

INTEROPERABILITY REPORT

Ascom i63

Meraki

Cloud-Managed Wi-Fi platform

Meraki MR 30.7

Ascom i63 v. 6.0.0

Utrecht, The Netherlands

November 2024

ascom

Contents

Introduction.....	3
About Ascom.....	3
About Meraki.....	3
Site Information.....	4
Test site	4
Participants	4
Test topology.....	4
Summary	5
General conclusions	5
Compatibility information	5
Feature overview	6
Known limitations.....	7
Appendix A: Test Configurations	8
Meraki Cloud-Managed Wi-Fi platform MR 30.7.....	8
Ascom i63 v 6.0.0 Network settings.....	21
Appendix B: Interoperability Verification Records	25
Document History	25

Introduction

This document describes a summary of the interoperability validation results of the Ascom and Meraki's platforms, furthermore it provides the necessary steps and guidelines to optimally configure the respective platforms. This report should be used in conjunction with configuration guides from both Meraki and Ascom.

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 19 countries and employs around 1,400 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

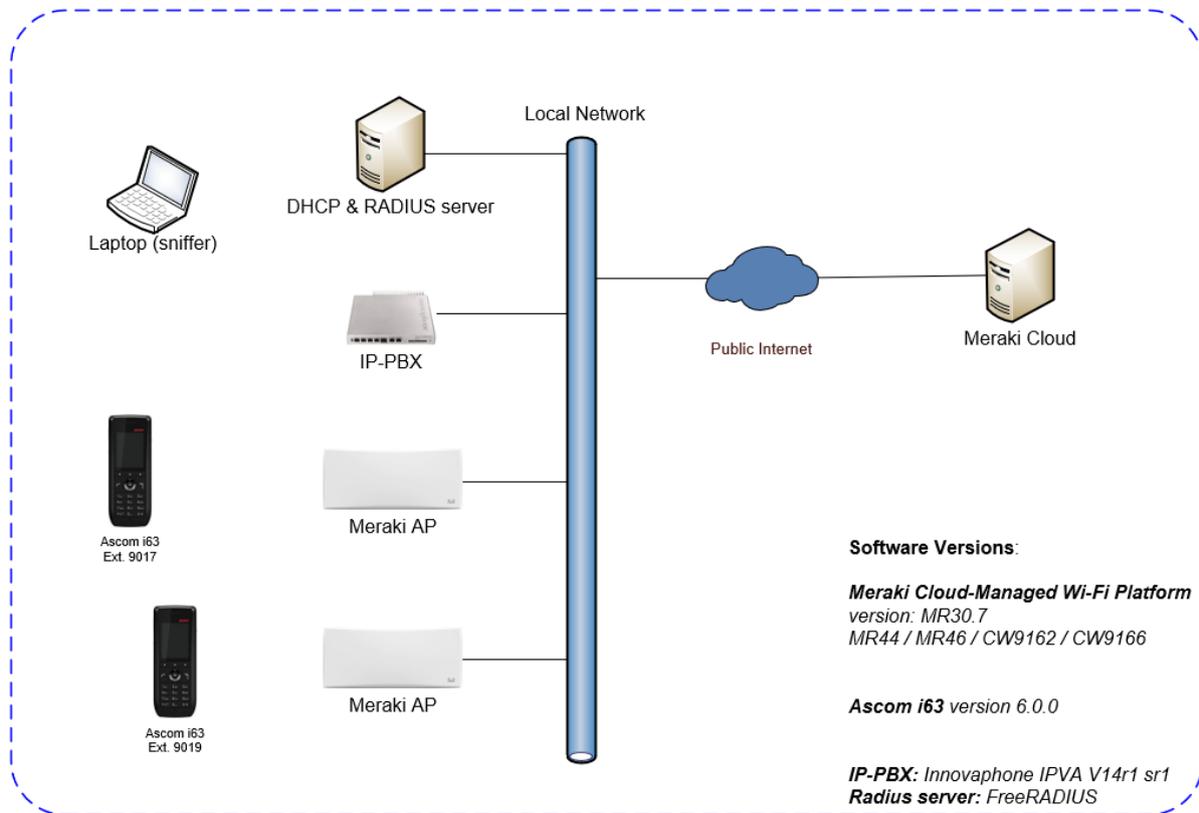
Test site

Ascom Nederland
Orteliuslaan 982
3528 BD Utrecht
The Netherlands

Participants

Remco van den Pangaart, Ascom NL

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.

