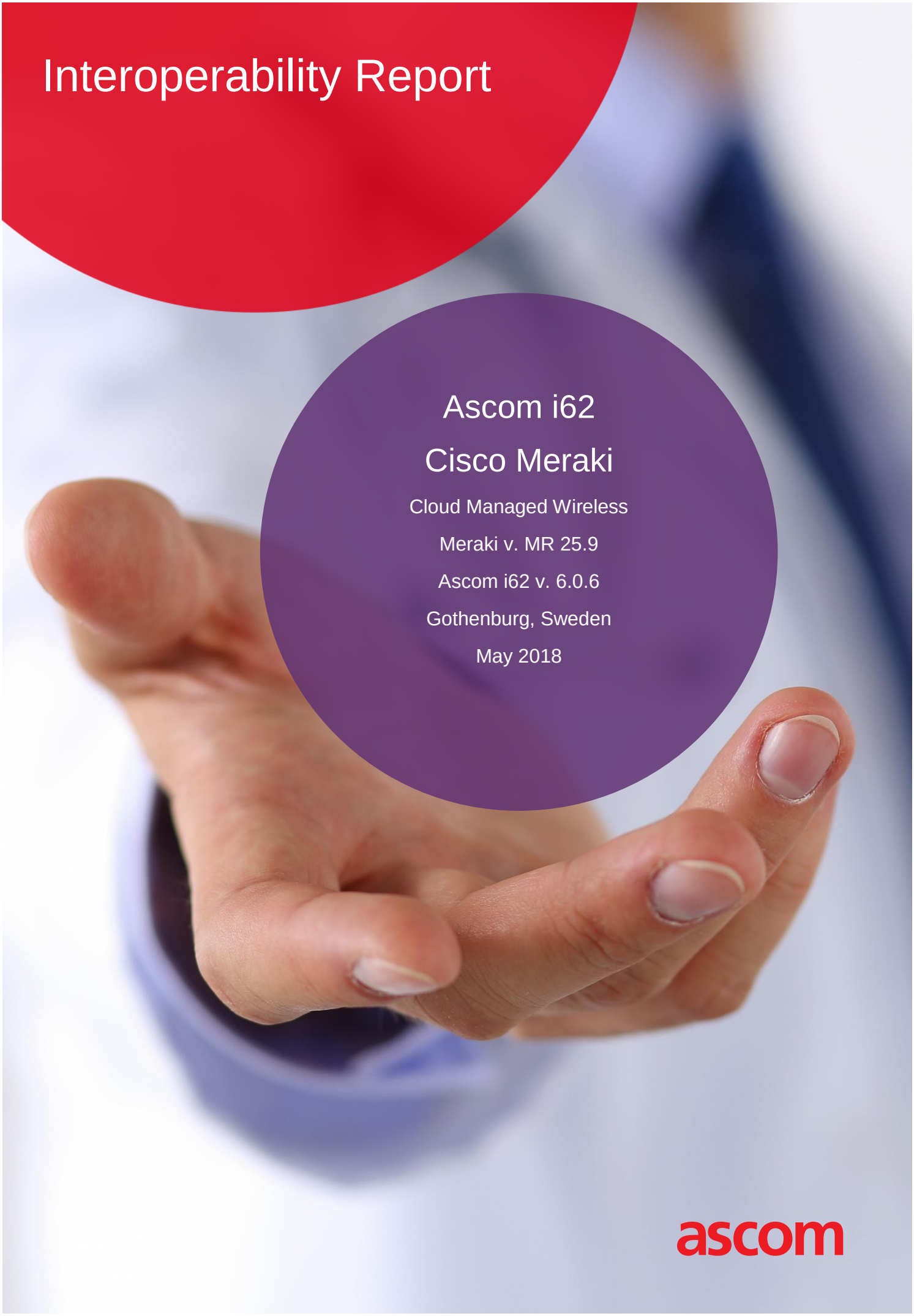
Interoperability Report



Ascom i62

Cisco Meraki

Cloud Managed Wireless

Meraki v. MR 25.9

Ascom i62 v. 6.0.6

Gothenburg, Sweden

May 2018

ascom

Contents

Introduction

This document describes a summary of the interoperability verification results of the Ascom and Meraki platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Meraki and Ascom's 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 subsidiaries in 15 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

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 230,000 customers and 3 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.

