

INTEROPERABILITY REPORT

Ascom Myco 4

Juniper Mist

Cloud-Managed Wi-Fi platform

Ascom Myco 4 v. A12_073 (AE 4.0.9)

Utrecht, The Netherlands

February 2024

ascom

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

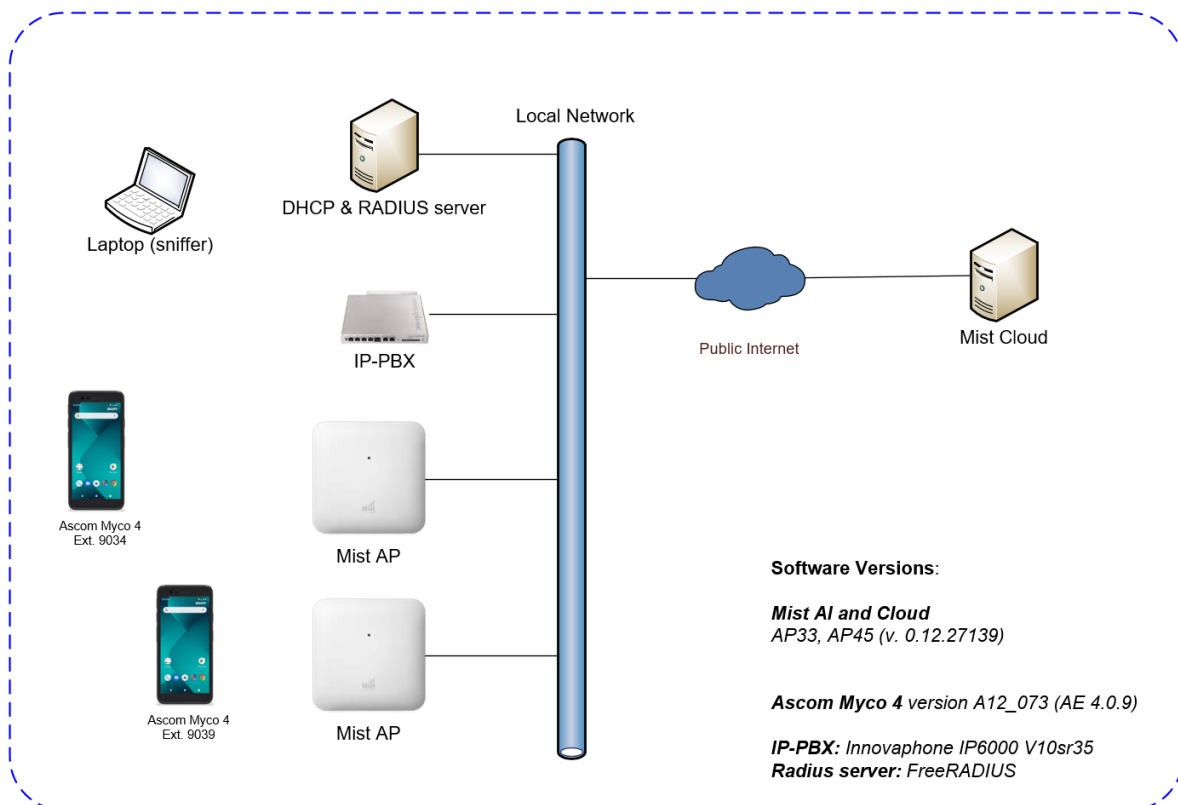
Test site

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

To maintain optimal roaming performance, it is recommended 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 with WPA3-SAE Transition Mode | OK | |
| Association with WPA3-SAE authentication, AES encryption | OK | |
| Association with WPA3-Enterprise + FT | OK | |
| Association with Protected Management Frames 802.11w | 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 recommended |
| WMM Prioritization | OK | |
| 802.11 Power-save mode | OK | |
| 802.11e U-APSD | N/T | Myco 4 is not using U-APSD |
| Roaming, WPA2-PSK, AES Encryption | OK | Typical roaming time 66ms |
| Roaming, WPA2-PSK, AES Encryption, 802.11r/FT | OK | Typical roaming time 62ms |
| Roaming, PEAP-MSCHAPv2 Auth, AES Encryption | OK | Typical roaming time 86ms |
| Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT | OK | Typical roaming time 55ms |
| Roaming, WPA3-SAE authentication, AES encryption | OK | Typical roaming time 73ms |
| Roaming, WPA3-SAE authentication, AES encryption, 802.11r/FT | OK | Typical roaming time 61ms |
| Roaming, WPA3-Enterprise + FT | OK | Typical roaming time 60ms |
| Association, and roaming on 6 GHz | OK | Typical roaming time 83ms |
| 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.