To accomplish optimal roaming performance, it is recommended to enable Fast Roaming (802.11r/FT) when using WPA3-Personal or 802.1X based authentication.

Please refer to the “Known limitations” section for details.

Compatibility information

Access point models have been selected in dialogue with Meraki (MR44, MR46, CW9162 and CW9166). 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 MR30.7:

Wi-Fi 6 (802.11ax):

MR36

MR44

MR46 / MR46E

MR56

MR76

MR78

MR86

Wi-Fi 6E

CW9162

CW9163E

CW9164

CW9166

CW9166D1

Feature overview

WLAN Compatibility and Performance

High Level Functionality	Result	Comments
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/A*	DTIM Period = 1, cannot be changed in Web GUI
PMKSA Caching	OK	
WMM Prioritization	OK	
WPA2-opportunistic/proactive Key Caching	OK	
802.11e U-APSD	OK	
CAC – TSPEC	N/A	Not supported by WLAN infrastructure
Roaming, WPA2-PSK, AES Encryption	OK	Typical roaming time 33ms
Roaming, WPA2-PSK, AES Encryption, 802.11r/FT	OK	Typical roaming time 24ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK	Typical roaming time 37ms (OKC enabled by default on WLAN infrastructure)
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption, 802.11r/FT	OK	Typical roaming time 28ms
Roaming, WPA3-SAE authentication, AES encryption	OK	Typical roaming time 104ms
Roaming, WPA3-SAE authentication, AES encryption + FT	OK	Typical roaming time 33ms
Roaming, WPA3-Enterprise + FT	OK	Typical roaming time 40ms
Channel usage controlled by 802.11k	Ok	
Association with Protected Management Frames 802.11w	OK*	

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

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 Web GUI.	
WPA3 Enterprise 192-bit mode is not supported by handset hardware.	No workaround available.	

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

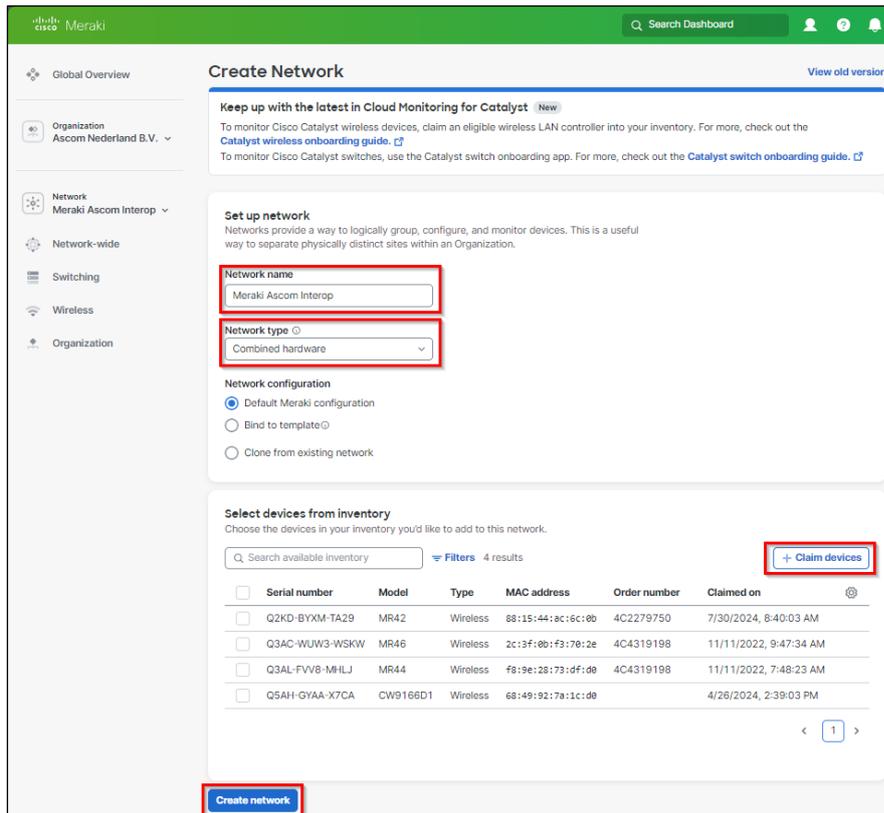
For detailed test results, refer to Appendix B: Interoperability Verification Records.

Appendix A: Test Configurations

Meraki Cloud-Managed Wi-Fi platform MR 30.7

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.