Site Information

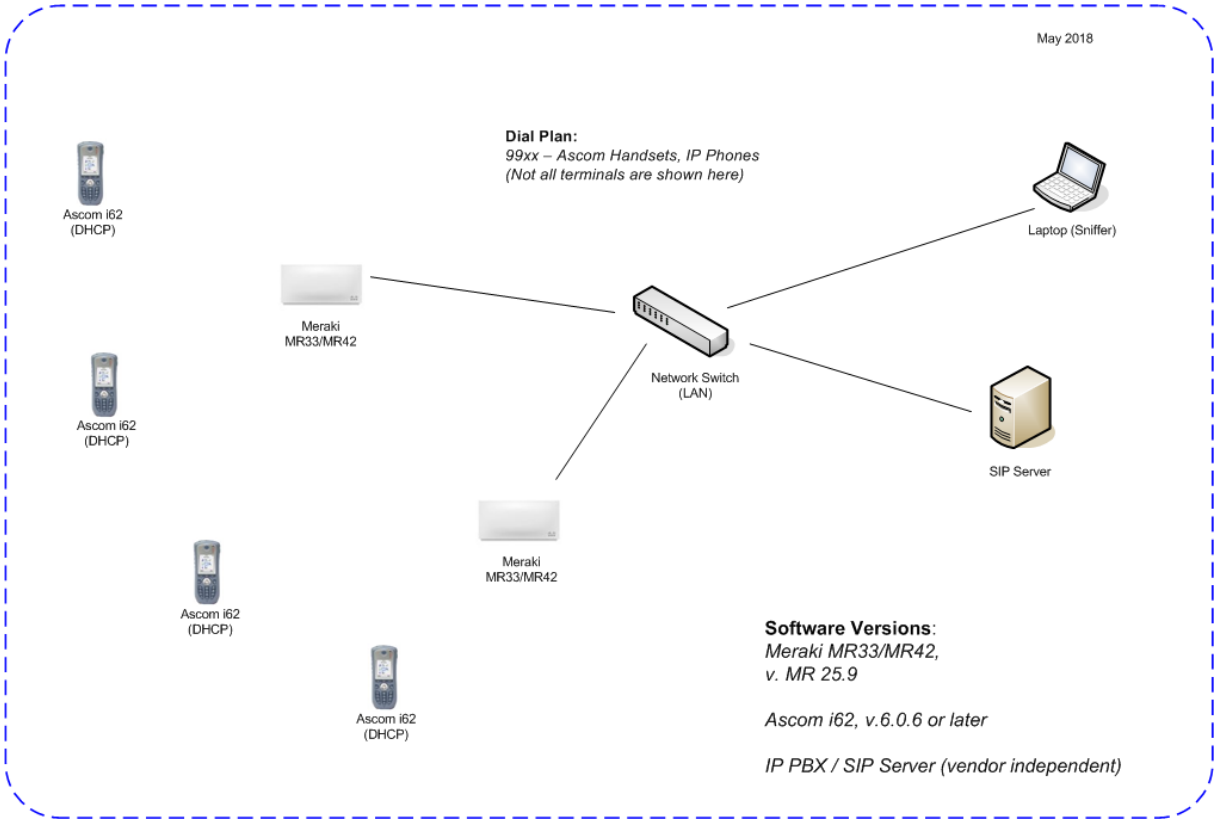
Interoperability Verification Site

Ascom,
Gothenburg,
Sweden

Participants

Matthew Williams, Ascom, Gothenburg

Test topology



Summary

General Conclusions

The verification, including association, authentication, roaming, and load tests produced good results overall. Roaming times were in general good with typical values within the range of 45-75 ms, both when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES). Battery lifetime in idle state was, however, below par due to a fixed DTIM period of one.

Load testing showed that at least twelve Ascom i62 Handsets could maintain a call via a single Meraki access point when tested in U-APSD mode. Note that twelve was the maximum number of devices tested and not the capacity limit.

Compatibility Information

The following Meraki access point models were selected for this interoperability validation: MR33, MR42. By testing these access points we are considered to cover a certain product range of Meraki access points.

Supported Partner Access Points with version MR 25.9:

MR20/MR30H/MR33

MR42/MR42E/MR52/MR53/MR53E

MR70/MR74/MR84

Overview of Results

Ascom i62, version 6.0.6
Meraki MR33/MR42, version MR 25.9

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	N/T *	DTIM Period = 1, cannot be changed through 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	Typical avg. 45-75 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK ***	Typical avg. 45-75 ms

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

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

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

Known limitations

Description	Workaround	Ticket(s) raised
Meraki advertises a DTIM Period of 1, which increases the battery consumption of the Ascom i62 in idle mode (observed standby time: >60 hours).	No workaround available. DTIM Period = 1 cannot be changed through GUI.	

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.

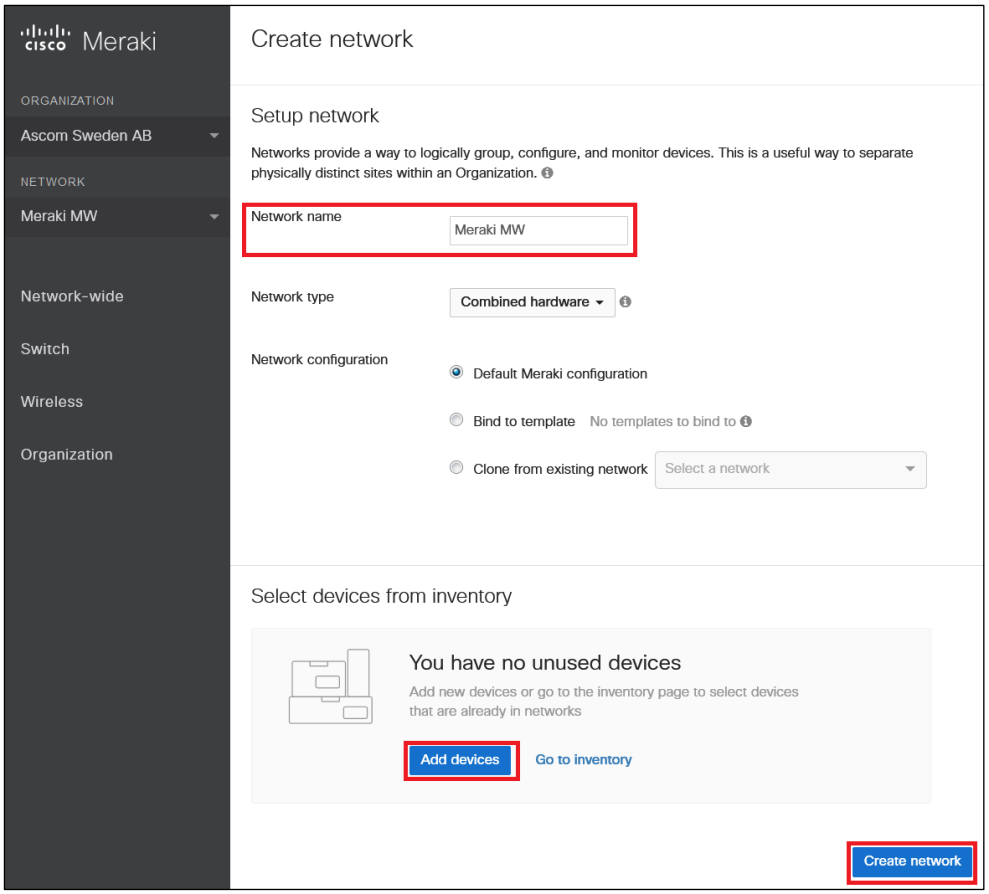
Appendix A: Interoperability Verification Configurations

Meraki MR33/MR42, v. MR 25.9

This section includes screenshots and explanations of basic settings required to use Ascom i62 handsets with Meraki Access Points. Please note the security settings of each test case, as they were modified according to needs of the test cases.

