** **Reveal**
☐ Multiple passphrases

Fast Roaming
☐ Default
☒ .11r

VLAN
☒ Untagged ☐ Tagged ☐ Pool ☐ Dynamic

Guest Portal
☒ No portal (go directly to internet)
☐ Custom guest portal
☐ Forward to external portal
☐ SSO with Identity Provider
☒ Bypass guest/external portal in case of exception

Apply to Access Points
 All APs AP Labels Specific APs

Isolation
 Prohibit peer to peer communication
☒ Disabled ☐ Same AP ☐ Same Subnet

Filtering (Wireless)
☒ ARP
☒ Broadcast/Multicast
☐ Allow mDNS
☐ Allow SSDP
☐ Allow IPv6 Neighbor Discovery
☐ Ignore Broadcast SSID Probe Requests

Custom Forwarding
 Custom Forwarding will be disabled for Untagged VLAN
☐ Custom Forwarding to Eth0 + PoE

SSID Scheduling
☐ Enabled ☒ Disabled

QoS Priority
☐ Override QoS

AirWatch
☐ Enabled ☒ Disabled

Bonjour Gateway
☐ Enabled ☒ Disabled

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)

The screenshot displays the MistIntop1X configuration page. The left sidebar contains navigation options: Monitor, Marvis, Clients, Access Points, Switches, WAN Edges, Mist Edges, Location, Analytics, Site, and Organization. The main content area is titled 'WLANs : MistIntop1X' and includes a warning: 'This is a Template WLAN. To view or make any changes to this WLAN please visit WLAN Template : MistIntop1X'. The configuration is organized into several panels:

- SSID:** Contains the WLAN ID '70519279-6460-4ab0-87ee-6b1aa65322f9'.
- WLAN Status:** Includes options for Enabled/Disabled, Hide SSID, and Broadcast AP name.
- Radio Band:** Options for 2.4 GHz, 5 GHz, and 6 GHz.
- Band Steering:** Option to Enable.
- Client Inactivity:** Option to Drop inactive clients after a specified time (1800 seconds).
- Geofence:** Options for Minimum client RSSI (2.4G, 5G, 6G) and Block clients having RSSI below the minimum.
- Data Rates:** Includes sections for 2.4G Custom Rates and 5G Custom Rates with dropdown menus for various rates (e.g., 12 Mandatory, 18 Supported, 24 Supported, 36 Supported, 48 Supported, 54 Supported).
- WIFI Protocols:** Option to Enable/Disable.
- WLAN Rate Limit:** Options for Limit uplink/downlink and Per-Client Rate Limit.
- Application Rate Limit:** Option to Enable/Disable.
- Security:** Includes Security Type (WPA3, WPA2, DWE, Open Access) and Enterprise (802.1X) / Personal (PSK) options. It also has checkboxes for MAC address authentication, Prevent banned clients, and Edit banned clients.
- Fast Roaming:** Includes options for Default, Opportunistic Key Caching (OKC), and 802.11r.
- 802.1X Web Redirect:** Option to Enable/Disable.
- Hotspot 2.0:** Option to Enable/Disable.
- Authentication Servers:** Includes RADIUS Authentication Servers (10.30.174.5 : 1812) and RADIUS Accounting Servers.
- NAS Identifier:** Field for NAS Identifier.
- NAS IP Address:** Field for NAS IP Address.
- CoA/DM Server:** Option to Enable/Disable.
- VLAN:** Options for Untagged, Tagged, Pool, and Dynamic.
- Guest Portal:** Options for No portal, Custom guest portal, Forward to external portal, SSO with Identity Provider, and Bypass guest/external portal.
- Apply to Access Points:** Options for All APs, AP Labels, and Specific APs.
- Isolation:** Options for Prohibit peer to peer communication, Disabled, Same AP, and Same Subnet.
- Filtering (Wireless):** Includes ARP, Broadcast/Multicast, Allow mDNS, Allow SSDP, Allow IPv6 Neighbor Discovery, and Ignore Broadcast SSID Probe Requests.
- Custom Forwarding:** Option to Enable/Disable.
- SSID Scheduling:** Option to Enable/Disable.
- QoS Priority:** Option to Override QoS.
- AirWatch:** Option to Enable/Disable.
- Bonjour Gateway:** Option to Enable/Disable.

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.