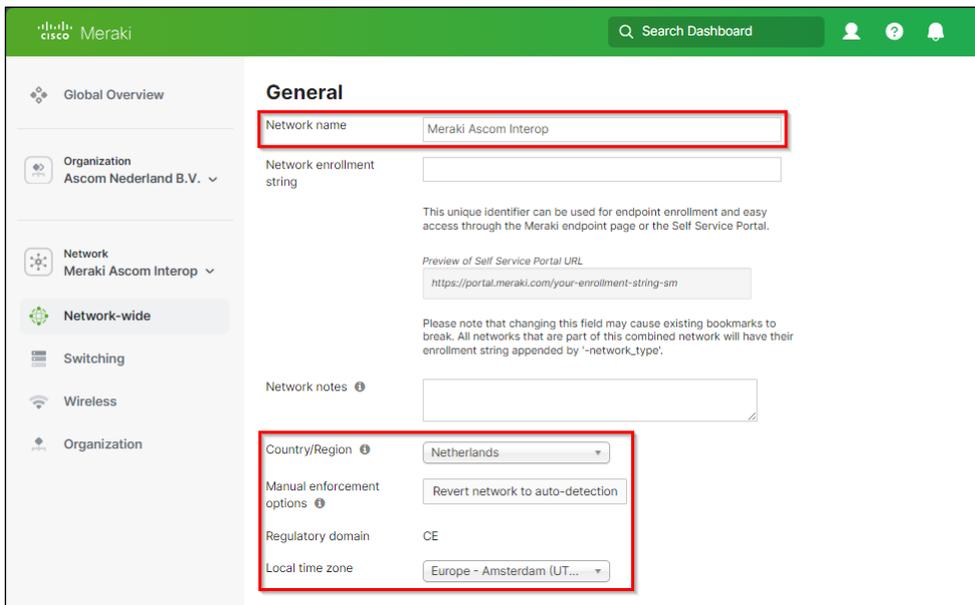
General settings (SSID, Authentication, Radio and QoS)



Network > Create a new network

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

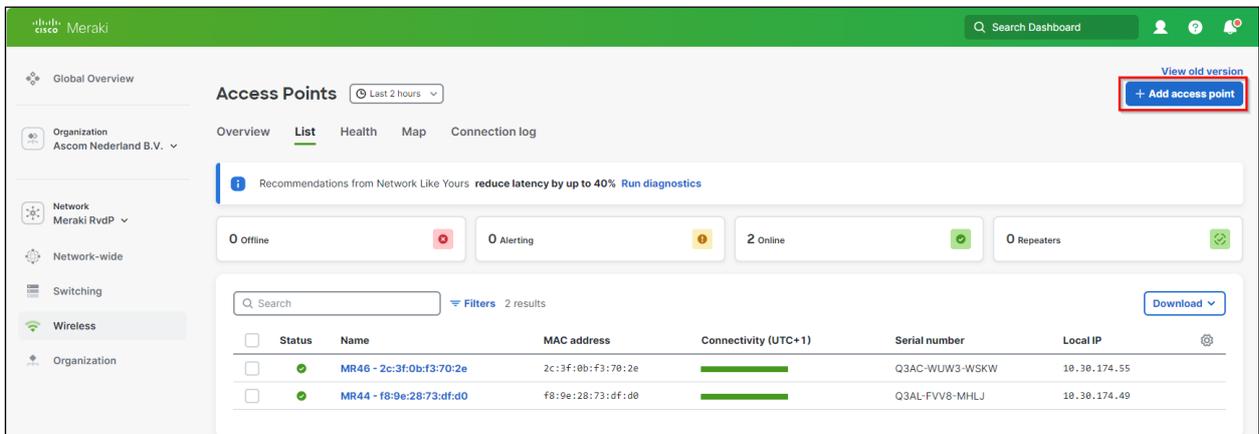
Please refer to Meraki's documentation on how to create a hierarchy of organizations, networks, and the concept of claiming to an inventory. Only after the latter devices can be added to networks.



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)

List of all configured SSIDs

The screenshot shows the Meraki configuration dashboard. On the left is a navigation sidebar with categories: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki Ascom Interop), Network-wide, Switching, Wireless, and Organization. The main content area is titled 'Configuration overview' and 'SSIDs', showing 4 of 15 SSIDs. A table lists settings for four SSIDs: MerakilntopPSK, Merakilntop1X, MerakilntopWPA3, and MerakilntopWPA3-1X. At the bottom of the table are 'Save Changes' and 'cancel' buttons, with a note: '(Please allow 1-2 minutes for changes to take effect.)'

