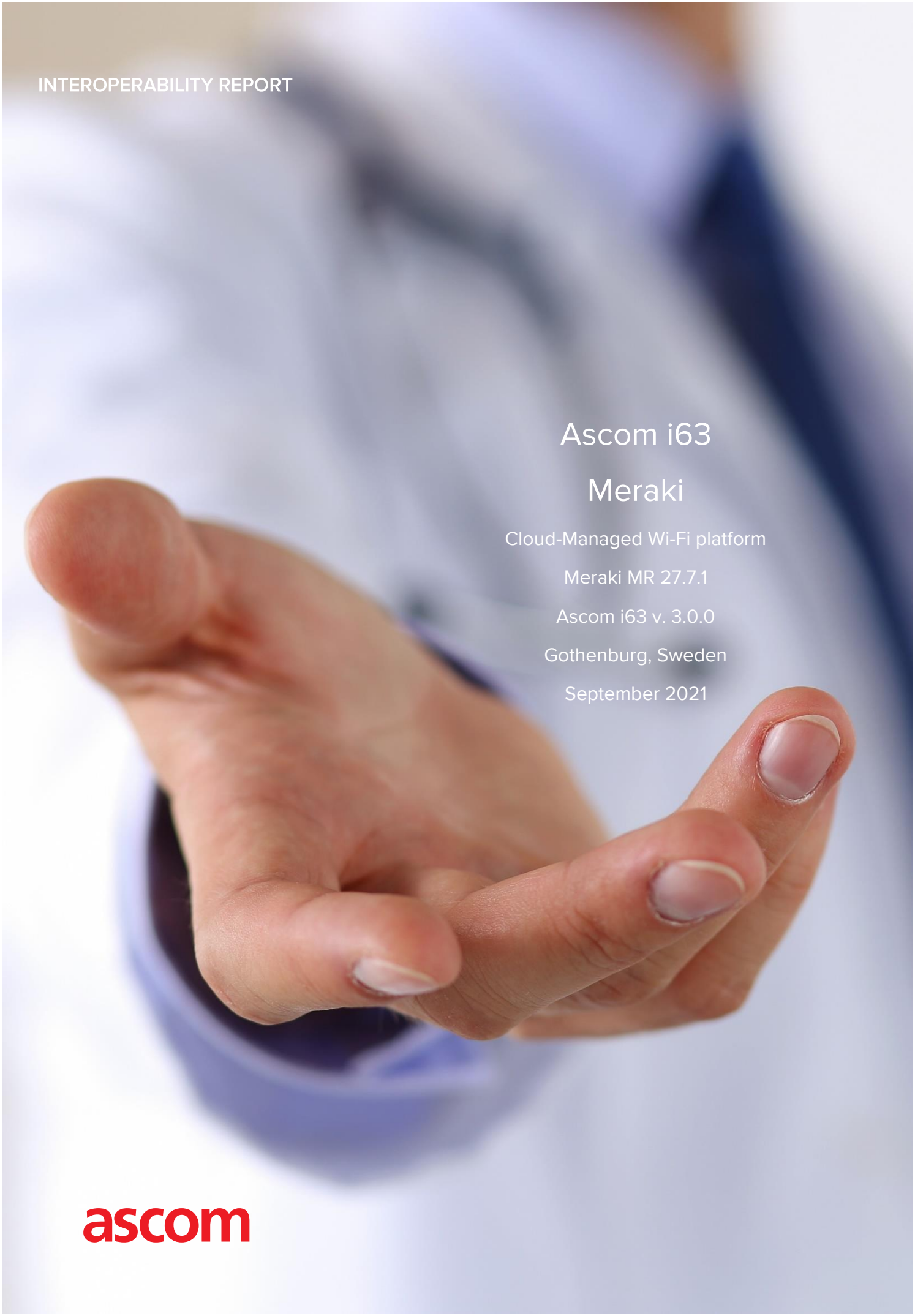
INTEROPERABILITY REPORT



Ascom i63

Meraki

Cloud-Managed Wi-Fi platform

Meraki MR 27.7.1

Ascom i63 v. 3.0.0

Gothenburg, Sweden

September 2021

ascom

Contents

Introduction

This document provides a summary of the interoperability verification results relating to Ascom's and Meraki's platforms. Moreover, it describes guidelines and the necessary steps to optimally configure each respective platform. The report should be used in conjunction with Meraki's and Ascom's user manuals and 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.

URL: http://www.ascom.com

About Meraki

We create 100% cloud managed IT that simply works

Technology can connect us, empower us, and drive us. At Cisco Meraki, we believe that by simplifying powerful technology, we can free passionate people to focus on their mission and reach groups previously left in the darkness.

Founded in 2006, Meraki has grown to become an industry leader in the IT space, with over 500,000 customers and several million network devices and counting online around the world. Our comprehensive set of solutions includes wireless, switching, security, communications, EMM, and security cameras, all managed through Meraki's web-based dashboard interface. This allows customers to seize new business opportunities and reduce operational costs.

