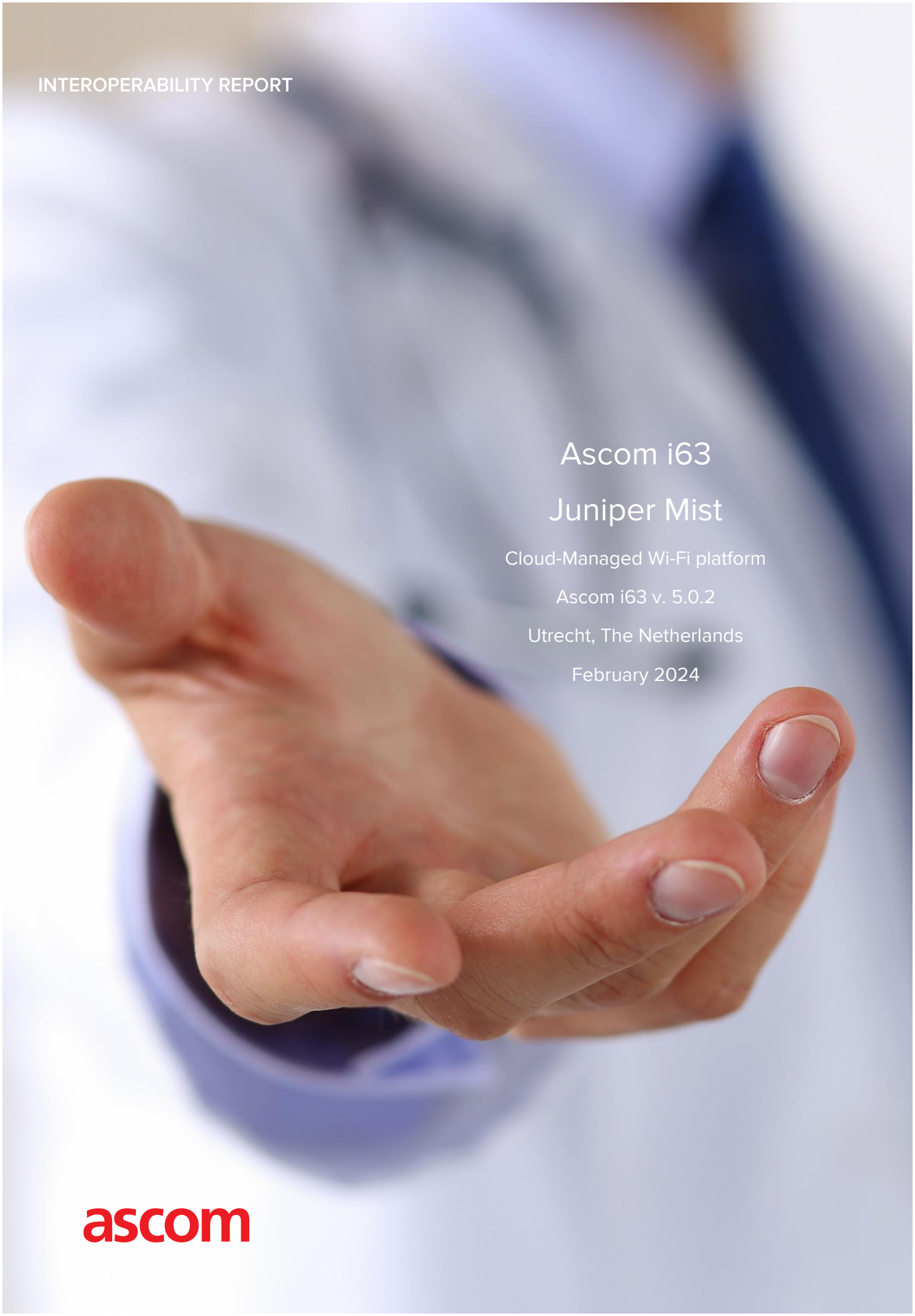
INTEROPERABILITY REPORT



Ascom i63

Juniper Mist

Cloud-Managed Wi-Fi platform

Ascom i63 v. 5.0.2

Utrecht, The Netherlands

February 2024

ascom

Contents

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

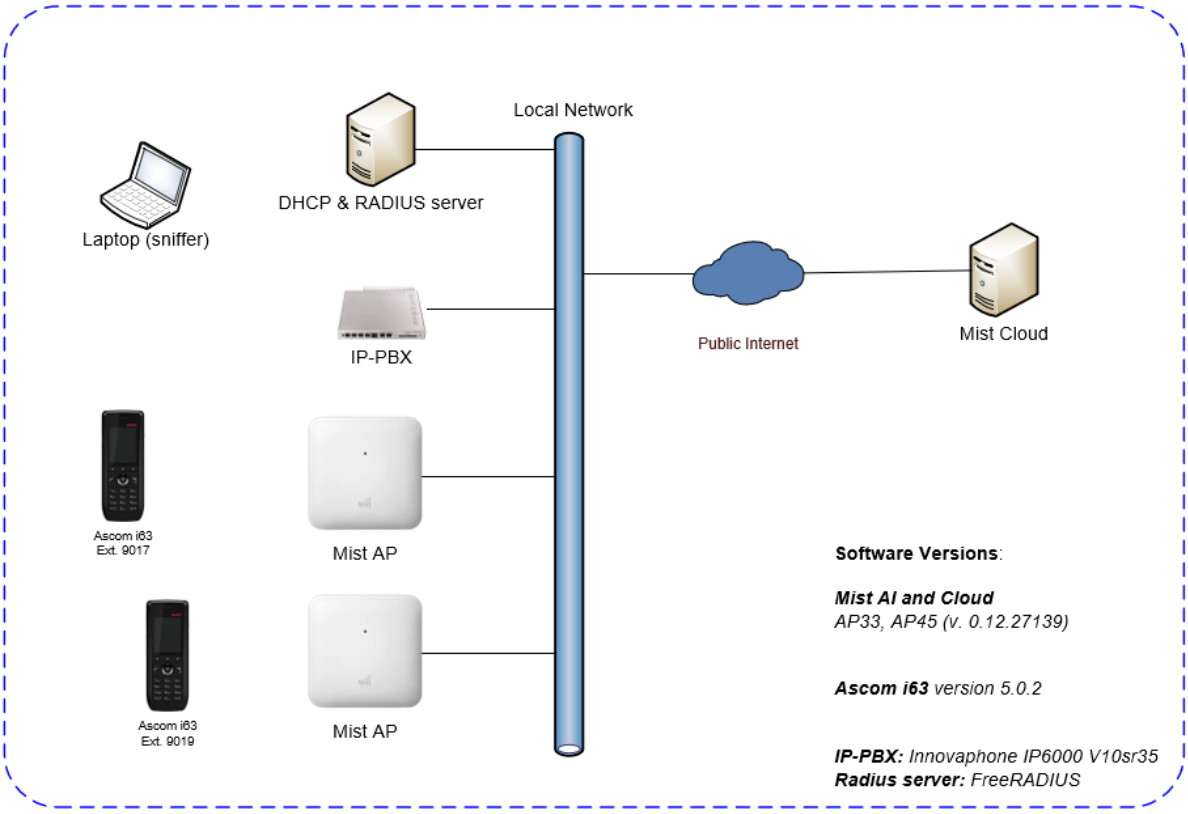
Test site

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, 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

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, *Option to change this value in the GUI can be activated by Juniper Mist Support if required/requested*
PMKSA Caching	OK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	OK	
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 46ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 39ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 50ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 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.

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**.