	MerakilntopPSK	Merakilntop1X	MerakilntopWPA3	MerakilntopWPA3-1X
Enabled	<input type="checkbox" value="enabled"/>	<input type="checkbox" value="enabled"/>	<input type="checkbox" value="enabled"/>	<input type="checkbox" value="enabled"/>
Name	rename	rename	rename	rename
Access control	edit settings	edit settings	edit settings	edit settings
Encryption	PSK (WPA2)	802.1X with custom RADIUS	PSK (WPA3-SAE)	802.1X with custom RADIUS
Sign-on method	None	None	None	None
Bandwidth limit	unlimited	unlimited	unlimited	unlimited
Client IP assignment	Local LAN	Local LAN	Local LAN	Local LAN
Clients blocked from using LAN	no	no	no	no
Wired clients are part of Wi-Fi network	no	no	no	no
VLAN tag	n/a	n/a	n/a	n/a
Tunnel	Disabled	Disabled	Disabled	Disabled
Splash page				
Splash page enabled	no	no	no	no
Splash theme	n/a	n/a	n/a	n/a

Wireless > SSIDs

WPA2 PSK (Personal)

The screenshot shows the Meraki dashboard interface for configuring WPA2 PSK (Personal). The left sidebar contains navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki RvdP), Network-wide, Switching, Wireless (selected), and Organization. The main content area is titled "Access control" and includes the following sections:

- SSID:** MerakiIntopPSK (highlighted with a red box).
- Basic info:** SSID (name) is MerakiIntopPSK (highlighted with a red box). SSID status is Enabled. There is an unchecked checkbox for "Hide SSID".
- Security:** WPA2 PSK configured. The "Password" option is selected (highlighted with a red box). The password field is empty with a masked input (dots) and an eye icon. Other security options include Open (no encryption), Opportunistic Wireless Encryption (OWE), MAC-based access control (no encryption), Enterprise with Meraki Cloud Authentication, Identity PSK with RADIUS, and Identity PSK without RADIUS.
- WPA encryption:** WPA2 only (highlighted with a red box).
- 802.11r:** Enabled (highlighted with a red box). Other options are Adaptive and Disabled.
- 802.11w:** Disabled (never use) is selected. Other options are Enabled (allow unsupported clients) and Required (reject unsupported clients).
- Mandatory DHCP:** Enabled.

Wireless > Configure > Access Control

- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security Select Password and enter WPA2 Pre-shared Key (PSK)
- Remember to enable SSID.

The screenshot shows the Cisco Meraki dashboard interface. The left sidebar contains navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki RvdP), Network-wide, Switching, Wireless (selected), and Organization. The main content area is titled 'Security' with a sub-header 'WPA2 PSK configured'. Below this, there are several configuration sections:

- Mandatory DHCP:** A toggle switch set to 'Enabled'.
- Splash page:** Set to 'None'.
- RADIUS:** A link to expand the section.
- Client IP and VLAN:** Sub-header 'Bridge mode'. It contains two radio button options:
 - Meraki AP assigned (NAT mode):** Unselected. Description: Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.
 - External DHCP server assigned:** Selected and highlighted with a red box. Description: Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras. Below this are two buttons: 'Bridged' (selected) and 'Tunneled'.
- Layer 3 roaming:** A checkbox that is unchecked.
- RADIUS guest VLAN:** A dropdown menu set to 'Disabled'.
- Bonjour forwarding:** A toggle switch set to 'Disabled'.
- VLAN tagging:** A dropdown menu set to 'Disabled'.
- Assign group policies by device type:** A toggle switch set to 'Disabled'.

 At the bottom, there is a warning message: 'Looking for Wireless options? Per-SSID band and bitrate settings have moved to the Radio Settings page.' with a 'Go to Radio Settings' button. Below the warning are 'Cancel' and 'Save' buttons, and a note: '(Please allow 1-2 minutes for changes to take effect.)'

Wireless > Configure > Access Control (step 2)

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

The screenshot shows the Meraki dashboard configuration for WPA2 802.1X (Enterprise). The interface is organized into a sidebar and a main content area. The sidebar includes navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki RvdP), Network-wide, Switching, Wireless, and Organization. The main content area is titled 'Access control' and is divided into sections: Basic info, Security, and WPA encryption. Red boxes highlight the SSID selection, SSID name, Enterprise with my RADIUS server option, and the 802.11r and 802.11w settings.