The configuration file is found at the end of Appendix B.

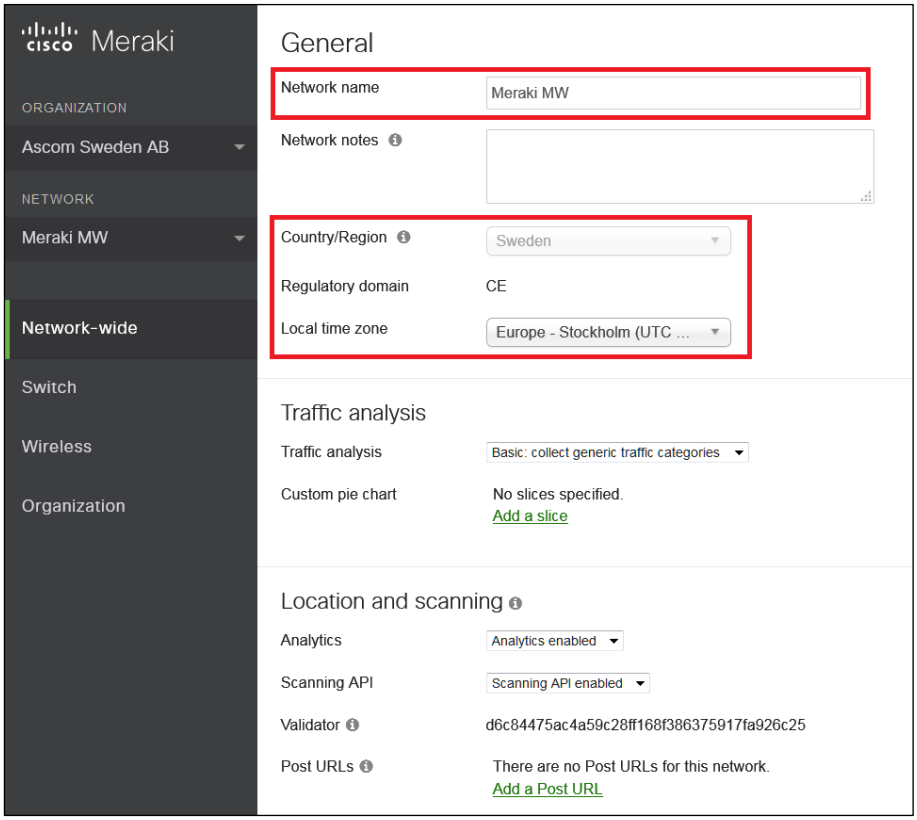
General settings (SSID, Authentication, Radio and QoS)



Network > Create a new network

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

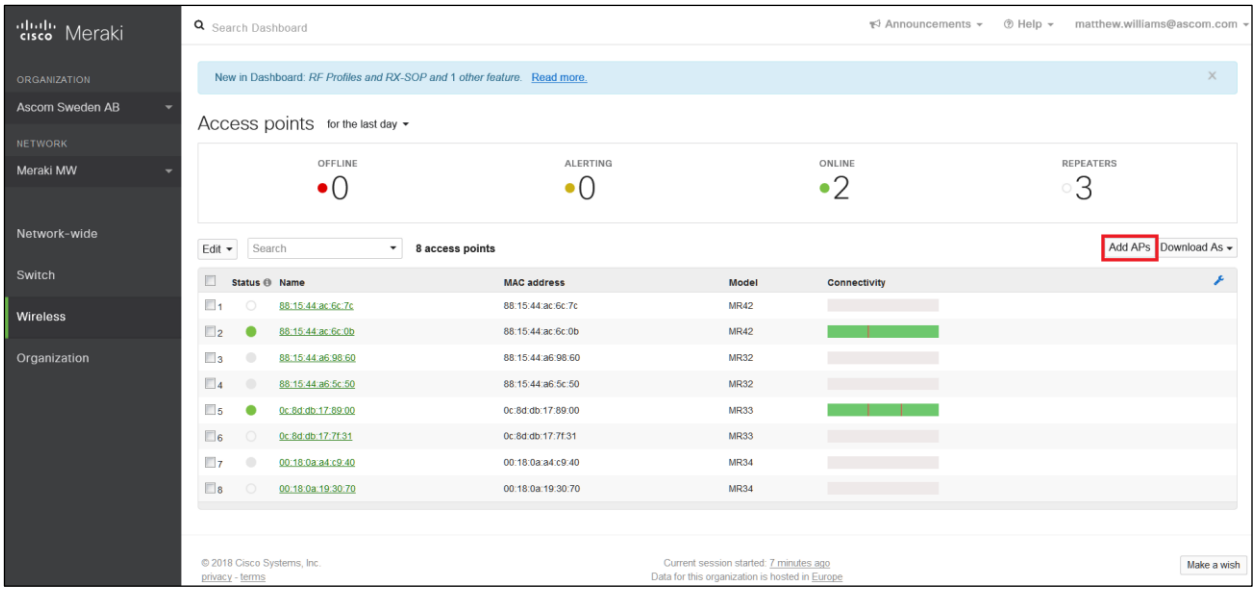
Please refer to Meraki's documentation on how to create a hierachy of organizations, networks and the concept of claiming to an inventory. Only after the latter can devices be added to networks.