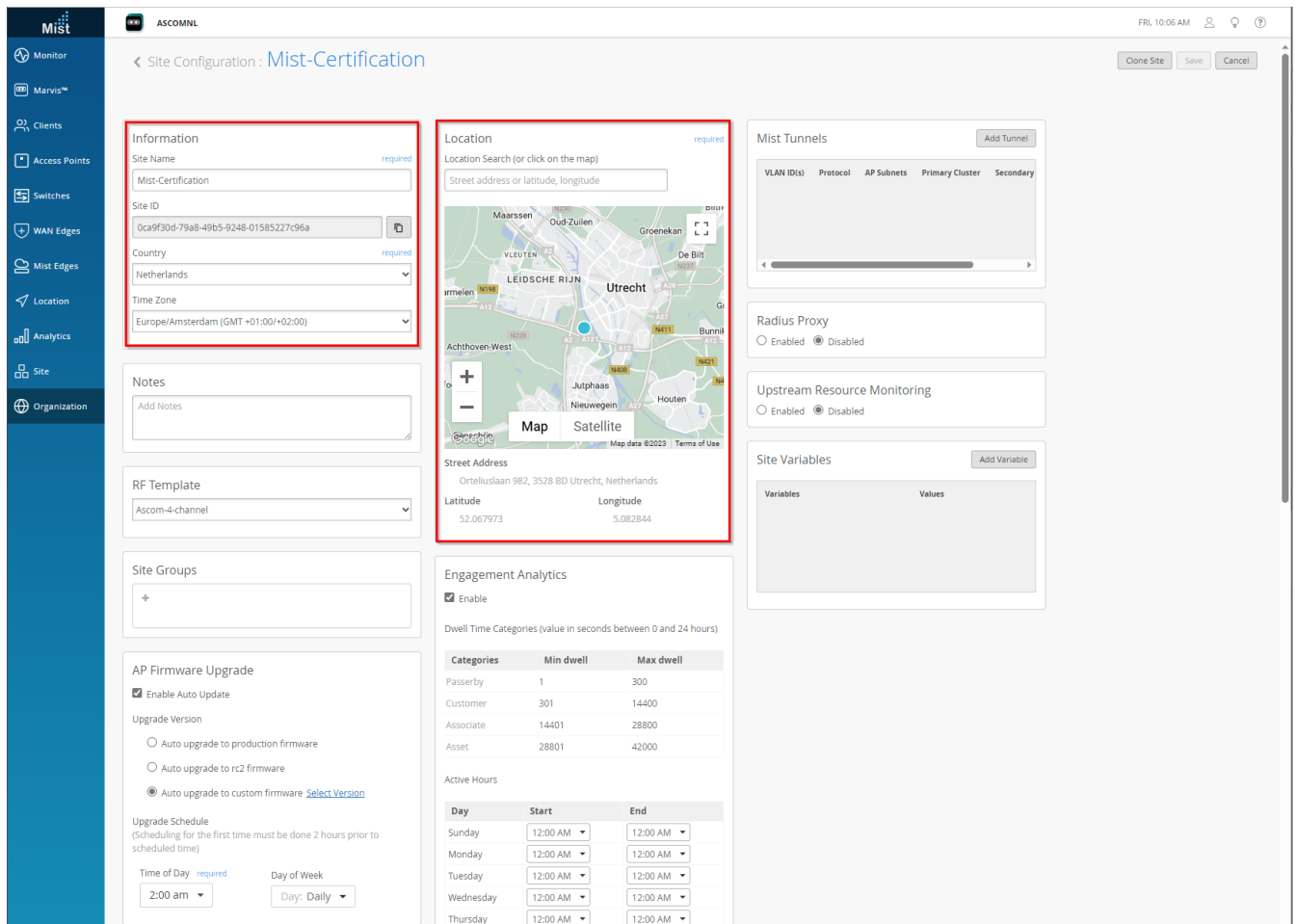
For detailed verification results, refer to Appendix B: Interoperability Validation Records.