Wireless > Configure > Access Control

- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security Select “Enterprise with” and select “my RADIUS server” (unless the internal server is used)
- Remember to enable SSID.

Meraki Search Dashboard

RADIUS 1 RADIUS server

RADIUS servers

#	Host IP or FQDN	Auth port	Secret	RadSec	Test	Actions
1	10.30.174.5	1812	<input type="checkbox"/>	Test	...

Add server 3 max.

RADIUS accounting servers

#	Host IP or FQDN	Acct port	Secret	RadSec	Actions
You have no servers defined					

Add server 3 max.

RADIUS testing

RADIUS CoA support

RADIUS proxy

RADIUS attribute specifying group policy name

Advanced RADIUS settings
(NAS ID, Called-station-ID, RADIUS timeout, retry count, fallback, EAP timers)

Client IP and VLAN Bridge mode

Meraki AP assigned (NAT mode)
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.

External DHCP server assigned
Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras.

Layer 3 roaming

Wireless > Configure > Access Control (step 2)

- Define a RADIUS server
- Select External DHCP server and Bridge Mode, should clients need to receive leases from a DHCP server on the LAN.

WPA3 PSK (Personal)

The screenshot shows the Meraki dashboard configuration for WPA3 PSK (Personal). The interface is divided into a sidebar and a main content area. The sidebar contains navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki Ascom Interop), Network-wide, Switching, Wireless, and Organization. The main content area is titled "Access control" and is divided into sections: Basic info, Security, and WPA encryption. Red boxes highlight the following elements: the SSID dropdown menu (MerakiIntopWPA3), the SSID (name) input field (MerakiIntopWPA3), the Password selection and input field, the WPA3 only encryption method selection, and the 802.11r Enabled selection. The SSID status is set to Enabled, and the Mandatory DHCP is set to Disabled.

Wireless > Configure > Access Control

- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security select Password and enter a password.
- Select WPA3 only as WPA encryption method
- Select Enabled for 802.11r to enable Fast Transition.
- Remember to enable SSID.

The screenshot shows the Meraki dashboard interface for configuring Access Control. The left sidebar contains navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki Ascom Interop), Network-wide, Switching, Wireless (selected), and Organization. The main content area is titled 'Access control' and shows the SSID 'MerakiIntopWPA3'. Below this are sections for 'Basic info', 'Security' (WPA3 SAE configured), 'Splash page' (None), and 'RADIUS'. The 'Client IP and VLAN' section is expanded, showing two radio button options: 'Meraki AP assigned (NAT mode)' and 'External DHCP server assigned'. The 'External DHCP server assigned' option is selected and highlighted with a red box. Under this option, there are two buttons: 'Bridged' (selected) and 'Tunneled'. There is also a checkbox for 'Layer 3 roaming' which is unchecked. Below the highlighted section are settings for 'RADIUS guest VLAN' (Disabled), 'Bonjour forwarding' (Disabled), and 'VLAN tagging' (Disabled). At the bottom, there is a notification: 'Looking for Wireless options? Per-SSID band and bitrate settings have moved to the Radio Settings page.' with a 'Go to Radio Settings' button. At the very bottom, there are 'Cancel' and 'Save' buttons, and a note: '(Please allow 1-2 minutes for changes to take effect.)'

Wireless > Configure > Access Control (step 2)

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

The screenshot displays the Meraki dashboard configuration for an SSID named "MerakintopWPA3-1X". The configuration is divided into several sections:

- SSID:** MerakintopWPA3-1X
- Basic info:**
 - SSID (name): MerakintopWPA3-1X
 - SSID status: Enabled
 - Hide SSID:
- Security:** WPA3 Enterprise with 1 RADIUS server
 - Open (no encryption): Any user can associate
 - Opportunistic Wireless Encryption (OWE): Any user can associate with data encryption
 - Password: Users must enter a passphrase to associate
 - MAC-based access control (no encryption): RADIUS server is queried at association time
 - Enterprise with:** my RADIUS server - User credentials are validated with 802.1X at association time
 - Identity PSK with RADIUS: RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address
 - Identity PSK without RADIUS: Devices are assigned a group policy based on its passphrase
- Wi-Fi Personal Network (WPN):** Enabled
- WPA encryption:** WPA3 only -
 - 802.11r: Enabled
 - Adaptive:
 - Disabled:
- 802.11w:**
 - Enabled (allow unsupported clients):
 - Required (reject unsupported clients):**
 - Disabled (never use):
- Mandatory DHCP:** Enabled

Wireless > Configure > Access Control

- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security Select "Enterprise with" and select "my RADIUS server" (unless the internal server is used)
- Select WPA3 only as WPA encryption method
- Select Enabled for 802.11r to enable Fast Transition.
- Remember to enable SSID.