Network-Wide > Configure > General

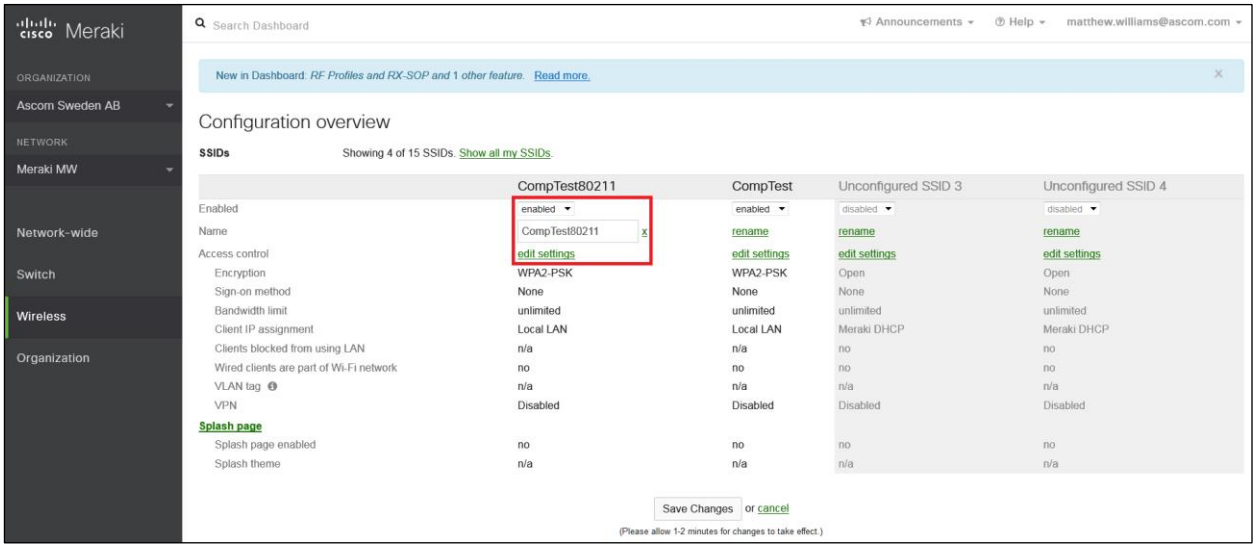
- Network Name defined in previous step
- Set Country/Region (Regulatory Domain inferred from this setting)
- Set the Local Time Zone
- Remember to save settings

All other parameters were left at their defaults during testing.



