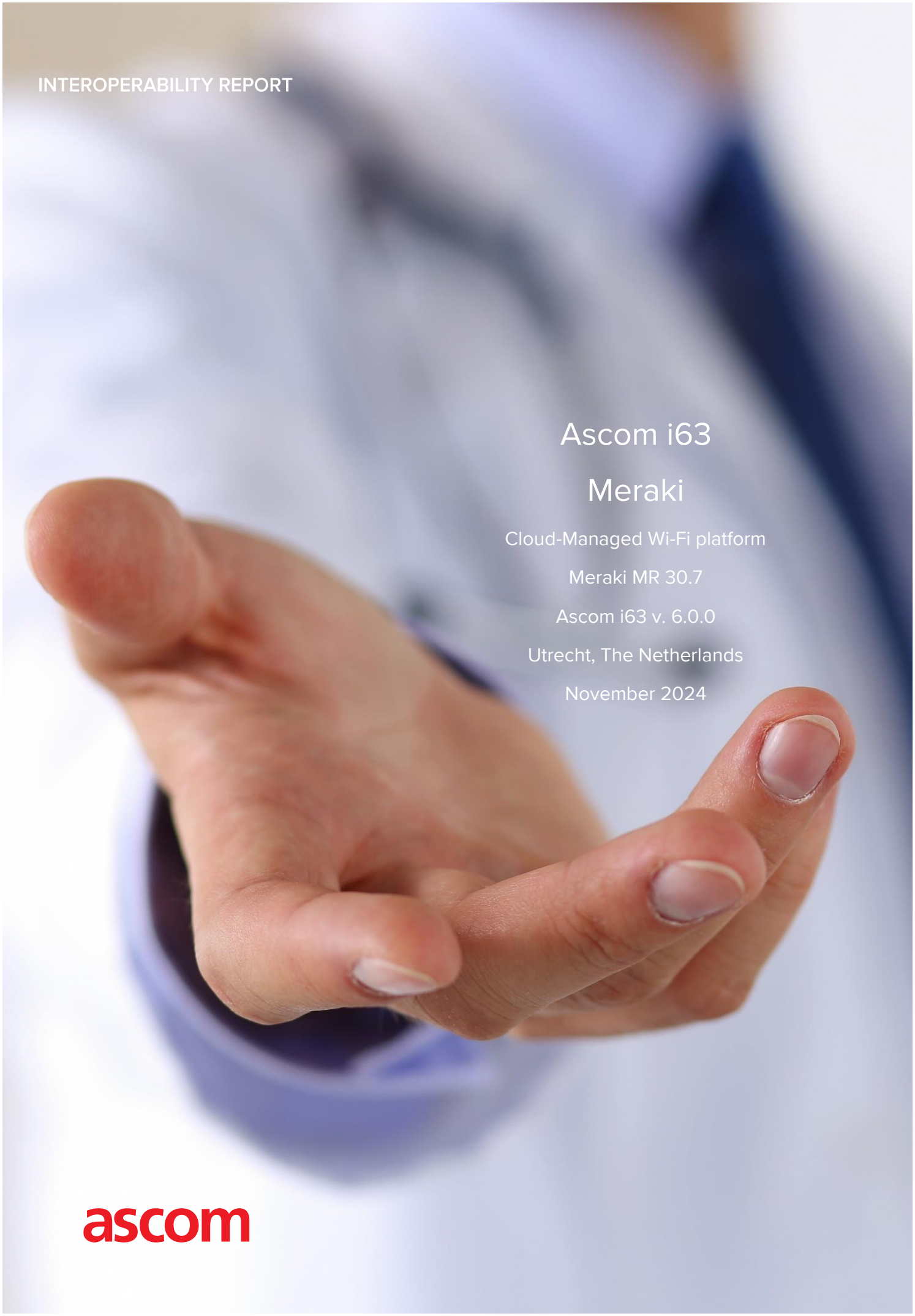
INTEROPERABILITY REPORT



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