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

General settings (SSID, Authentication, Radio and QoS)



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.

WPA2-PSK

The screenshot shows the Mist WLAN configuration page for a template named 'MistIntopPSK'. The interface is divided into several sections, with key configuration areas highlighted by red boxes:

- SSID:** 'MistIntopPSK'
- WLAN ID:** '641f5422-fc58-4484-ad89-044cd209d9c3'
- WLAN Status:** Enabled
- 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), (5G), (6G) all set to 0
- Data Rates:** Custom Rates selected. 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.
- Security:** Security Type: WPA2, WPA3, OWE, Open Access. Authentication: Enterprise (802.1X), Personal (PSK). Passphrase: [Redacted]
- Fast Roaming:** .11r
- VLAN:** Untagged
- Guest Portal:** No portal (go directly to internet)
- Apply to Access Points:** All APs
- Isolation:** Prohibit peer to peer communication: Disabled
- Filtering (Wireless):** ARP, Broadcast/Multicast, Allow mDNS, Allow SSDP, Allow IPv6 Neighbor Discovery, Ignore Broadcast SSID Probe Requests
- Custom Forwarding:** Custom Forwarding to: ETH0 + PoE
- SSID Scheduling:** Disabled
- QoS Priority:** Override QoS
- AirWatch:** Disabled
- Bonjour Gateway:** Disabled
- WiFi Protocols:** WiFi-6 Enabled
- 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:** 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)

WPA2-Enterprise (802.1X)

The screenshot displays the Mist management console for configuring a WLAN named 'MistIntop1X'. The configuration is for WPA2-Enterprise (802.1X) authentication. Key settings include:

- SSID:** MistIntop1X
- WLAN ID:** 70519279-6460-4ab0-87ee-6b1aa65322f9
- Security:** Security Type is WPA2, with Enterprise (802.1X) selected.
- Fast Roaming:** Enabled, with Opportunistic Key Caching (OKC) selected.
- Authentication Servers:** A RADIUS server is configured with IP 10.30.174.5 and port 1812.
- Data Rates:** Custom rates are defined for 2.4G and 5G bands.
- WLAN Status:** Enabled.

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.

WPA3-Personal (SAE)

The screenshot displays the Juniper Mist configuration page for a WLAN named "MistIntopWPA3". The interface is divided into several sections:

- SSID:** MistIntopWPA3
- WLAN ID:** b88d7458-7ee3-4f66-a9cc-96e0aac56a98
- WLAN Status:** Enabled
- 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), (5G), (6G)
- Data Rates:** Custom Rates (2.4G, 5G, 6G)
- Security:** Security Type: WPA3 Personal (SAE); Passphrase: [Redacted]
- Fast Roaming:** Enabled
- WLAN:** Untagged
- Guest Portal:** No portal (go directly to internet)
- Apply to Access Points:** All APs
- Isolation:** Prohibit peer to peer communication: Disabled
- Filtering (Wireless):** ARP, Broadcast/Multicast
- Custom Forwarding:** Custom Forwarding to: Eth0 + PoE
- SSID Scheduling:** Disabled
- QoS Priority:** Override QoS
- AirWatch:** Disabled
- Bonjour Gateway:** Disabled

Example of how to configure the system for WPA3-Personal (SAE) authentication.