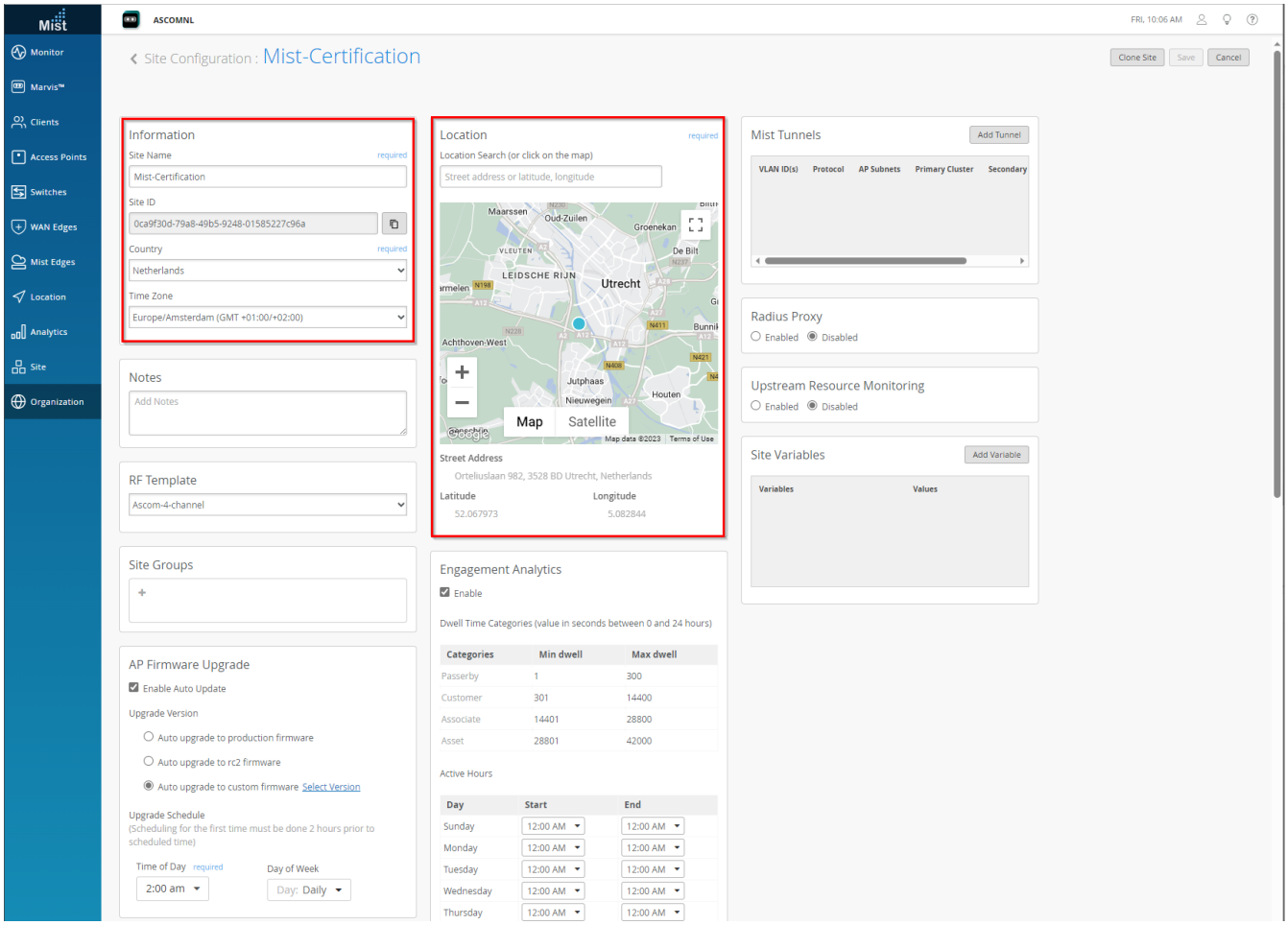
For detailed verification results, refer to Appendix B: Interoperability Validation Records.

Appendix A: Validation Configurations

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.