URL: http://meraki.cisco.com

Site Information

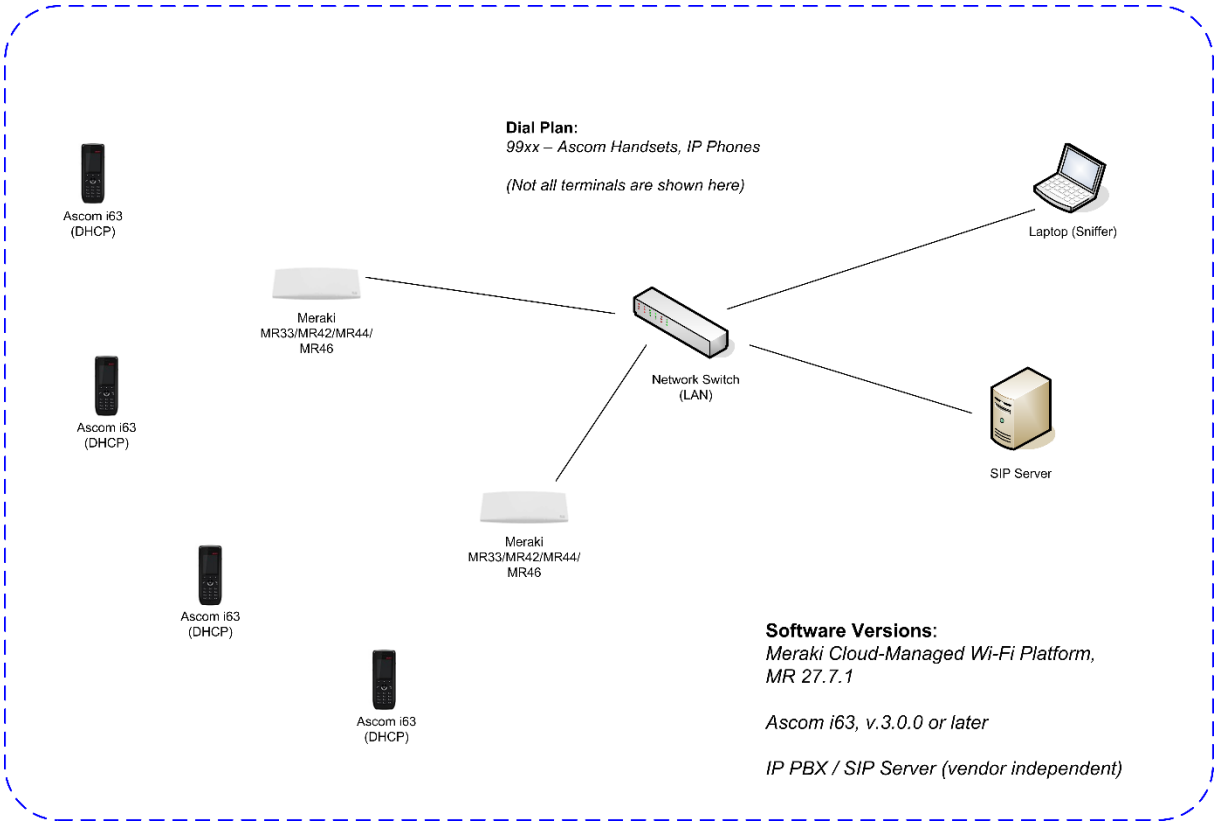
Test site

Ascom
Grimbodalen 2
Gothenburg
Sweden

Participants

Matthew Williams-Morley, Ascom SE

Test topology



Summary

General conclusions

The steps of Ascom interoperability verification produced satisfactory results regarding most test areas, including authentication, stability, roaming, QoS, and power-save related areas. However, it was noted that roaming with WPA3 (SAE/PSK, Enterprise not tested) did not perform to our satisfaction. Until further notice, WPA3 is not supported. Please refer to the “Known limitations” section for details.

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

Compatibility information

Access point models have been selected in dialogue with Meraki (MR33, MR42, MR44, and MR46). By testing these models as our baseline, we are considered to cover listed Meraki access points based on chipset compatibility.

Supported Partner Access Points with SW version MR27.7.1:

Wi-Fi 5 (802.11ac wave 2):

MR20
MR30H/MR33
MR42/MR42E
MR52/MR53/MR53E
MR70/MR74
MR84

Wi-Fi 6 (802.11ax):

MR36
MR44/MR46/MR46E
MR76
MR86

Feature overview

WLAN Compatibility and Performance

High Level Functionality	Result	Comments
Association, Open with No Encryption	N/T	
Association, WPA2-PSK / AES Encryption	OK	
Association, PEAP-MSCHAPv2 Auth, AES Encryption	OK	
Association with EAP-TLS authentication	OK	
Association with WPA3 SAE (PSK) authentication	OK *	Problem with roaming
Association with WPA3 Enterprise authentication	NOK *	192-bit data encryption and/or GCMP is not supported by handset
Association, Multiple ESSIDs	OK	
Beacon Interval and DTIM Period	N/A *	DTIM Period = 1, cannot be changed in Web GUI
PMKSA Caching	OK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
Traffic Specification (TSPEC)	N/A	Not supported by WLAN
802.11 Power-save mode	N/A **	
802.11e U-APSD	OK	
802.11e U-APSD (load test)	OK	
Roaming, WPA2-PSK, AES Encryption	OK	802.11r/FT recommended
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 25-30ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK ***	802.11r/FT recommended, typical roaming time 40-45ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 30-35ms
Roaming, WPA3-PSK Authentication	NOK *	Problem with roaming
Roaming, WPA3-Enterprise Authentication	N/T *	
Channel usage controlled by 802.11k	OK	
Protected Management Frames (802.11w)	NOK *	Problem with roaming

*) Refer to the section “Known Limitations” in this report.

**) Ascom requires that U-APSD is enabled in the WLAN.

***) Observed times are with Opportunistic/Proactive Key Caching enabled (default).

Average roaming times are measured using 802.11a/n/ac. Please refer to Appendix B for detailed test results.

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
Meraki advertises a DTIM Period of 1, which may increase the battery consumption of the Ascom i63 in idle mode.	No workaround available. DTIM Period = 1 cannot be changed in GUI.	
WPA3-PSK and WPA3-Enterprise. Problem related to the Ascom i63 with roaming resulting on poor connectivity and audio gaps.	WPA3 is not supported. Use another authentication method such as WPA2 (without 802.11w/PMF enabled).	WH2-3388 See also Ascom i63 Release Notes for v.3.0.0.
WPA3-Enterprise. 192-bit data encryption and/or GCMP is not supported by handset. Problem associating when required by WLAN.	WPA3 is not supported. No workaround.	MRS-697 (for analysis)

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

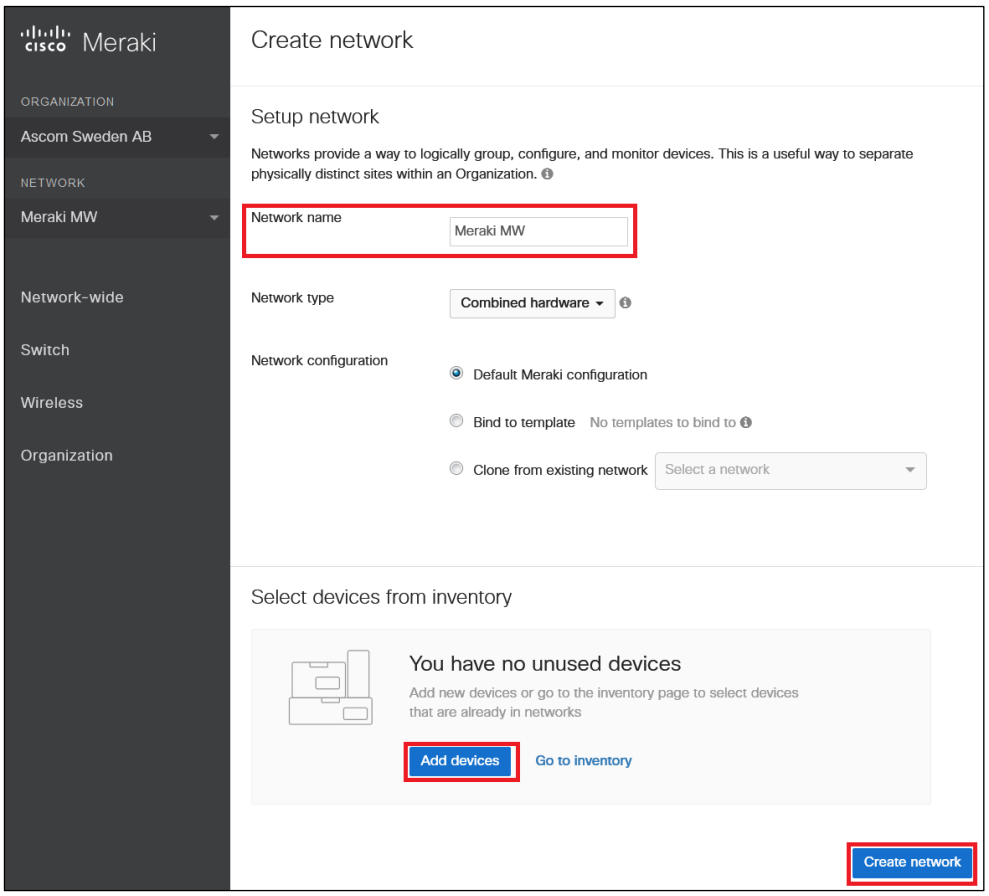
For detailed test results, refer to Appendix B: Interoperability Verification Records.