Site > Wireless > WLANs

- Define SSID
- Select Security Type WPA3 Personal (SAE)
- Enter WPA3 Pre-shared key (passphrase)

WPA3-Enterprise (802.1X)

The screenshot shows the Juniper Mist configuration interface for a WLAN named 'MistIntopWPA3-1X'. The interface is divided into several sections:

- SSID:** 'MistIntopWPA3-1X' (highlighted with a red box).
- WLAN ID:** 'db448a89-ab15-4010-9455-3f3b1be9753e'.
- WLAN Status:** Enabled.
- 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), (5G), (6G) all set to 0.
- Data Rates:** Custom Rates selected. 2.4G Custom Rates: 1, 6, 12 Mandatory, 18 Supported, 24 Supported, 36 Supported, 48 Supported, 54 Supported. 5G Custom Rates: 6, 9, 12 Mandatory, 18 Supported, 24 Supported, 36 Supported, 48 Supported, 54 Supported. 6G Custom Rates: 6, 9, 12 Mandatory, 18 Supported, 24 Mandatory, 36 Supported, 48 Supported, 54 Supported.
- Security:** WPA3 Enterprise (802.1X) selected (highlighted with a red box). Other options include WPA3, WPA3/WPA2 Transition, OWE, and Personal (SAE).
- Fast Roaming:** .11r selected (highlighted with a red box). Other options include Default, Opportunistic Key Caching (OKC), and Zebra Compatibility.
- 802.1X Web Redirect:** Disabled.
- Hotspot 2.0:** Disabled.
- Authentication Servers:** RADIUS selected. A RADIUS Authentication Server is configured with IP 10.30.174.5 and port 1812 (highlighted with a red box).
- RADIUS Accounting Servers:** No accounting servers defined.
- NAS Identifier:** Empty field.
- NAS IP Address:** Empty field.
- CoA/DM Server:** Disabled.
- VLAN:** Untagged.
- Guest Portal:** No portal (go directly to internet).
- Apply to Access Points:** All APs.
- Isolation:** Prohibit peer to peer communication: Disabled.
- Filtering (Wireless):** ARP, Broadcast/Multicast, Allow mDNS, Allow SSDP, Allow IPv6 Neighbor Discovery, Ignore Broadcast SSID Probe Requests.
- Custom Forwarding:** Custom Forwarding to: ETH0 + PoE.
- SSID Scheduling:** Disabled.
- QoS Priority:** Override QoS.
- AirWatch:** Disabled.
- Bonjour Gateway:** Disabled.

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

Site > Wireless > WLANs

- Define SSID
- Select Security Type WPA3 Enterprise (802.1X)
- Define a RADIUS server.

NOTE: To accomplish optimal roaming performance, 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.