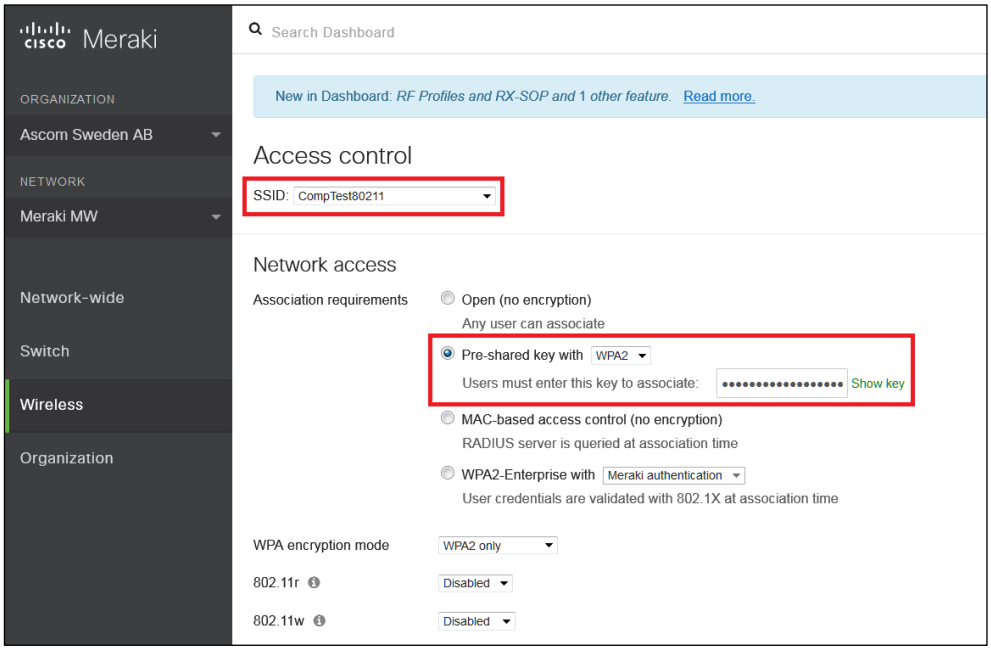
Wireless > Monitor > Access Points

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



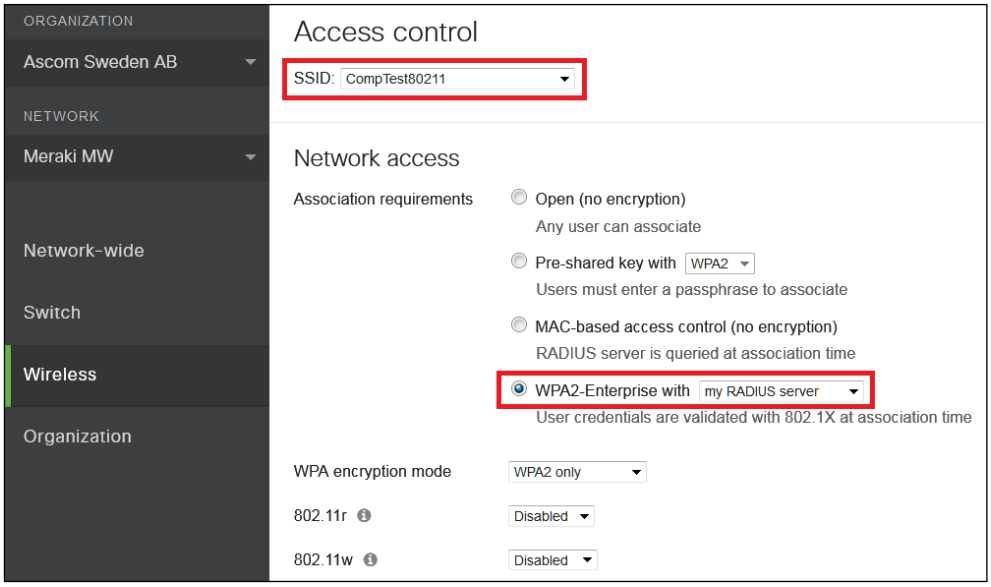
Wireless > Configure > SSID

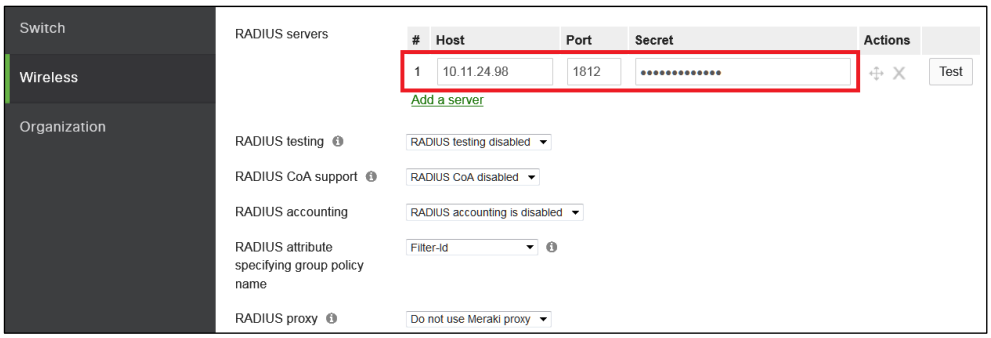
- Define Name (SSID)
- Edit Access Control (Security Settings, see next page)
- Remember to enable SSID



Wireless > Configure > Access Control (WPA2-PSK)

- Select SSID
- Enter WPA2 Pre-shared Key

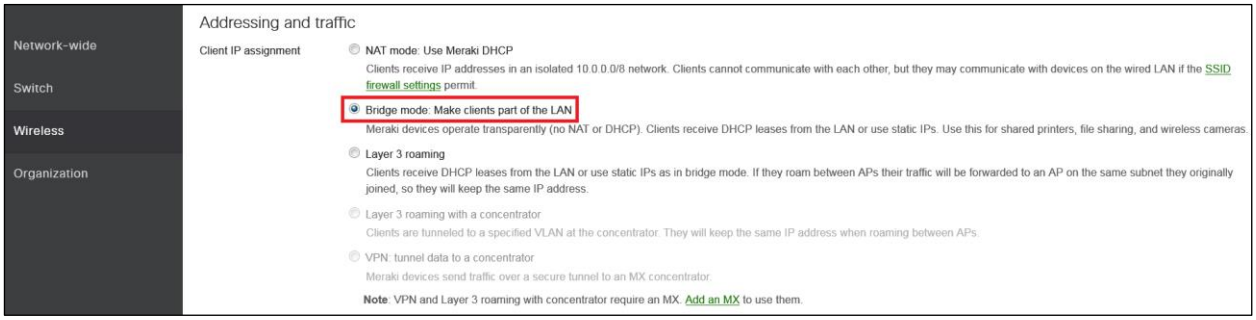




Wireless > Configure > Access Control (802.1X)

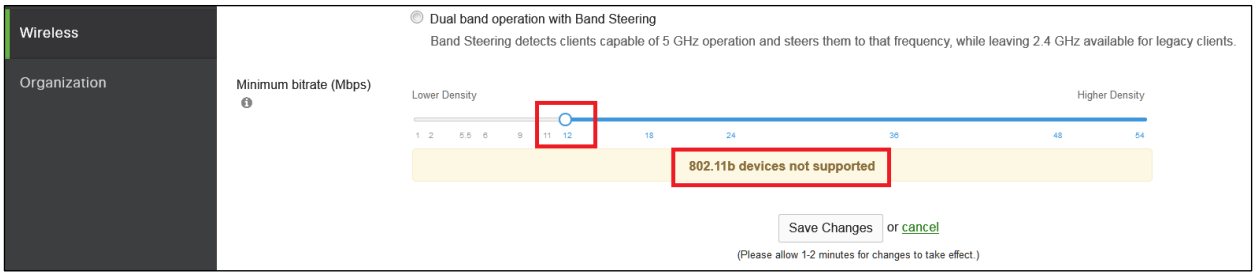
- Select SSID
- Select WPA2-Enterprise with “my RADIUS server” (unless the internal server is used)
- Define a RADIUS server
- Opportunistic Key Caching is enabled by default.

NOTE: Ensure that unsupported features 802.11r (fast roaming) & 802.11w (protected management frames) are disabled (default).



Wireless > Configure > Access Control (step 2)