Appendix A: Test Configurations

Meraki Cloud-Managed Wi-Fi platform MR 27.7.1

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

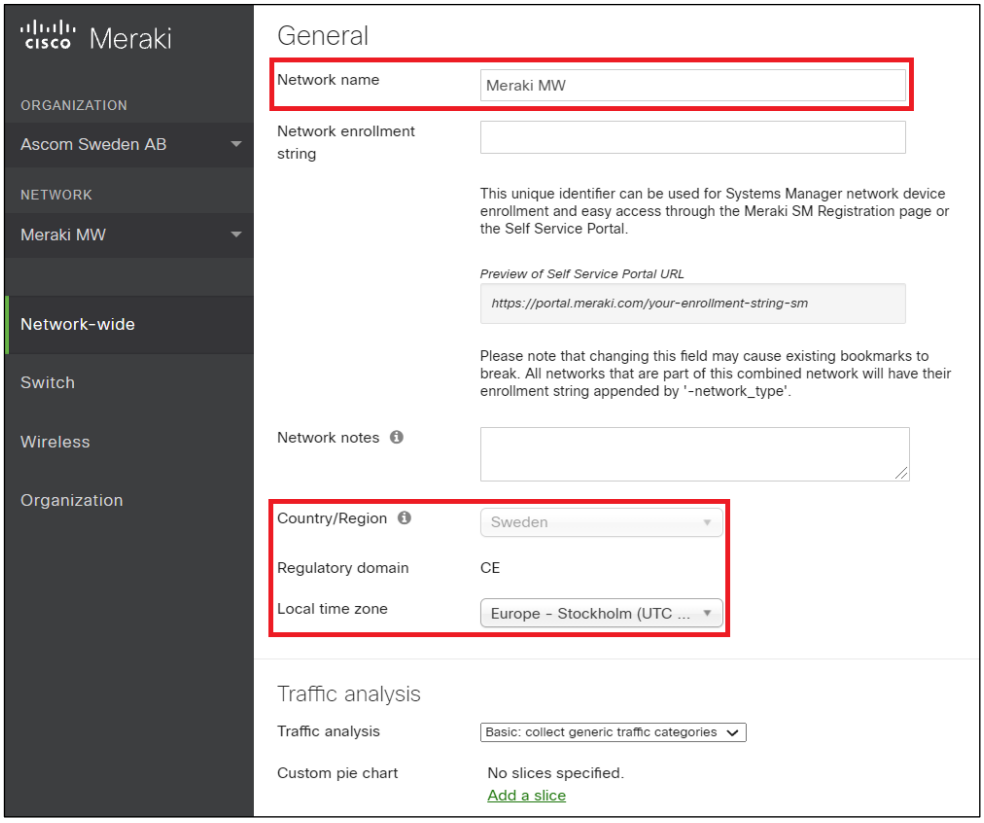
General settings (SSID, Authentication, Radio and QoS)



Network > Create a new network

- Define Network Name
- Optional: Define Network Type
- Add devices
- Create network

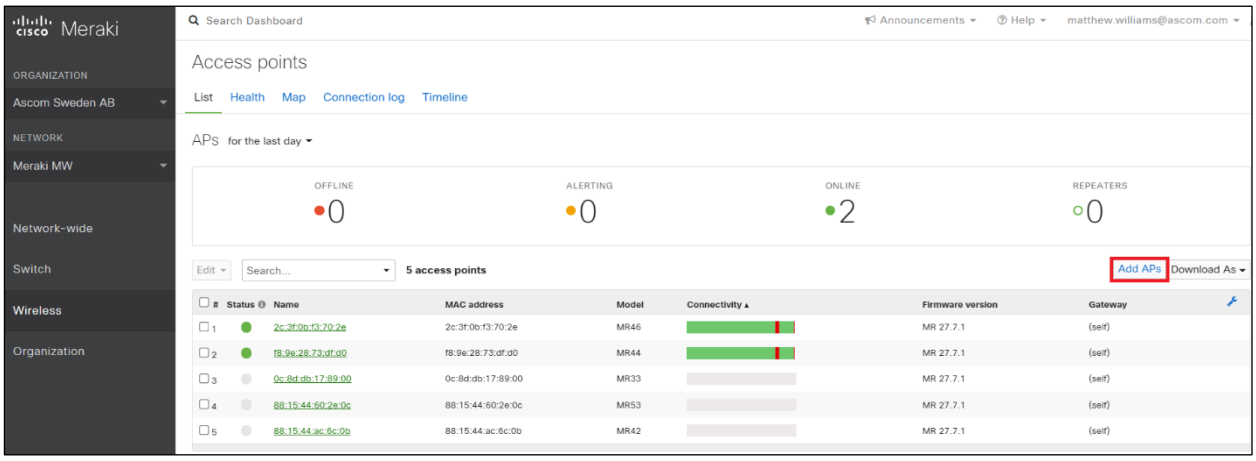
Please refer to Meraki's documentation on how to create a hierarchy of organizations, networks, and the concept of claiming to an inventory. Only after the latter can devices be added to networks.