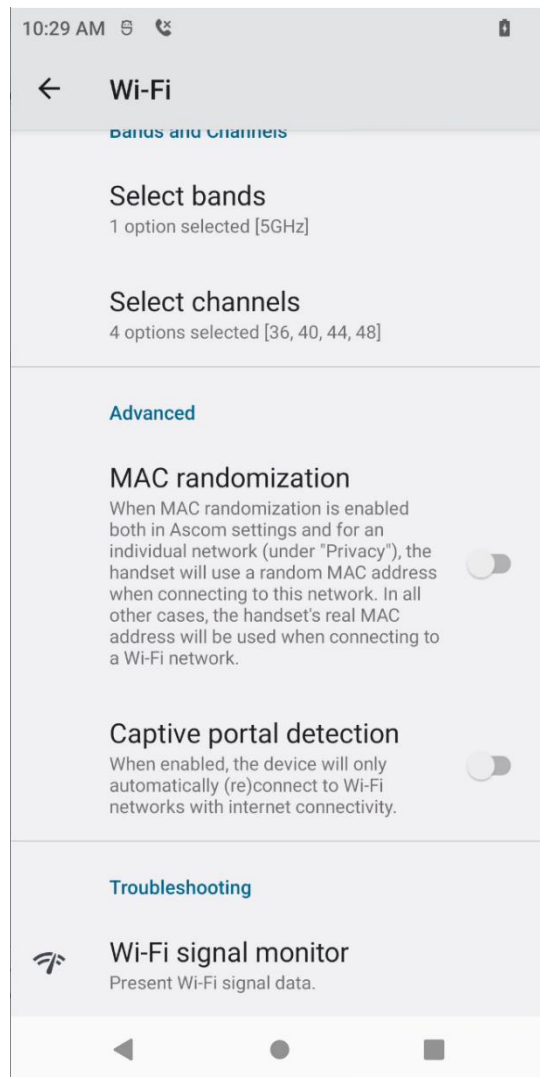
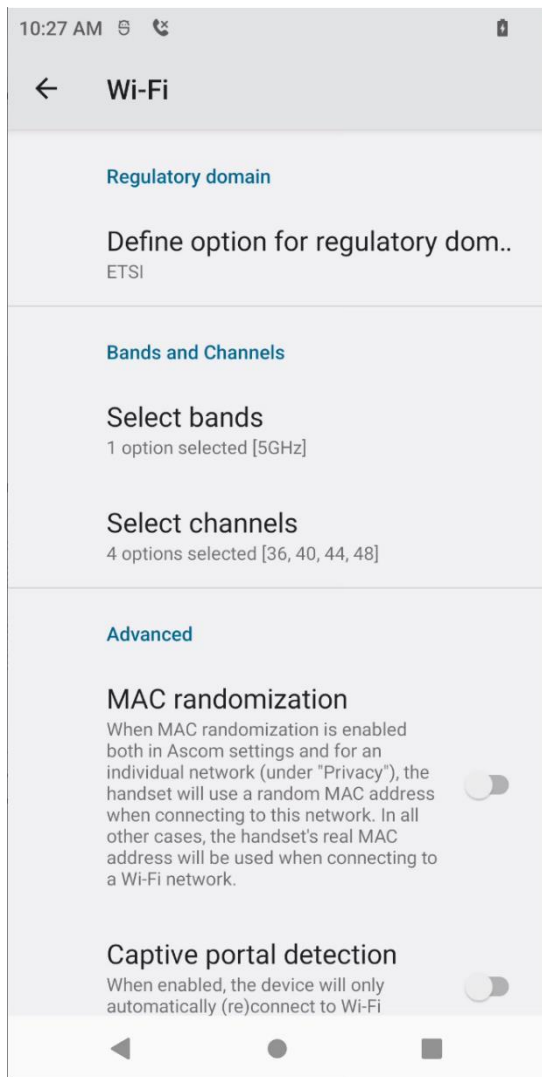
Ascom recommends only use channel 1, 6 and 11 for 802.11b/g/n. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines below.

General guidelines when deploying Ascom Myco 4 handsets in 802.11a/n/ac/ax 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 40MHz, 80MHz or 160MHz channel bonding environments. The recommendation is, however, to avoid 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.**

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.