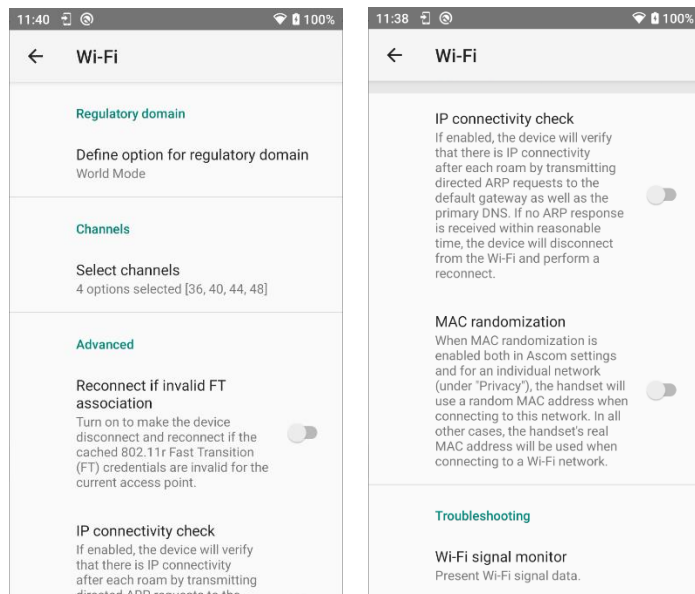
Ascom recommends only using channel 1, 6 and 11 for 802.11b/g/n. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines below.

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 Myco 3 handsets in 802.11a/n/ac environments:

- 1. 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.**
- 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.**

Ascom Myco 3 Wi-Fi settings



Settings -> Ascom settings -> Wi-Fi

- Select Regulatory domain according to your region.
- Make sure that the enabled channels in the Myco 3 match the channel plan used in the system.

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

11:47 100%

← Add network

Network name
MistIntopPSK

Security
WPA/WPA2-Personal

Password
.....

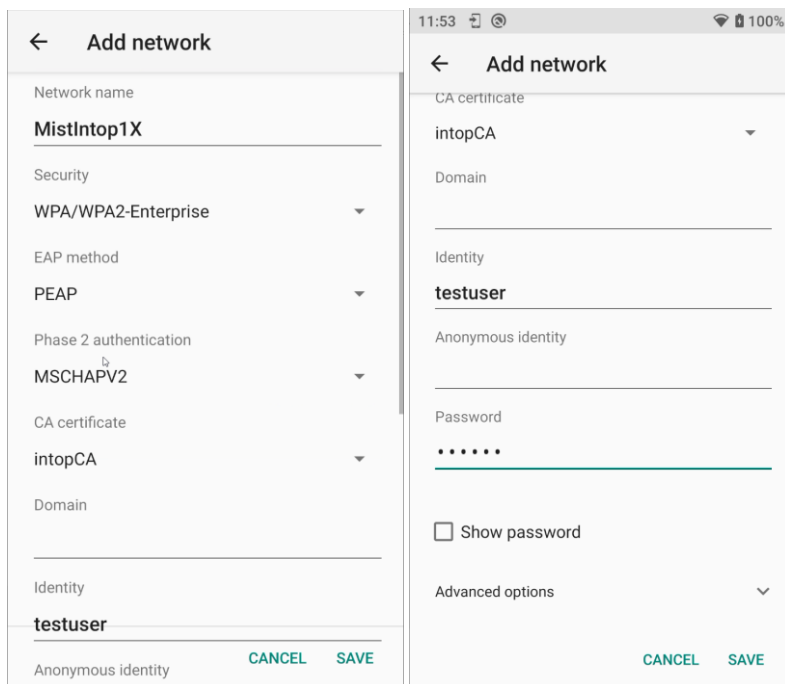
☐ Show password

Advanced options

CANCEL SAVE

Pre-shared key authentication configuration example

- Configure Network name.
- Select Security WPA/WPA2-Personal
- Enter Password



802.1X

- Configure Network name.
- Select Security WPA/WPA2-Enterprise
- Select EAP method PEAP
- Select Phase 2 authentication MSCHAPV2
- Select CA certificate
Certificates can be installed either via an MDM tool or manually.
Manual installation: Settings -> Security -> Encryption and Credentials -> Install from SD card.
- Configure Identity and Password.

Appendix B: Interoperability Validation Records

Pass	12
Fail	0
Comments	7
Not verified	11
Total	30

Refer to the attached file for detailed verification results.

Document History

Rev	Date	Author	Description
D	01-February-2024	NLRPa	Initial draft