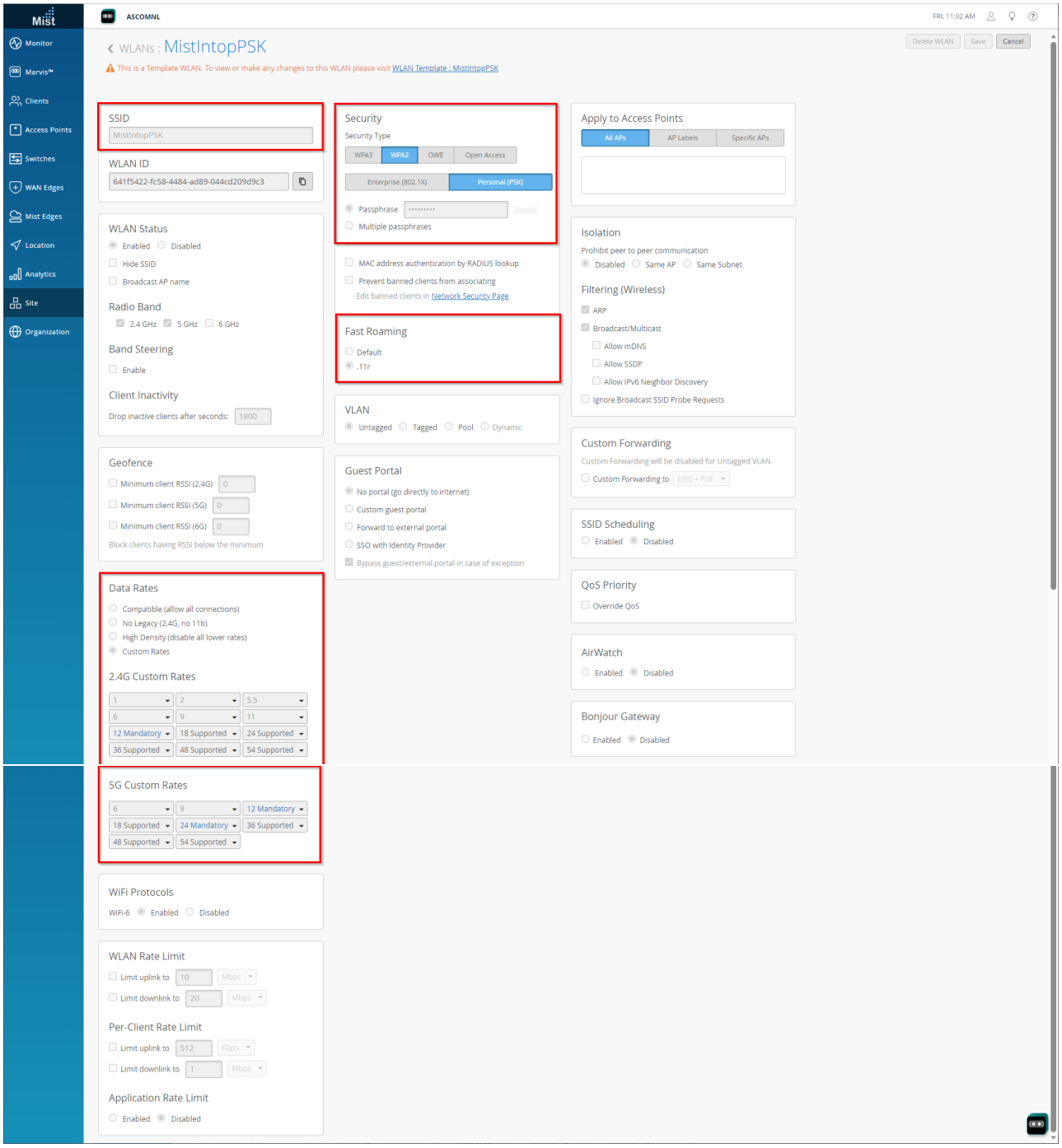
General settings (SSID, Authentication, Radio and QoS)