Ascom Myco 4 Wi-Fi settings

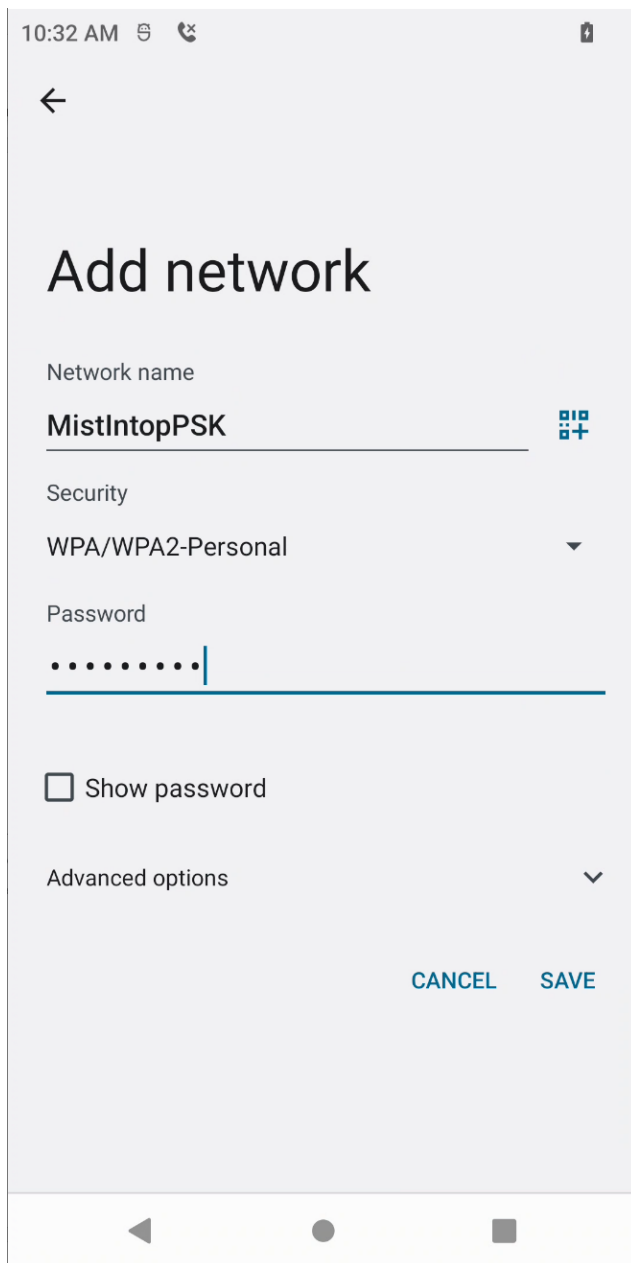


Settings -> Ascom settings -> Wi-Fi

- Select Regulatory domain according to your region.
- Make sure that the enabled channels in the Myco 4 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”.