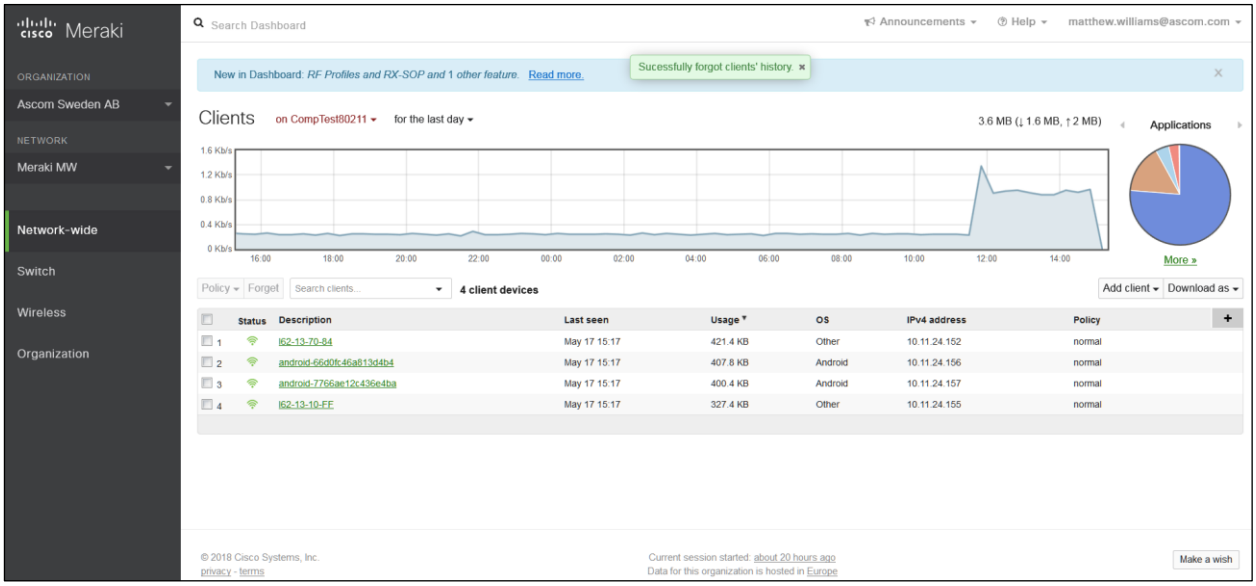
- Select Bridge Mode should clients need to recieve leases from a DHCP server on the LAN



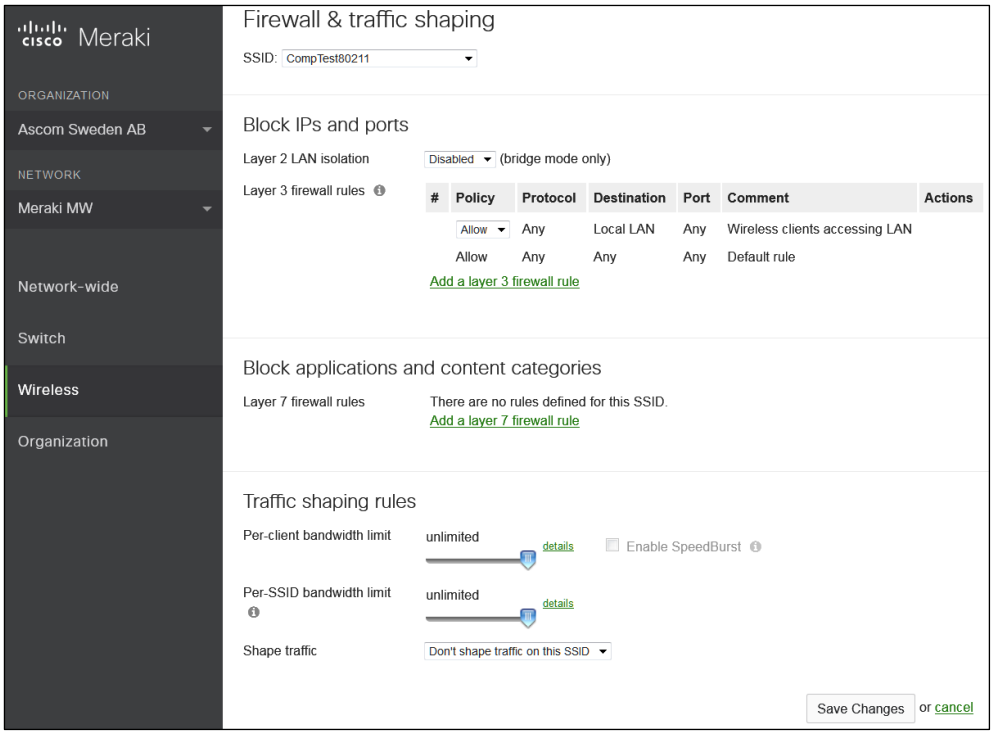
Wireless > Configure > Access Control (step 3)

- 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.

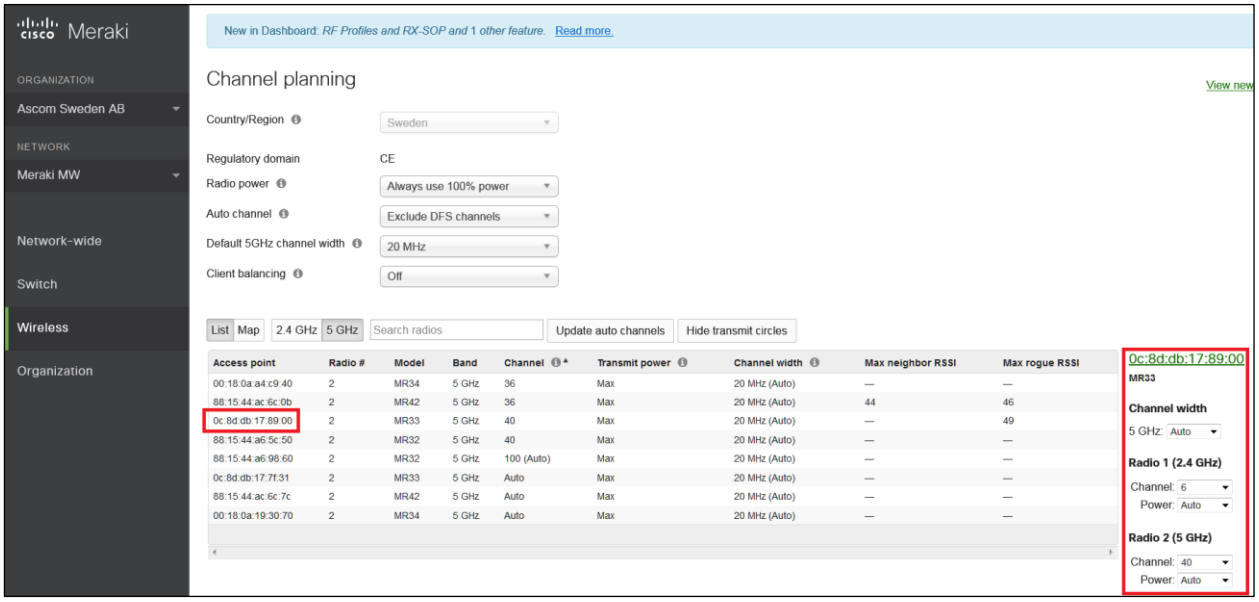


SSID Overview (Network-Wide > Monitor > Clients)