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

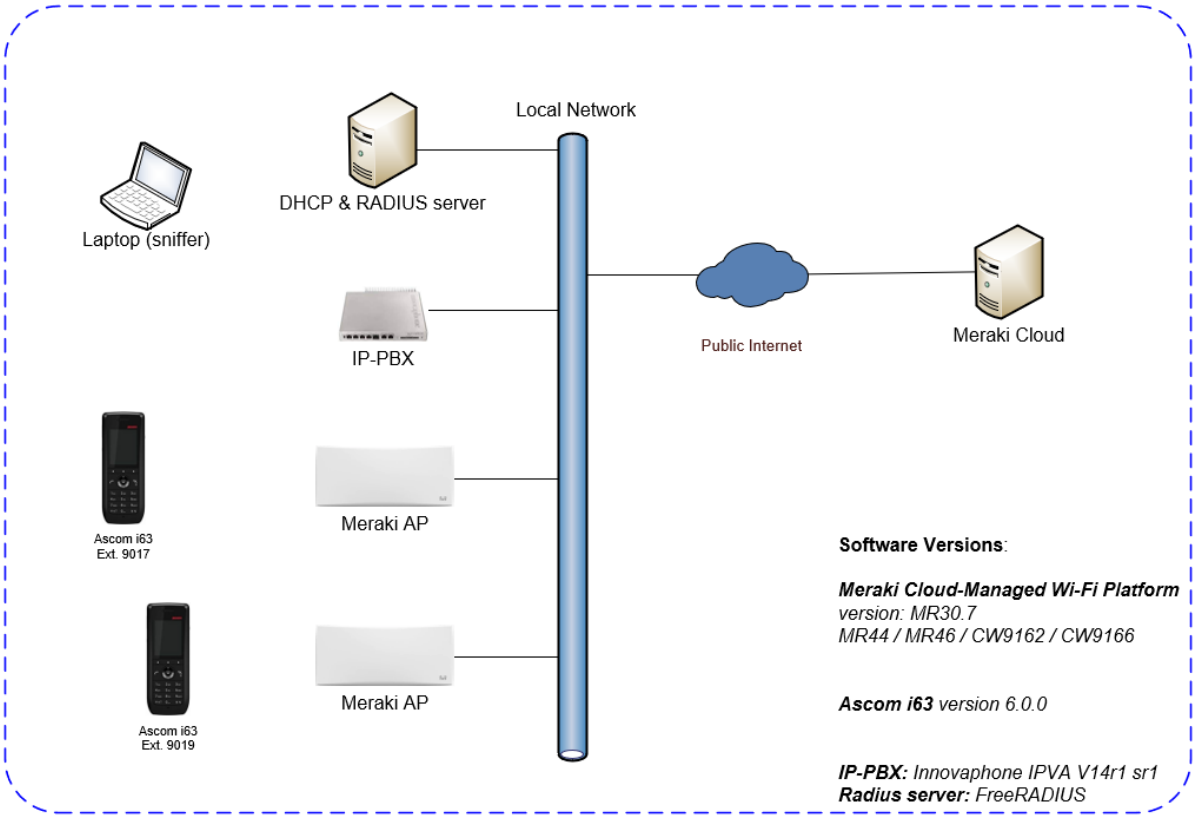
Test site

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**.