WPA2 PSK

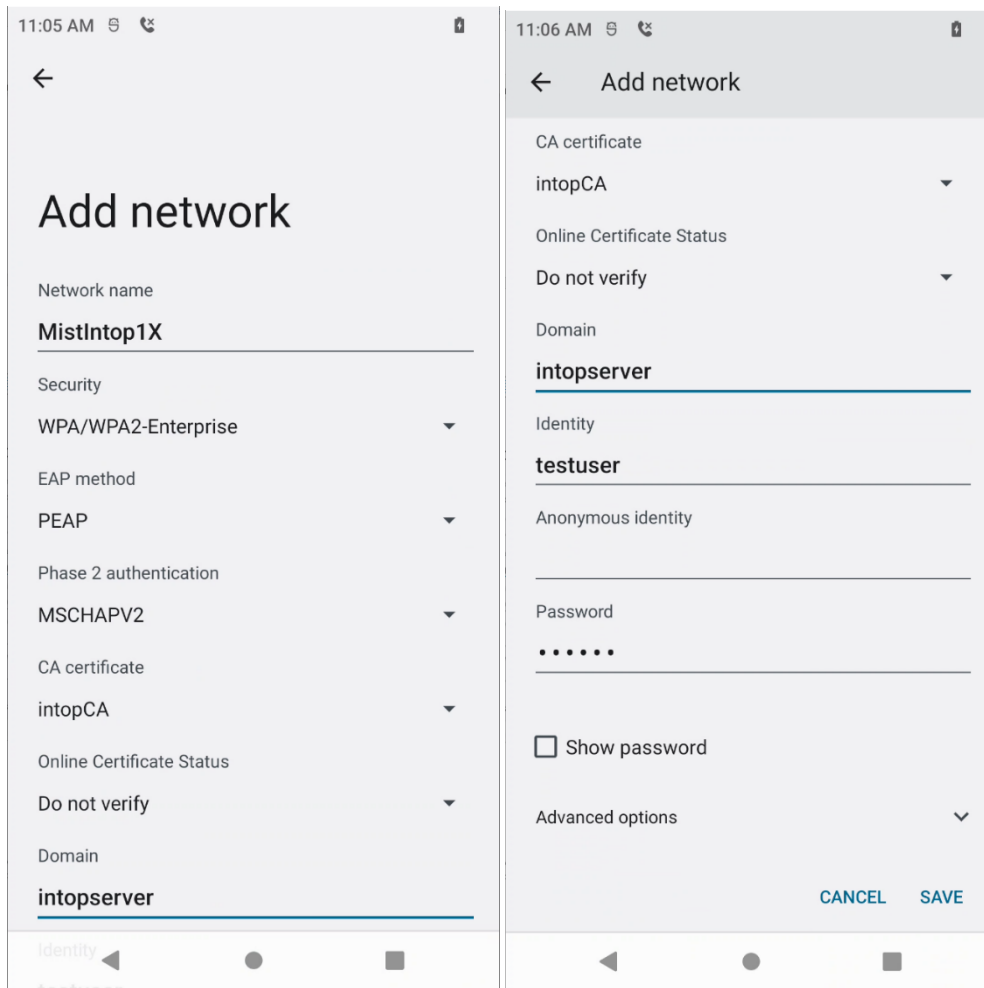


The screenshot shows an Android mobile interface for adding a network. At the top, the status bar displays '10:32 AM' and various icons. Below the status bar is a back arrow. The main title is 'Add network'. The 'Network name' field contains 'MistIntopPSK' and has a QR code icon to its right. The 'Security' dropdown menu is set to 'WPA/WPA2-Personal'. The 'Password' field is filled with ten dots and has a cursor at the end. Below the password field is a checkbox labeled 'Show password' which is currently unchecked. At the bottom of the form area are two buttons: 'CANCEL' and 'SAVE'. The bottom of the screen shows the standard Android navigation bar with back, home, and recent apps icons.

Pre-shared key authentication configuration example

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

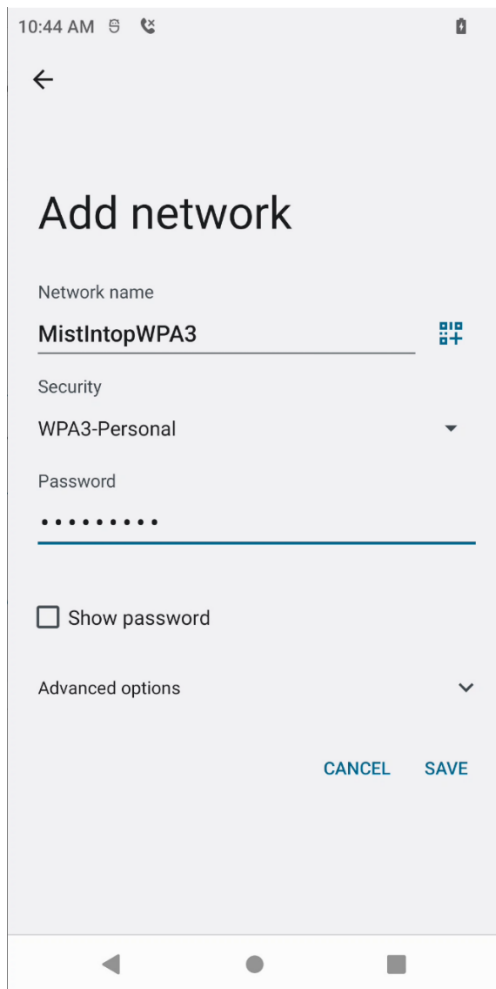
WPA2-Enterprise (802.1X)



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 Domain, Identity and Password.

WPA3-Personal (SAE)