Network-Wide > Configure > General

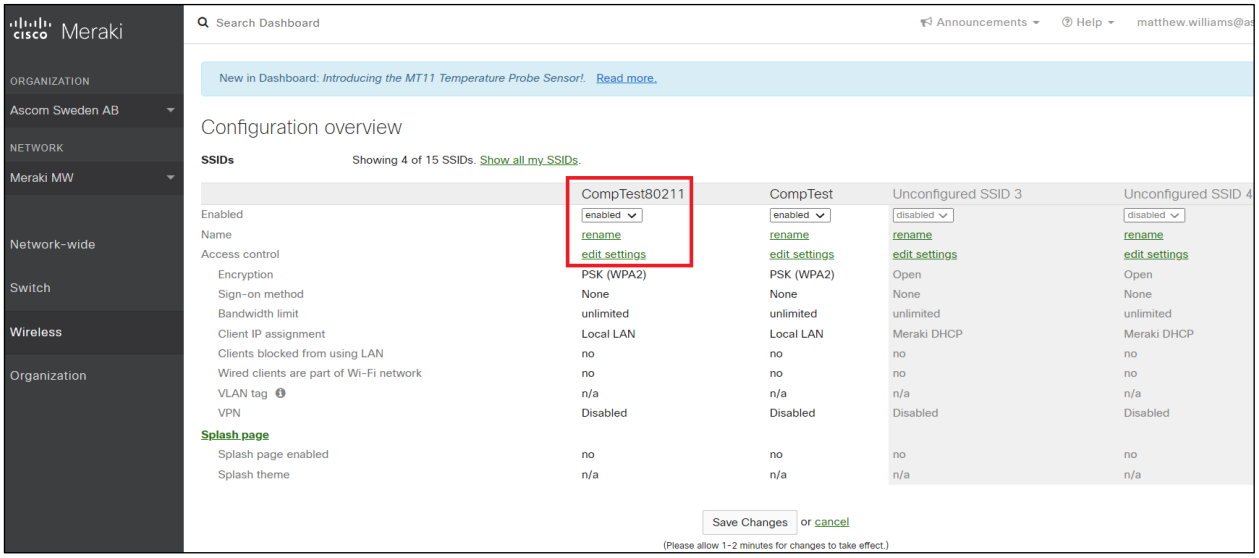
- Network Name defined in previous step
- Set Country/Region (Regulatory Domain inferred from this setting)
- Set the Local Time Zone
- Remember to save settings

NOTE: All other parameters were left at their defaults throughout testing.



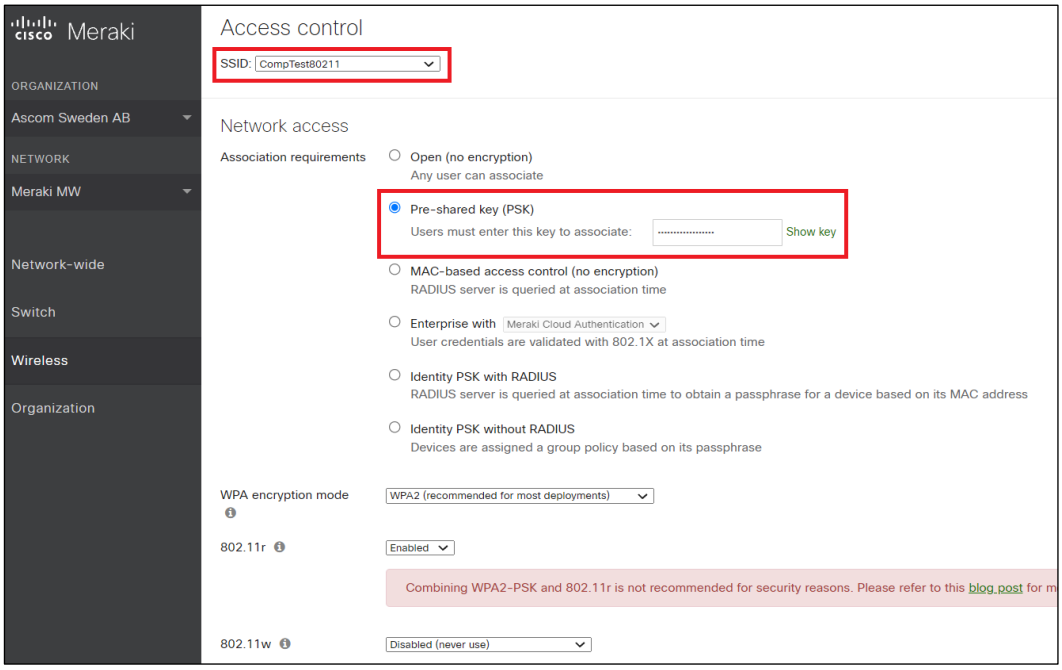
Wireless > Monitor > Access Points

- Add AP's to the network (if not already done when creating network)