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

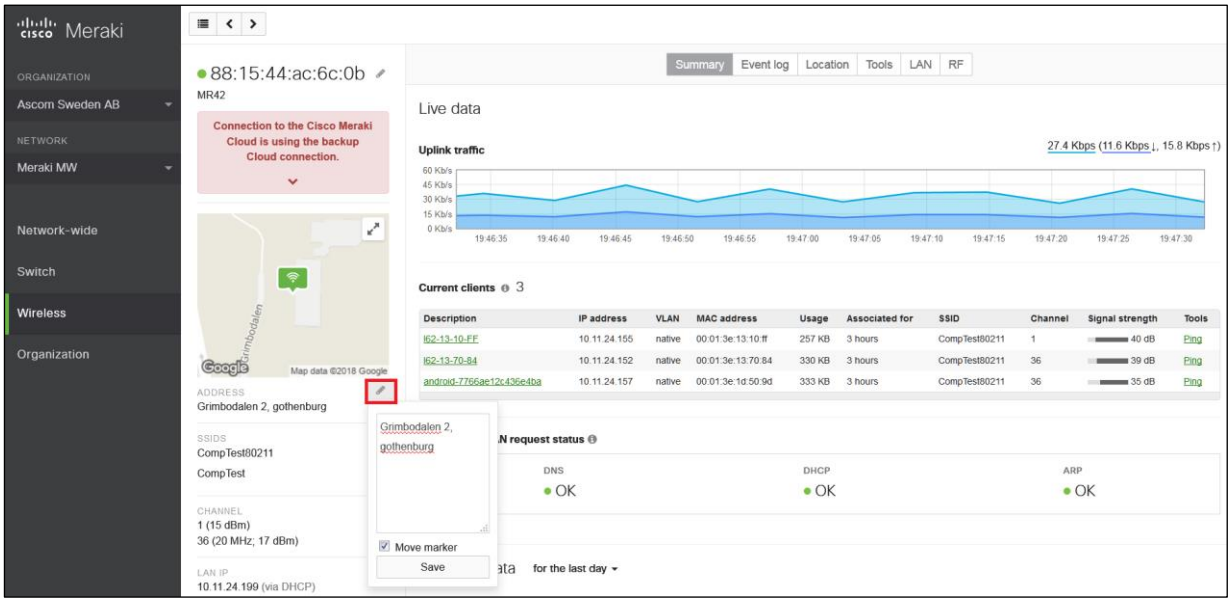
- No need to modify (included as reference)
- To match default mappings, ensure the i62 uses DSCP AF 31 (or best effort) for signalling and DSCP EF 46 for Voice.



Wireless > Configure > Radio Settings

- Regulatory Domain inferred from Country/Region of network
- Select MAC of an AP
- Adjust Radio1 and Radio2 to the appropriate settings
- Remember to Save Changes

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



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

- Edit the location of the AP

These settings served as our baseline throughout most of testing.

General guidelines when deploying Ascom I62 handsets in 802.11a/n/ac environments:

1. ***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 this limit.***

2. ***Using 40 MHz channels (or "channel-bonding") will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 40MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.***

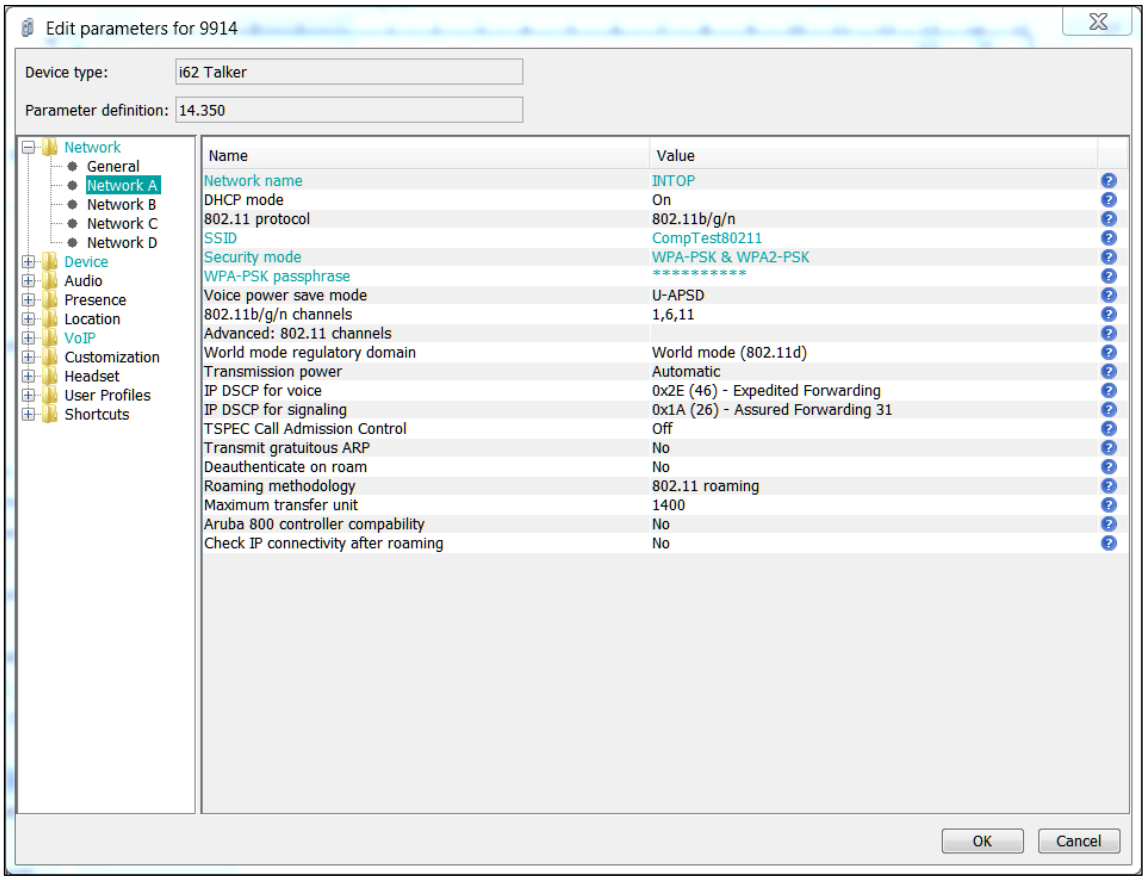
3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***