Organization > Admin > Site Configuration

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

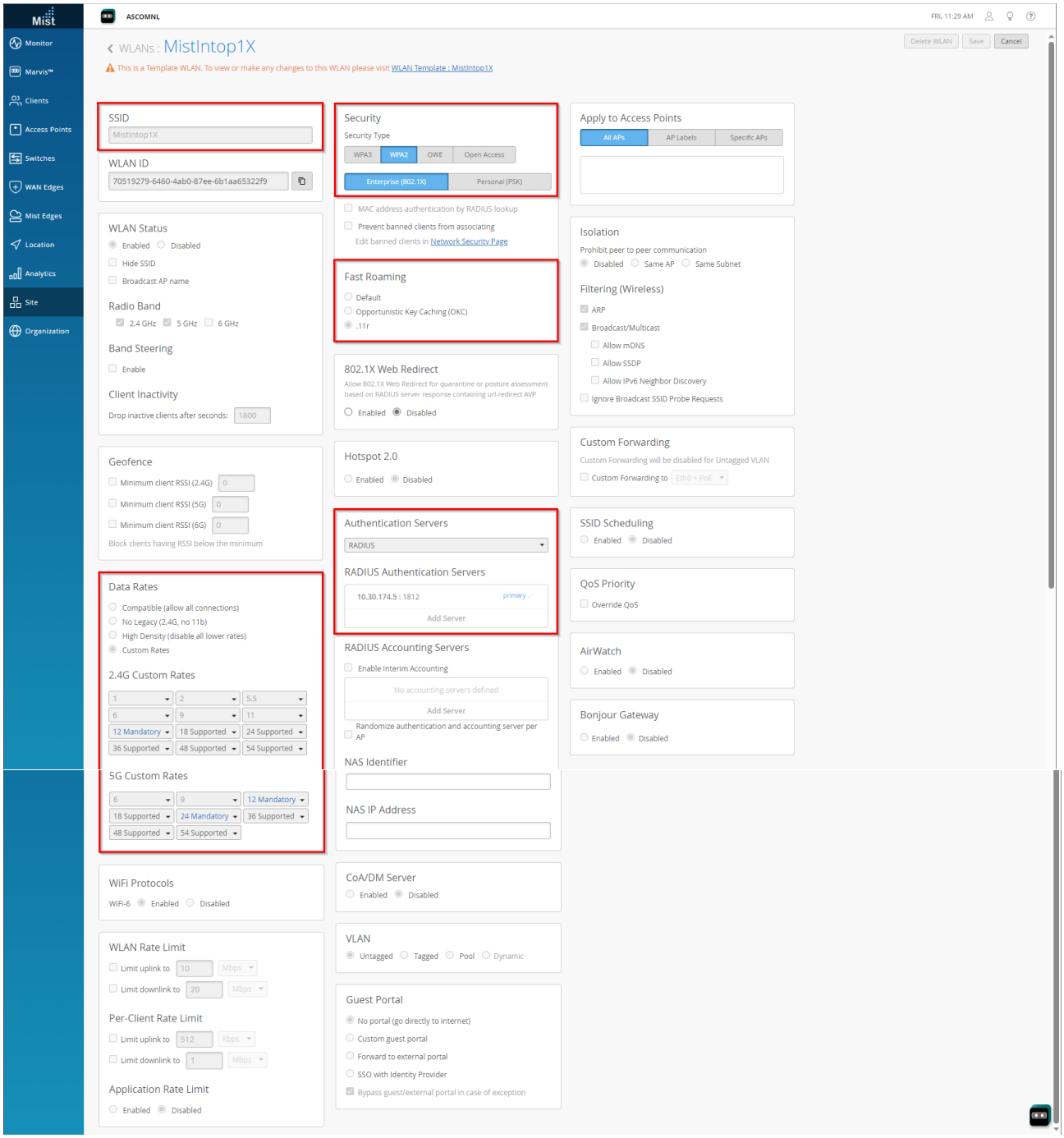
Please refer to Mist's documentation on how to create a Mist account, organization, sites, templates, networks and the claiming of access points to an organization. Only after the latter can devices be assigned to a site.



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)



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.