Meraki Search Dashboard

Global Overview

Organization: Ascom Nederland B.V.

Network: Meraki Ascom Interop

Network-wide

Switching

Wireless

Organization

RADIUS 1 RADIUS server

RADIUS servers

#	Host IP or FQDN	Auth port	Secret	RadSec	Test	Actions
1	10.30.174.2	1812	<input type="checkbox"/>	Test	...

[Add server](#) 3 max.

RADIUS accounting servers

#	Host IP or FQDN	Acct port	Secret	RadSec	Actions
You have no servers defined					

[Add server](#) 3 max.

RADIUS testing

RADIUS CoA support

Dashboard RADIUS proxy

RADIUS attribute specifying group policy name:

Advanced RADIUS settings [>](#)
(NAS ID, Called-station-ID, RADIUS timeout, retry count, fallback, EAP timers)

Client IP and VLAN Bridge mode

Meraki AP assigned (NAT mode)
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.

External DHCP server assigned
Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras.

[Bridged](#) [Tunneled](#)

Layer 3 roaming

Wireless > Configure > Access Control (step 2)

- Define a RADIUS server
- Select External DHCP server and Bridge Mode, should clients need to receive leases from a DHCP server on the LAN.

Data Rate Configuration

2.4GHz radio settings

The screenshot shows the Cisco Meraki configuration interface for 2.4 GHz radio settings. The left sidebar contains navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki RvdP), Network-wide, Switching, and Wireless (selected). The main content area is titled '2.4 GHz radio settings' and includes the following settings:

- Turn off 2.4 GHz radio:** See band selection above.
- Channel assignment method:** Unless manually overridden, AutoChannel will assign radios to channels 1, 6, or 11. [Change channels used by AutoChannel...](#)
- Radio transmit power range (dBm):** A slider ranging from 2 to 30 dBm, with a current value of approximately 15 dBm.
- Set RX-SOP...**
- Minimum bitrate:** A slider ranging from 1.2 to 54 Mbps, with a current value of 12 Mbps. A red box highlights the 12 Mbps value, and a yellow warning box below it states '802.11b devices not supported'.

Wireless > Radio settings > RF profiles > Basic Indoor Profile

- Select Minimum bitrate: 12 Mbps

5GHz radio settings

The screenshot shows the Cisco Meraki configuration interface for 5 GHz radio settings. The left sidebar contains navigation options: Global Overview, Organization (Ascom Nederland B.V.), Network (Meraki RvdP), Network-wide, Switching, and Wireless (selected). The main content area is titled '5 GHz radio settings' and includes the following settings:

- Turn off 5 GHz radio:** See band selection above.
- Channel width:** A dropdown menu with 'Auto' selected and 'Manual' as an alternative.
- Channel assignment method:** Unless manually overridden, AutoChannel will assign radios to channels with low interference. [Change channels used by AutoChannel...](#)
- Radio transmit power range (dBm):** A slider ranging from 2 to 30 dBm, with a current value of approximately 15 dBm.
- Set RX-SOP...**
- Minimum bitrate:** A slider ranging from 6 to 54 Mbps, with a current value of 12 Mbps. A red box highlights the 12 Mbps value, and a yellow warning box below it states '802.11b devices not supported'.

Wireless > Radio settings > RF profiles > Basic Indoor Profile

- Select Minimum bitrate: 12 Mbps

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

These settings served as our baseline throughout most of the 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.