4. ***Make sure that all non-DFS channel 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 VoWIFI deployments.***

***) Dynamic Frequency Selection (radar detection)**

See Appendix B for the configuration used for the certification process.

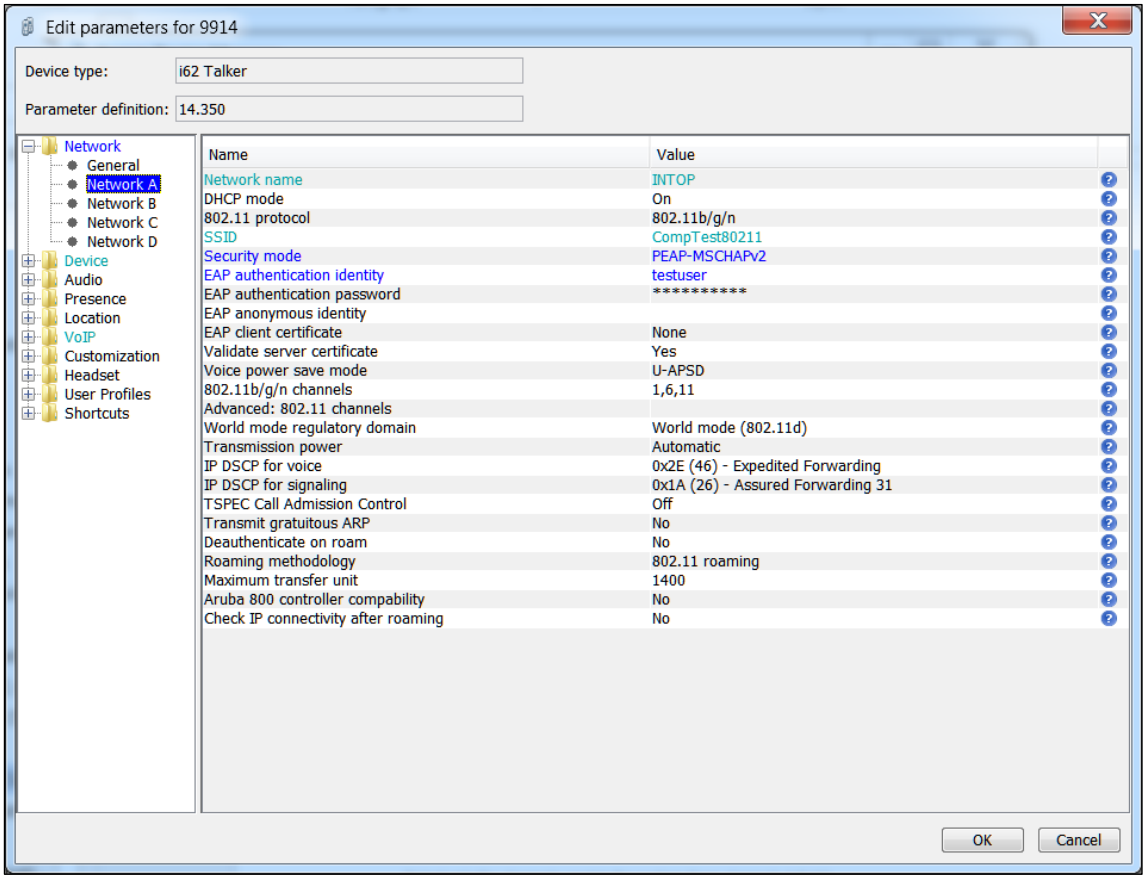
Ascom i62 Settings Summary



Network settings for WPA2-PSK

- Select frequency band according to system setup (here 802.11b/g/n).
- Select only the channels used in the system (here channels 1,6,11).

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



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

- Select frequency band according to system setup (here 802.11b/g/n).
- Select only the channels used in the system (here channels 1,6,11).

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

Appendix B: Interoperability Verification Records

Test Protocol

Refer to attached Excel file for detailed test results.

The test specification containing information about each test case can be found here (requires login):
https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability/Templates/

Meraki Test Configuration

Not included here, please see explanation below:

On Meraki, configurations aren't backed up in the conventional way. To save and modify configurations, one has to clone the network in the cloud and then, while the other acts as backup, make changes to only one network. Please refer to Meraki's documentation for further information:

https://documentation.meraki.com/zGeneral_Administration/Organizations_and_Networks/Creating_and_Deleting_Dashboard_Networks

Document History

Rev	Date	Author	Description
PA1	2018-05-18	SEMW	First draft
PA2	2018-05-23	SEMW	Peer review
R1	2018-05-30	SEMW	Final version