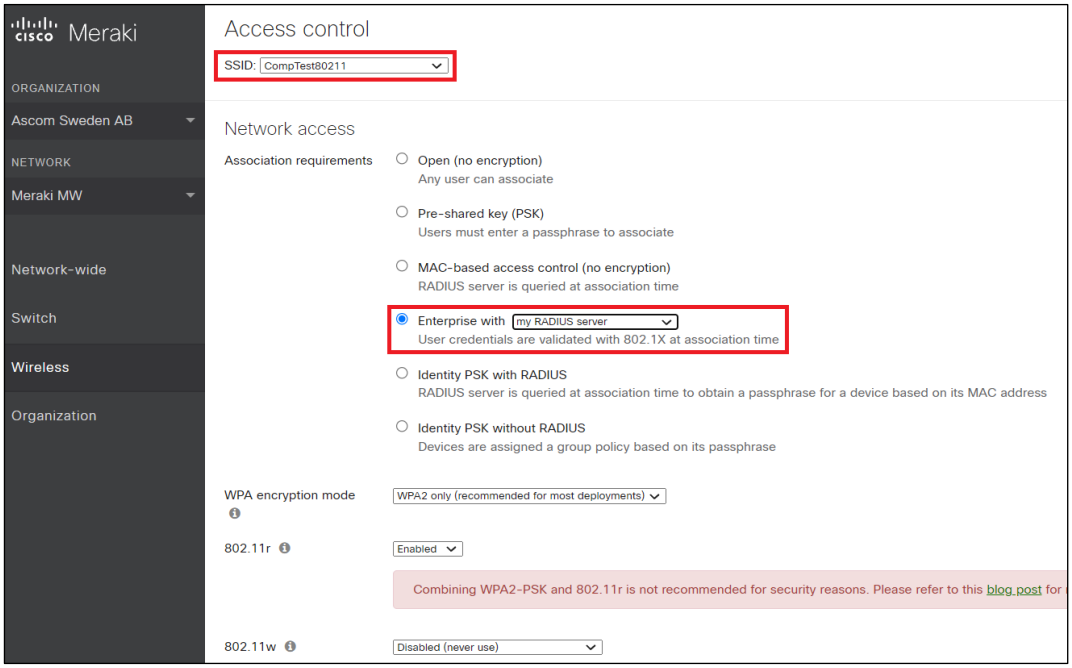
Wireless > Configure > SSID

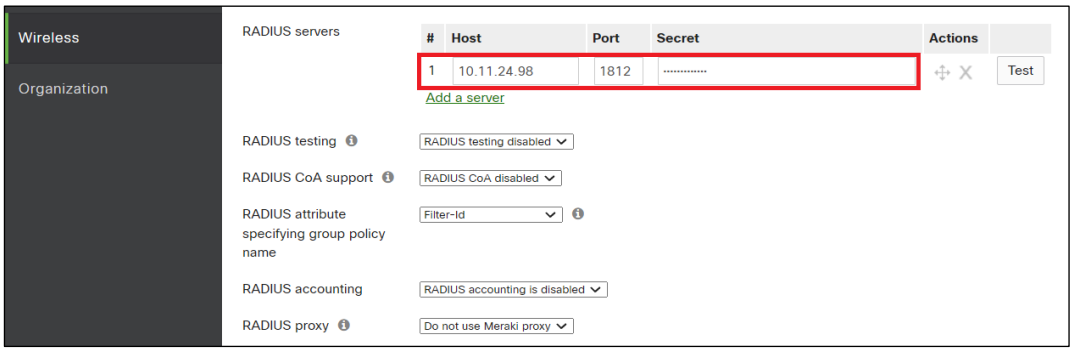
- Define Name (SSID)
- Edit Access Control (Security Settings, see next page)
- Remember to enable SSID



Wireless > Configure > Access Control (WPA2-PSK)

- Select SSID
- Enter WPA2 Pre-shared Key (PSK)





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

Configuration of authentication using external Radius server, 802.1X. In this example, WPA2-AES is used.

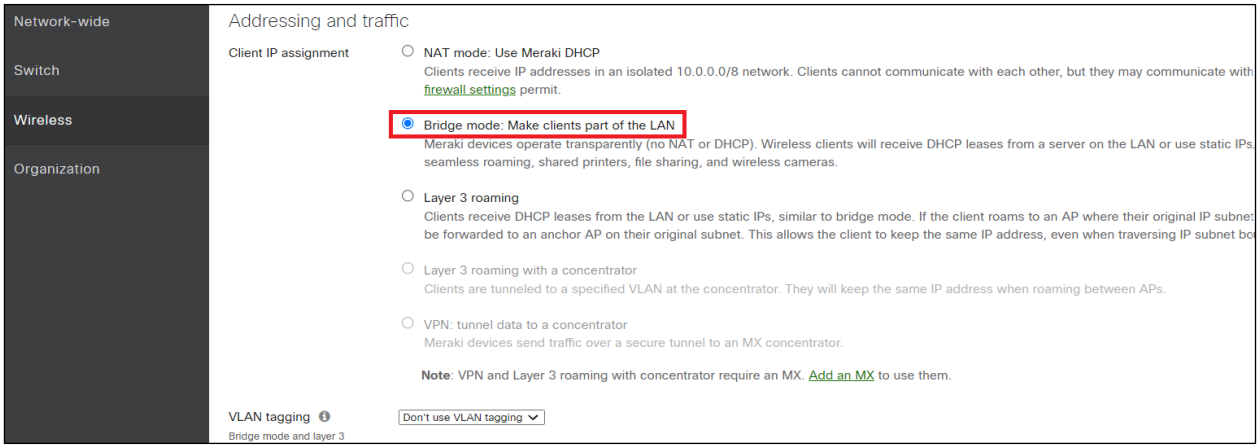
Wireless > Configure > Access Control (802.1X)

- Select SSID
- Select WPA2-Enterprise with “my RADIUS server” (unless the internal server is used)
- Define a RADIUS server
- Opportunistic Key Caching is enabled by default (applicable when Fast Roaming (802.11r/FT) is not negotiated by clients)

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

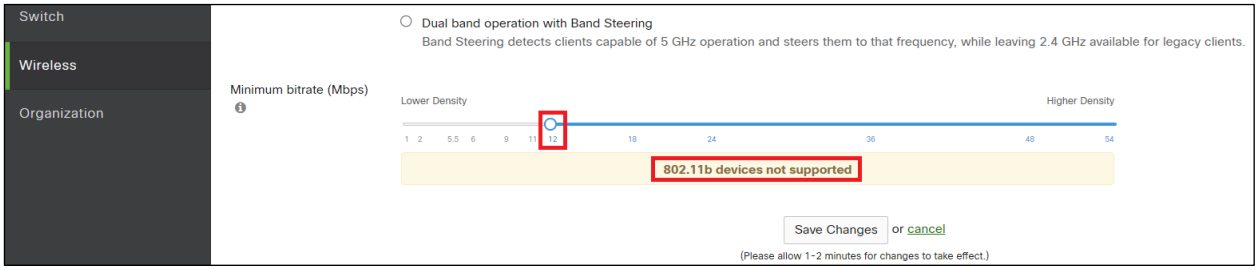
802.11r/FT is not supported by Ascom i62 and Myco 1 & 2. Nevertheless, these devices can operate on SSIDs where 802.11r (FT) is advertised in conjunction with a legacy method.

Ensure that 802.11w (Protected Management Frames) is disabled (default).



Wireless > Configure > Access Control (step 2)

- Select Bridge Mode should clients need to receive leases from a DHCP server on the LAN