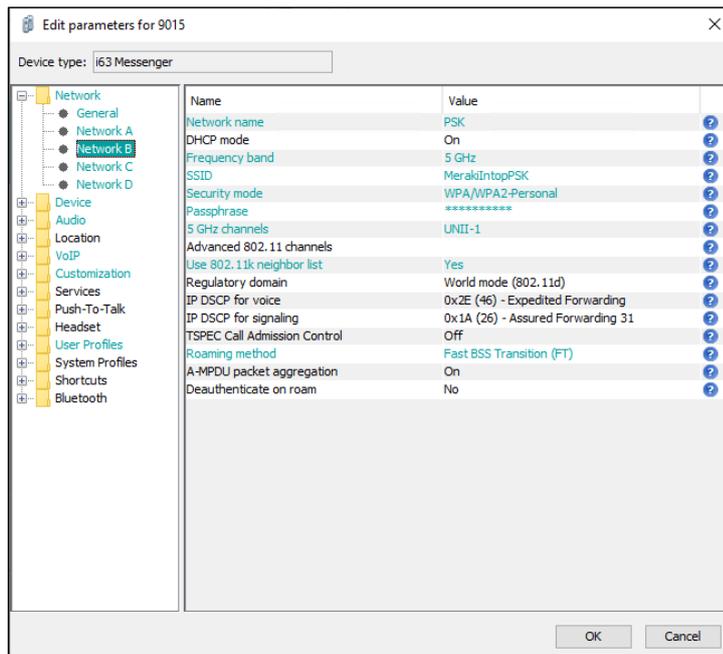
General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac/ax environments:

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)

Ascom i63 v 6.0.0 Network settings

WPA2-Personal (PSK) Network Settings

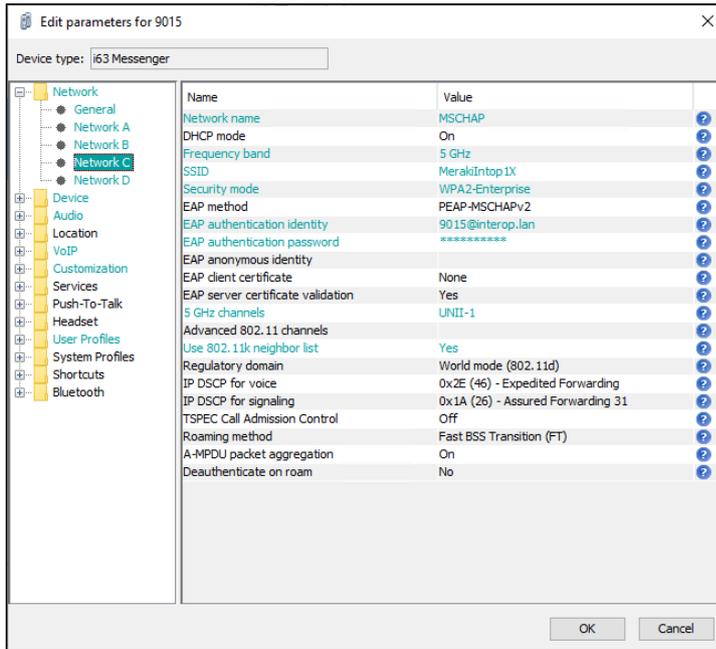


Network settings for WPA2-Personal

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA/WPA2-Personal.
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter "Use 802.11k neighbor list" to "Yes" to utilize the system provided channels list
- Set Roaming method to Fast BSS Transition (FT).

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".

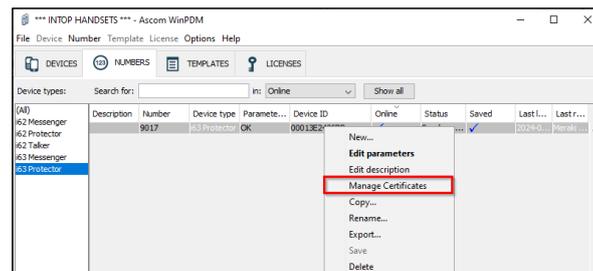
WPA2-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



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

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA2-Enterprise.
- Enter the EAP authentication identity and password.
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