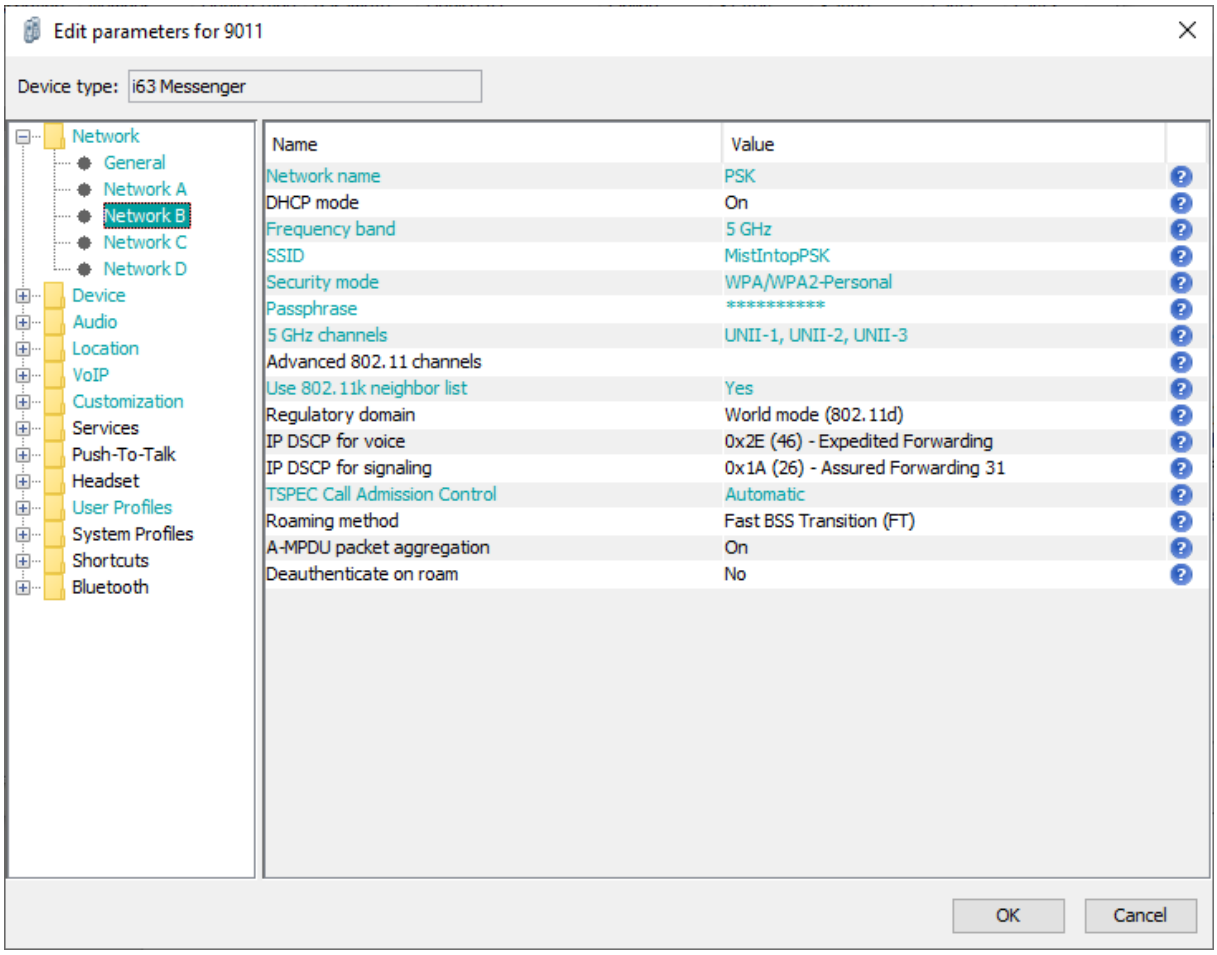
Ascom recommends only using channels 1, 6 and 11 for 802.11b/g/n. For 802.11a/n/ac use channels according to the infrastructure manufacturer, country regulations and per guidelines below.

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:

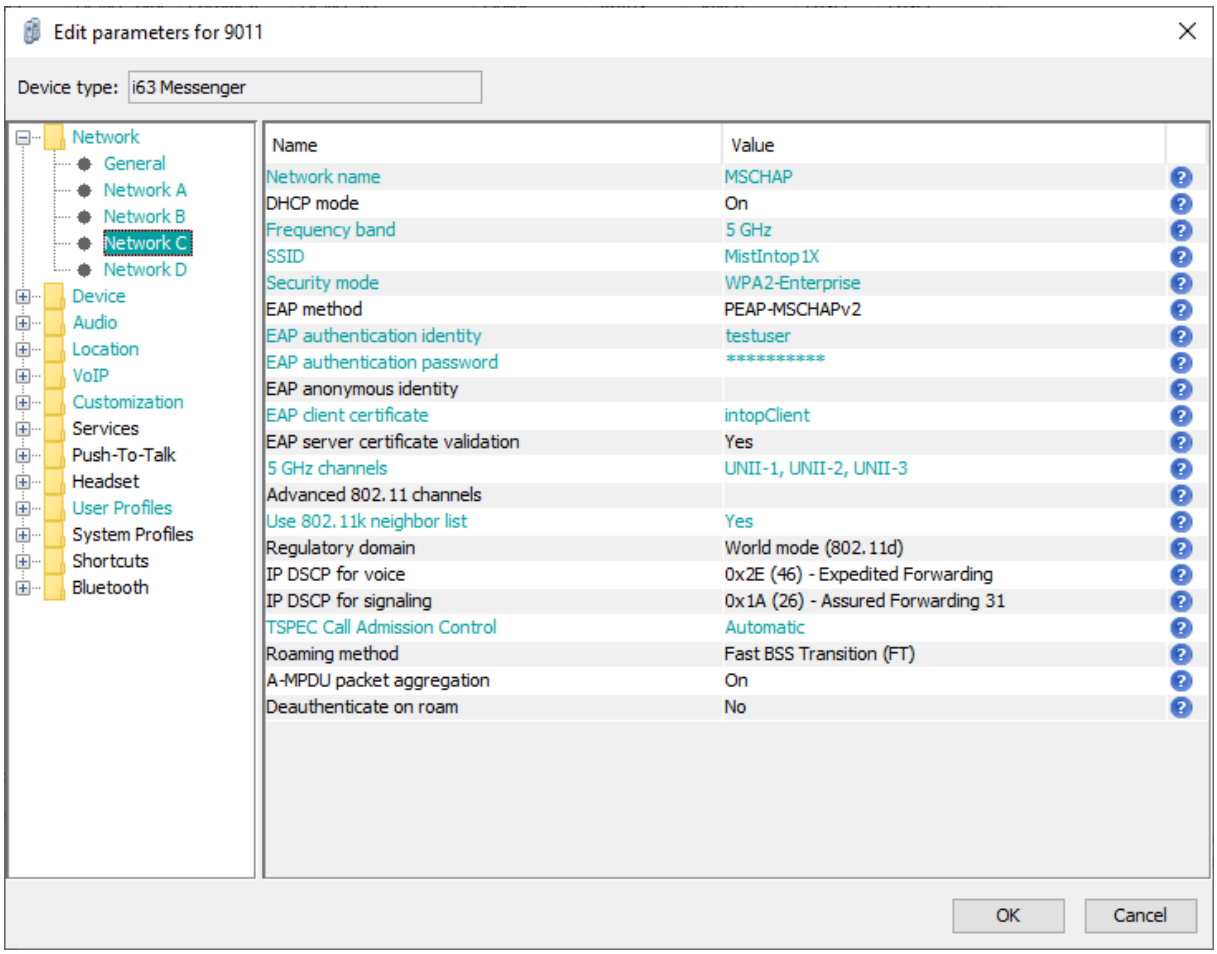
1. **For environments not utilizing 802.11k Neighbor Report - Enabling more than 8 channels in the system will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels in the system can be allowed. Ascom does not recommend exceeding these limits unless 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 i63 v.5.0.2



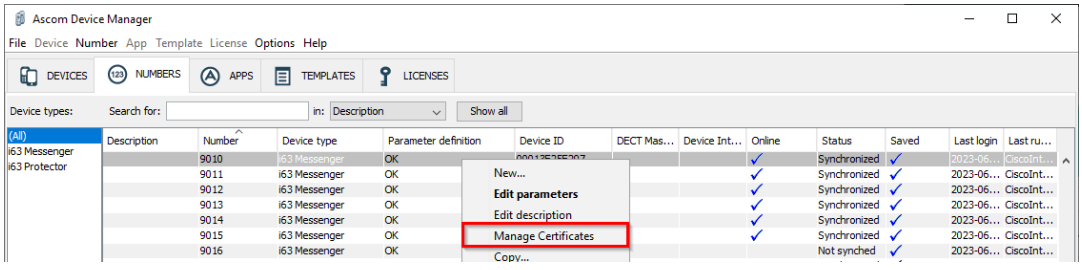
Network settings for WPA2-PSK

- 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”.



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”.



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