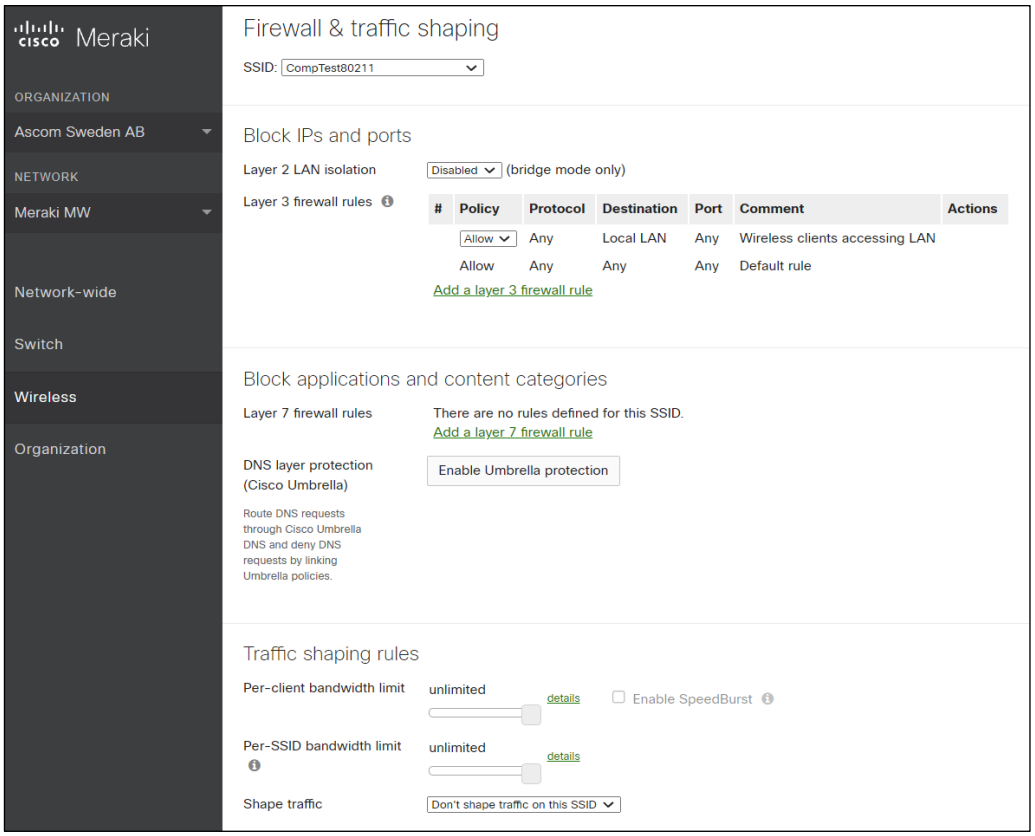


Wireless > Configure > Access Control (step 3)

- Select Minimum Bitrate: 12 Mbps
- Remember to Save Changes

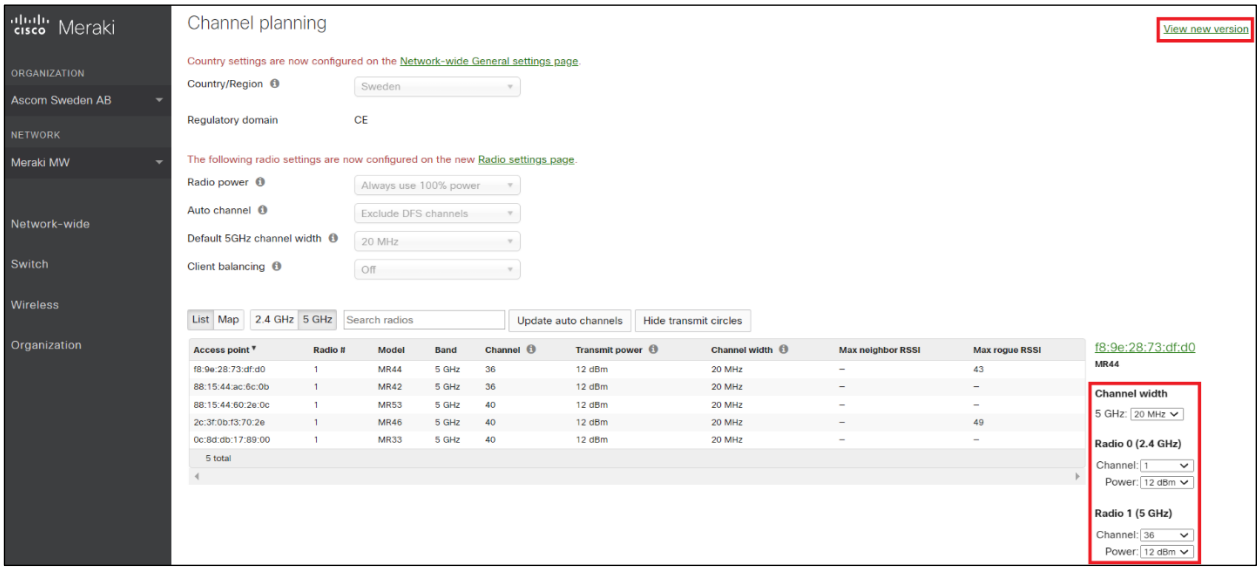
NOTE: Ascom recommends disabling the lowest transmit rates and recommends that 12 Mbps is the lowest basic rate.

SSID Overview (Network-Wide > Monitor > Clients)



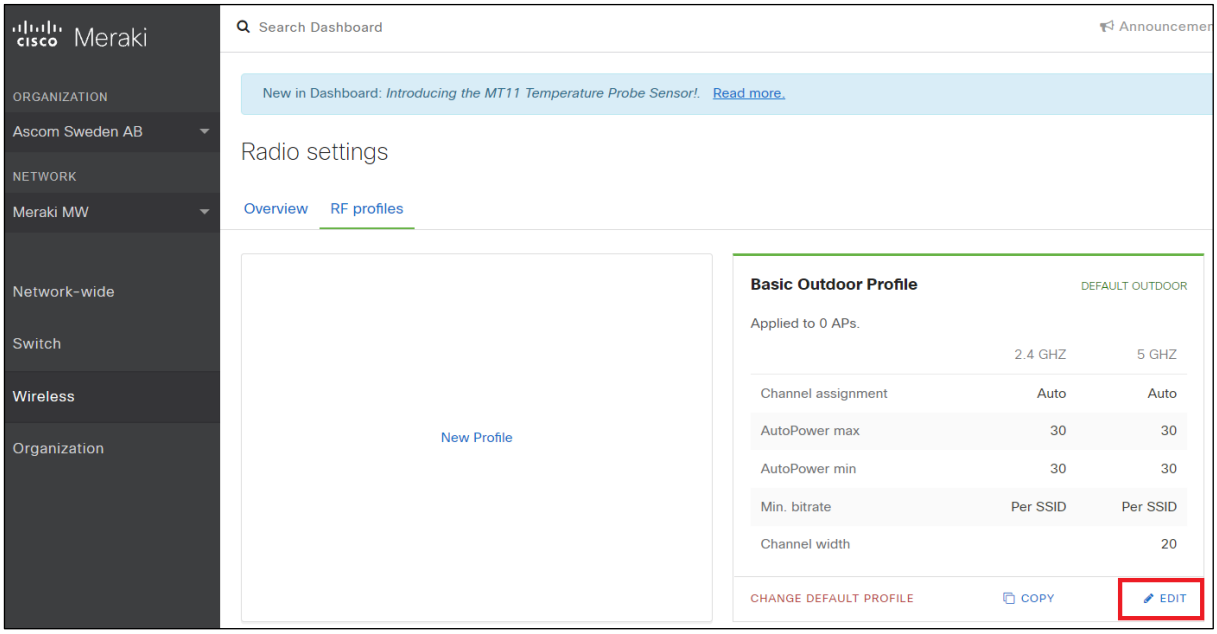
QoS Settings (Wireless > Configure > Firewall & traffic shaping)