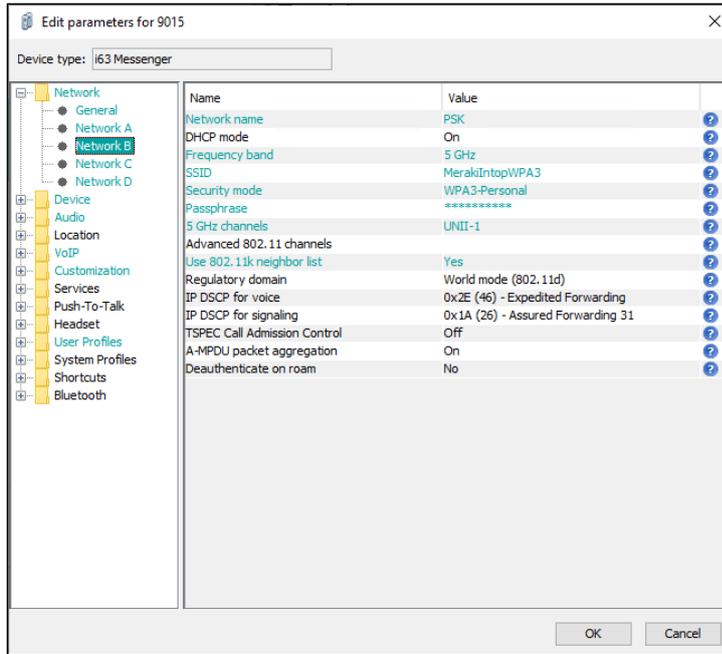
NOTE: The FCC no longer allows 802.11d to determine the regulatory domain. Accordingly, devices deployed in the United States must have the “Regulatory domain” set to “USA”.



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

Note that for EAP-TLS both Root and client certificates are needed.

WPA3-Personal (SAE) Network Settings

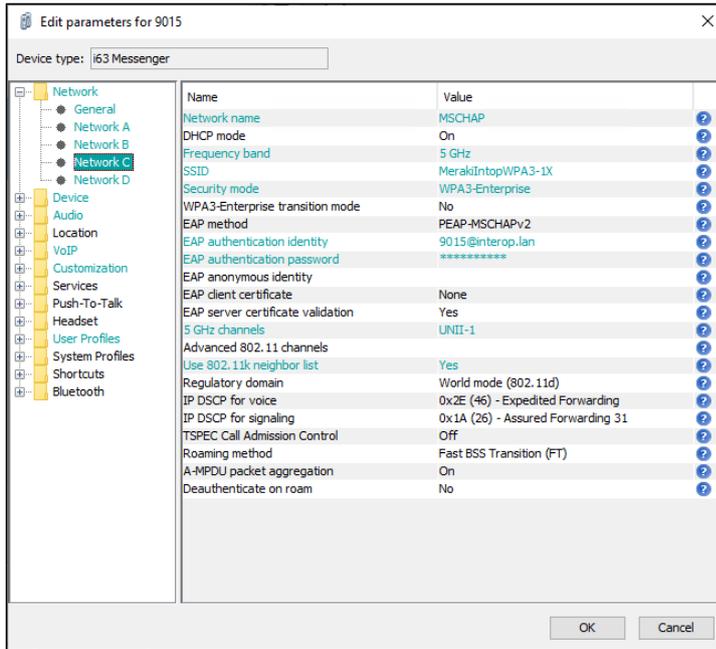


Network settings for WPA3-Personal

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA3-Personal.
- Enter the configured Passphrase
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

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”.

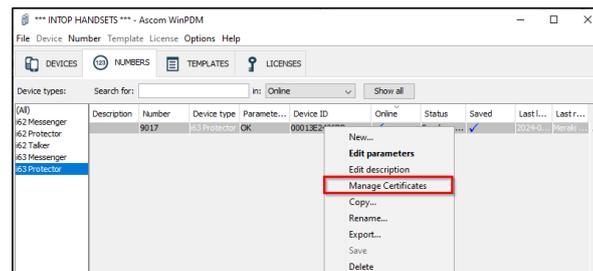
WPA3-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



Network settings for WPA3-Enterprise .1X authentication (PEAP-MSCHAPv2)

- Select frequency band according to system setup (here 5GHz)
- Enter the name of SSID configured in the WLAN system.
- Select Security mode WPA3-Enterprise.
- Enter the EAP authentication identity and password.
- Select only the channels used in the system or set parameter “Use 802.11k neighbor list” to “Yes” to utilize the system provided channels list

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 client certificate to be uploaded to the phone by “right clicking” -> Manage certificates.

Note that for EAP-TLS both Root and client certificates are needed.

Appendix B: Interoperability Verification Records

Pass	22
Fail	0
Comments	10
Not verified	3
Total	35

Refer to the attached file for detailed verification results.

Our Interoperability pages are available on the Ascom portal on the following link (requires login):
<https://oneascom.sharepoint.com/sites/AscomPartners/AscomPortal/SitePages/Interoperability.aspx>

Document History

Rev	Date	Author	Description
D1	04-Nov-2024	NLRPa	First draft.
D3	19-Nov-2024	NLRPa	Minor corrections after internal review