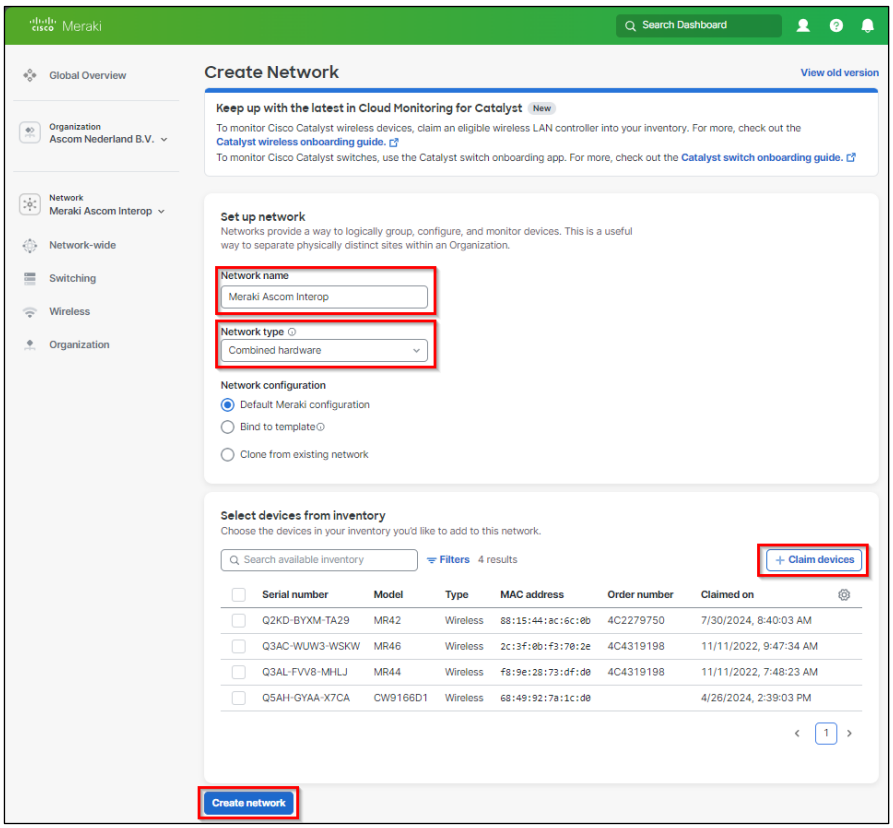
For detailed test results, refer to Appendix B: Interoperability Verification Records.

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.

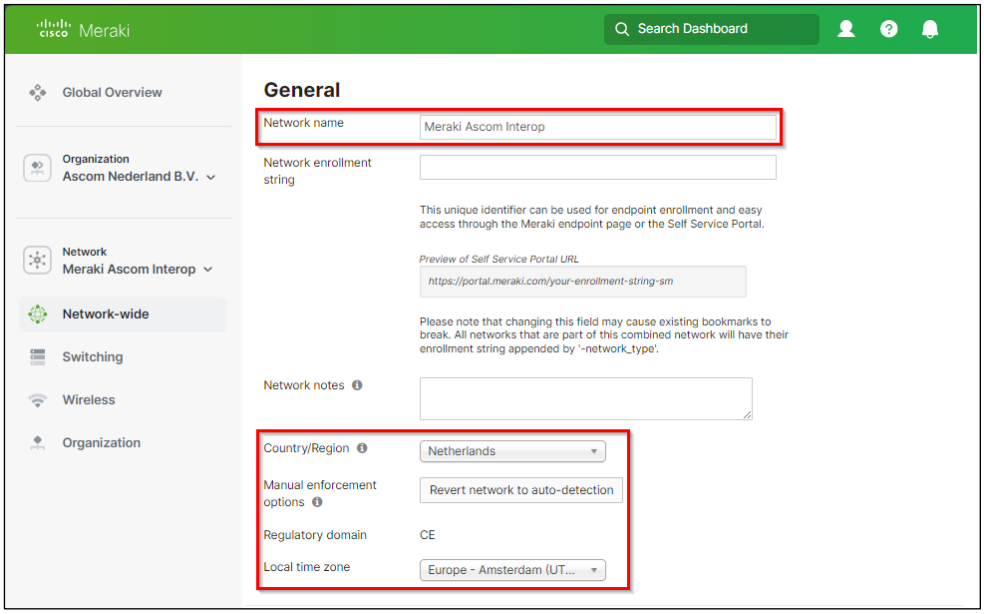
General settings (SSID, Authentication, Radio and QoS)