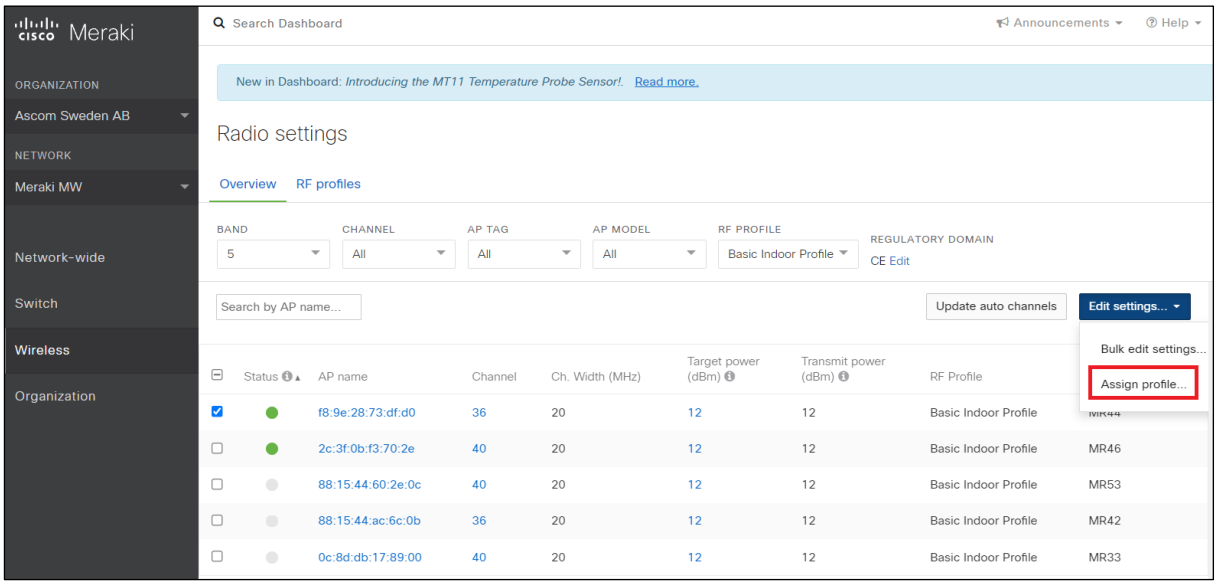
- No need to modify (included as reference)
- To match default mappings, ensure the i63 uses DSCP AF 31 (or best effort) for signaling and DSCP EF 46 for Voice.



Wireless > Configure > Radio Settings (old version/method)

- Regulatory Domain inferred from Country/Region of network
- Select MAC of an AP
- Adjust Radio0 and Radio1 to the appropriate settings
- Remember to Save Changes

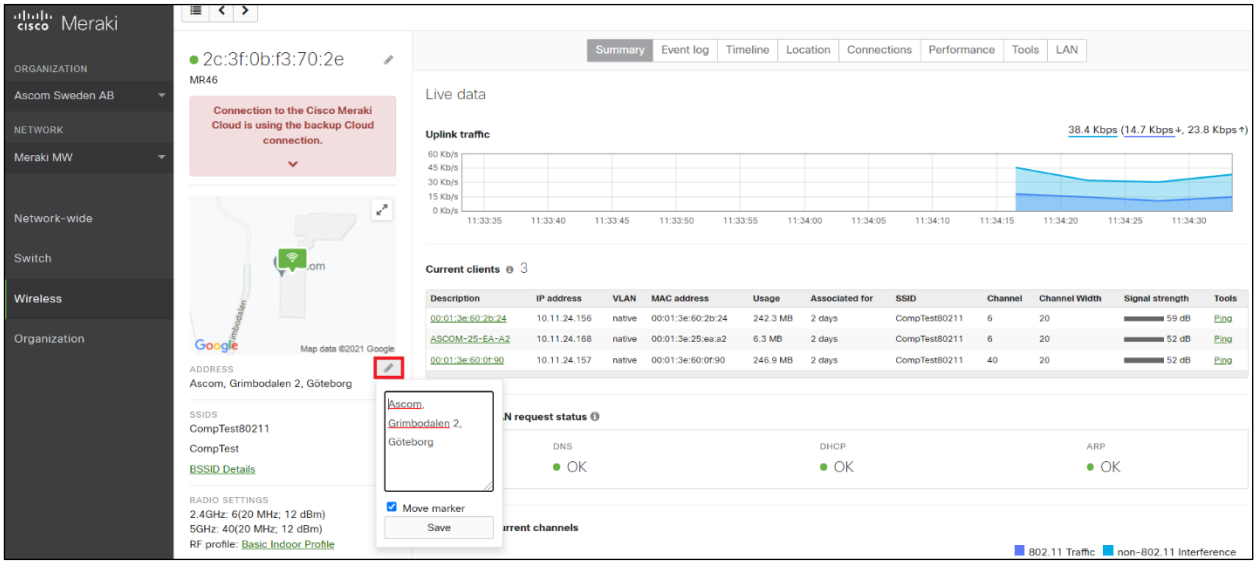




Wireless > Configure > Radio Settings (new version/method)

- Regulatory Domain inferred from Country/Region of network
- Edit the appropriate RF profile
- Select one or several APs
- Assign RF profile to APs
- Optional: Manual adjustments to Channel and Target power (dBm)
- Remember to Save Changes

NOTE: Recommended setting for 802.11b/g/n is to only use channels 1, 6 and 11. For 802.11a/n/ac/ax, use channels according to the infrastructure manufacturer, country regulations, and guidelines below (p. 16).



Wireless > Monitor > Access Points > MAC (of an AP)