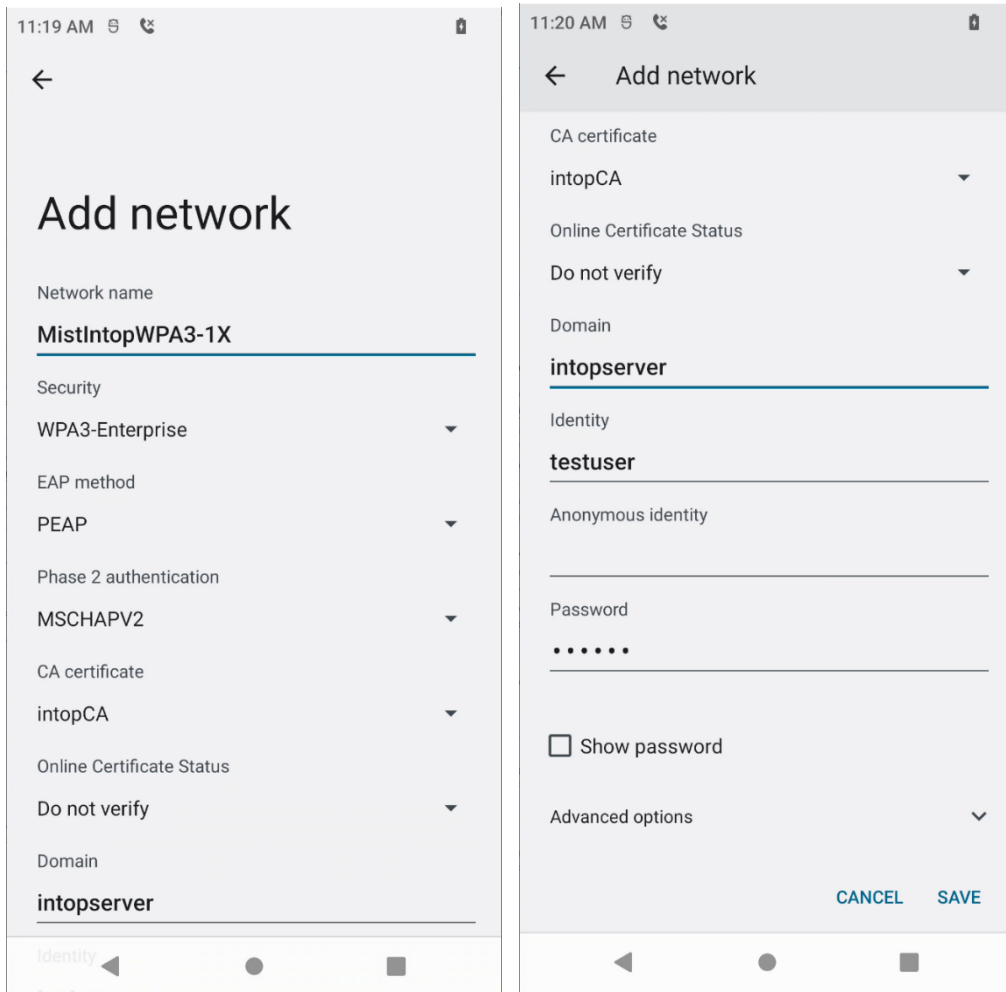
The screenshot shows an Android mobile interface for adding a new network. At the top, the status bar displays '10:44 AM' and signal strength. Below the status bar is a back arrow icon. The main heading is 'Add network'. Underneath, there are three input fields: 'Network name' with the text 'MistIntopWPA3' and a QR code icon; 'Security' with a dropdown menu set to 'WPA3-Personal'; and 'Password' with a series of dots. Below the password field is a checkbox labeled 'Show password' which is currently unchecked. At the bottom of the form area, there is a dropdown menu for 'Advanced options'. At the very bottom of the screen, there are two buttons: 'CANCEL' and 'SAVE'. The bottom navigation bar of the phone is visible at the very bottom of the screenshot.

WPA3-Personal (SAE) authentication configuration example

- Configure Network Name
- Select Security: WPA3-Personal
- Enter Password

Note: When backwards compatibility is required on the SSID for non-WPA3-capable Ascom handsets, use “WPA3 Transition Mode”. Transition mode is a mixed mode that enables the use of WPA2 to connect clients that do not fully support WPA3.

WPA3-Enterprise (802.1X authentication)



WPA3-Enterprise (802.1X authentication) configuration example

- Configure Network Name
- Select Security: WPA3-Enterprise
- Select EAP method: PEAP and Phase 2 authentication: MSCHAPv2.
- Select CA Certificate
Certificates can be installed either via an MDM tool or manually.
Manual installation: Setting – Security – Encryption and credentials – Install a certificate – Wi-Fi certificate.
- Configure Domain, Identity and Password.

Note: When backwards compatibility is required on the SSID for non-WPA3-capable Ascom handsets, use “WPA3 Transition Mode”. Transition mode is a mixed mode that enables the use of WPA2 to connect clients that do not fully support WPA3.

Appendix B: Interoperability Validation Records

| | |
|--------------|----|
| Pass | 22 |
| Fail | 0 |
| Comments | 4 |
| Not verified | 3 |
| Total | 29 |

Refer to the attached file for detailed verification results.

Document History

| Rev | Date | Author | Description |
|-----|------------------|--------|---|
| D1 | 30-January-2024 | NLRPa | Initial draft |
| D2 | 06-February-2024 | NLRPa | Added screenshot |
| P1 | 16-February-2024 | NLRPa | Minor Adjustment after internal peer review |
| P2 | 20-February-2024 | NLRPa | Added WPA3 test results in Verification overview table. |