- Edit the location of the AP

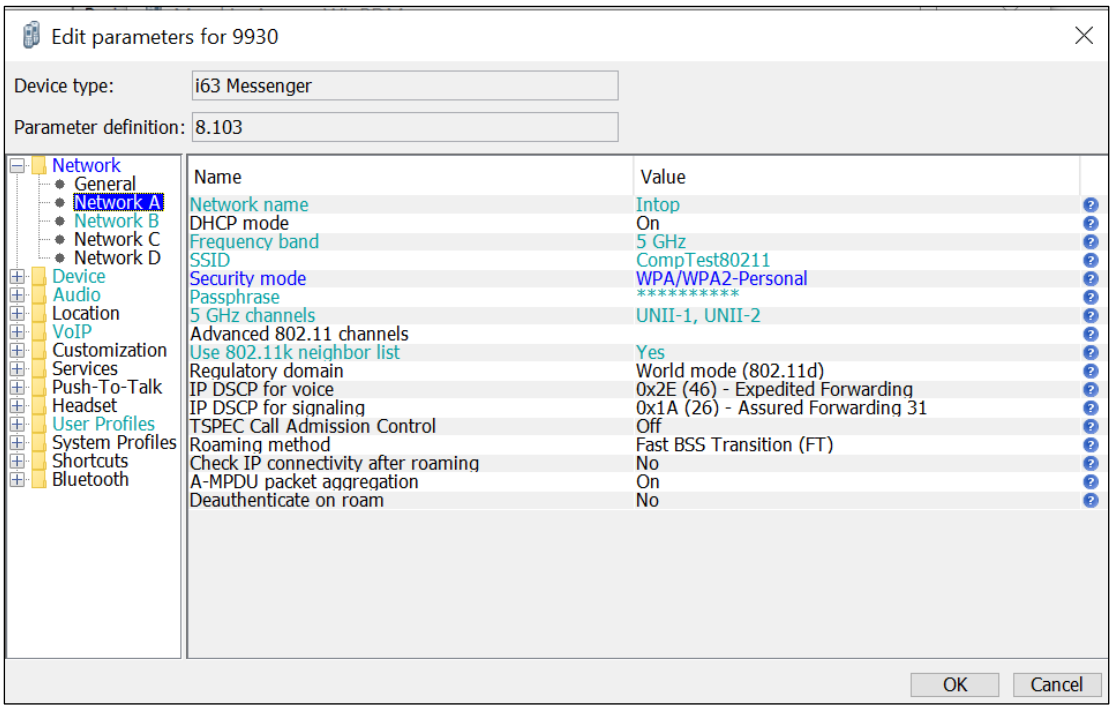
These settings served as our baseline throughout most of testing.

Take note of that TX power levels and channels were set manually for testing purposes. A typical setup will rely on global settings for channel and power configuration.

General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac/ax environments:

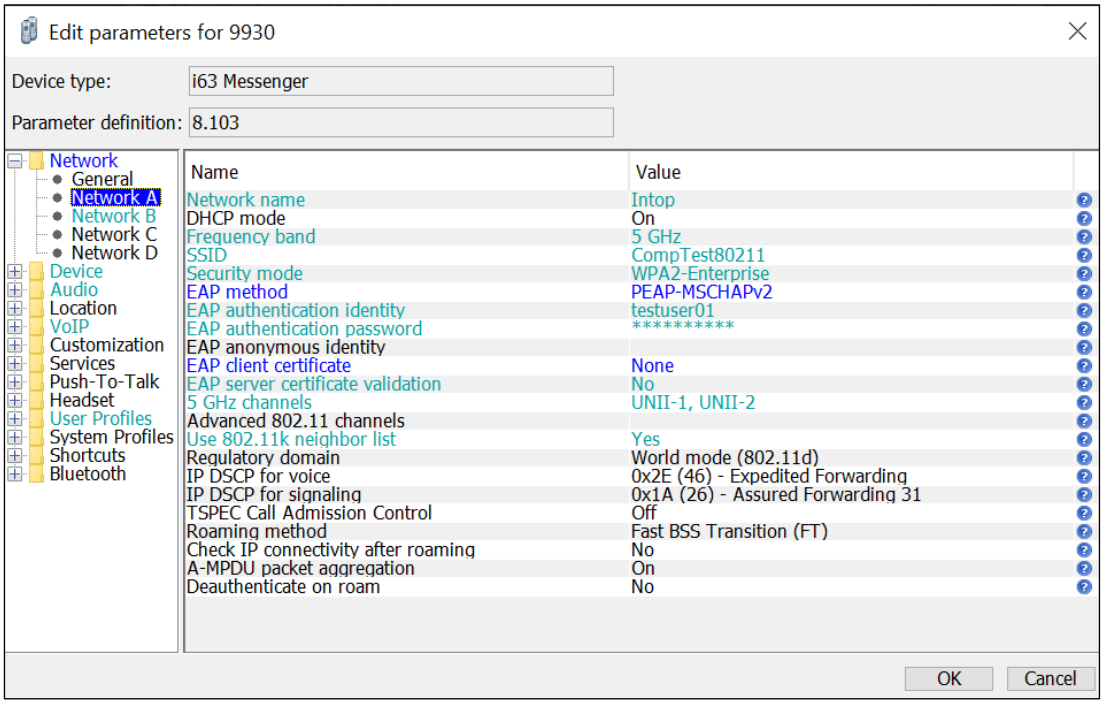
1. **For environments not utilizing 802.11k Neighbor Reports, enabling more than 8 channels will degrade roaming performance. In situations where UNII1 and UNII3 bands are used, a maximum of 9 enabled channels can be allowed. Ascom does not recommend exceeding these limits unless 802.11k is in use.**
2. **Ascom does support and can coexist in 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 the "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)**



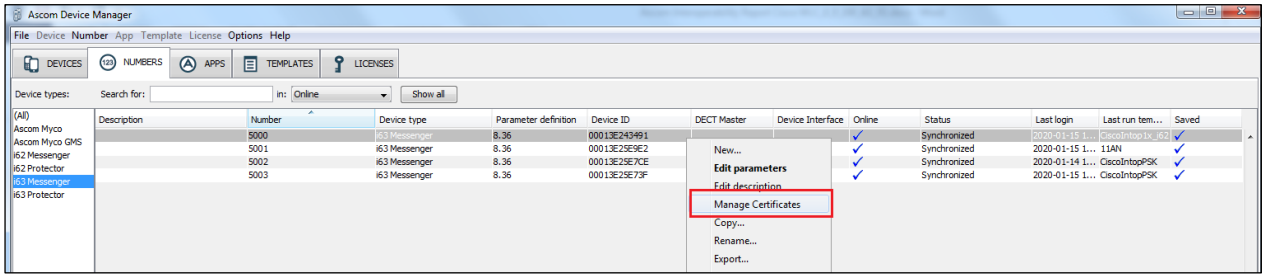
Network settings for WPA2-PSK

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



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

NOTE: The FCC no longer allows 802.11d to determine the regulatory domain. Accordingly, devices deployed in the United States must have the "Regulatory domain" set to "USA".



802.1X Authentication requires a CA certificate to be uploaded to the phone by “right clicking” - > Manage certificates.

Note that both CA and client certificates are needed for TLS.

Appendix B: Interoperability Verification Records

Pass	15 (15) *
Fail	0 (0)
Comments	7 (7)
Not verified	4 (4)
Total	26 (26)

*) 802.11ax AP's (802.11ac wave 2 AP's)

Please see attached files for detailed test results.

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

Document History

Rev	Date	Author	Description
PA1	29-Sept-2021	SEMW	First draft.
PA2	05-Oct-2021	SEMW	Further updates and screenshots added.
R1	12-Oct-2021	SEMW	Adjustments relating to feedback from the peer review.