Network > Create a new network

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

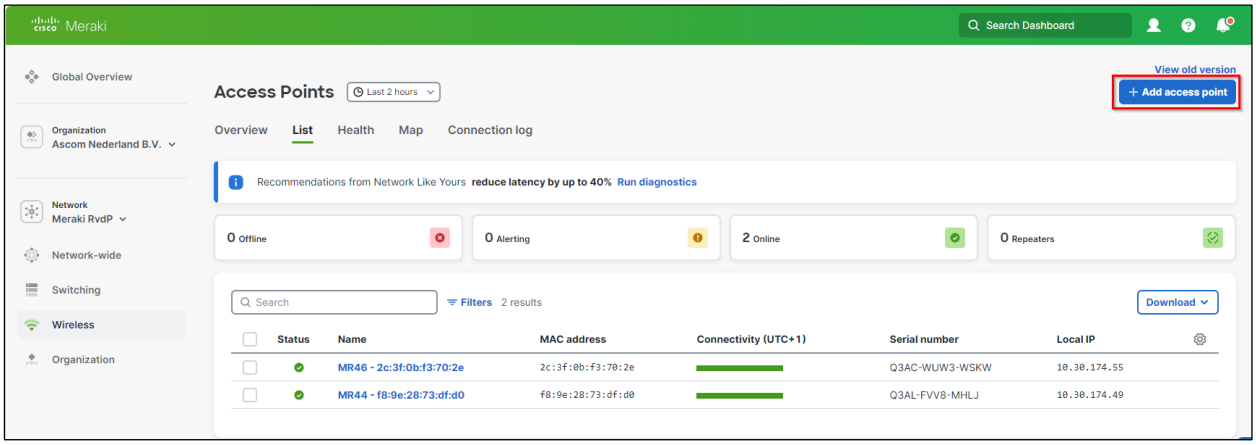
Please refer to Meraki's documentation on how to create a hierarchy of organizations, networks, and the concept of claiming to an inventory. Only after the latter devices can be added to networks.



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

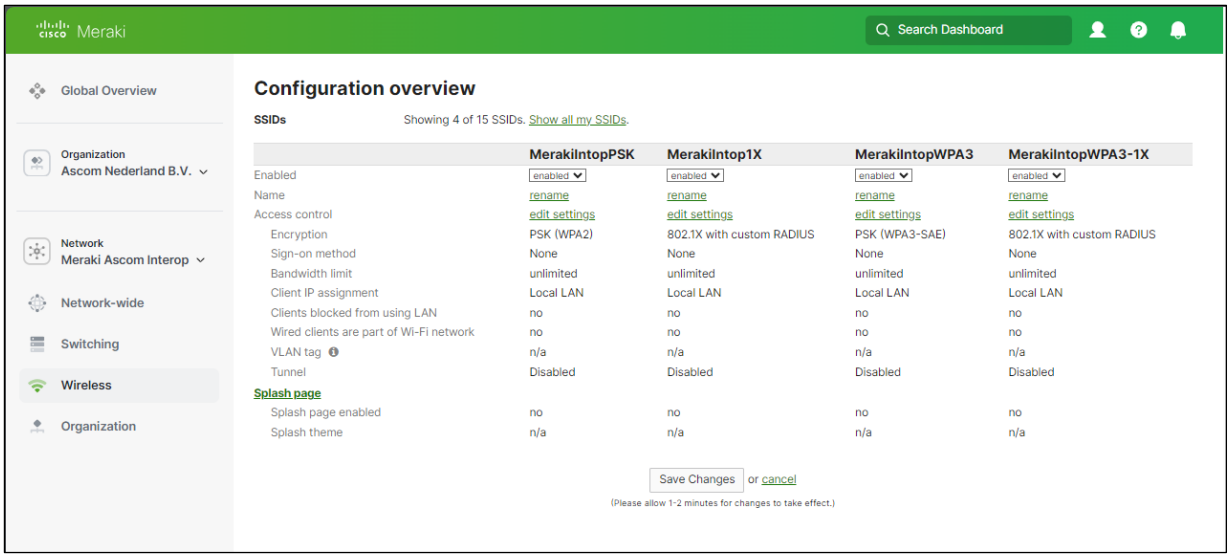
NOTE: All other parameters were left at their defaults throughout testing.



Wireless > Monitor > Access Points

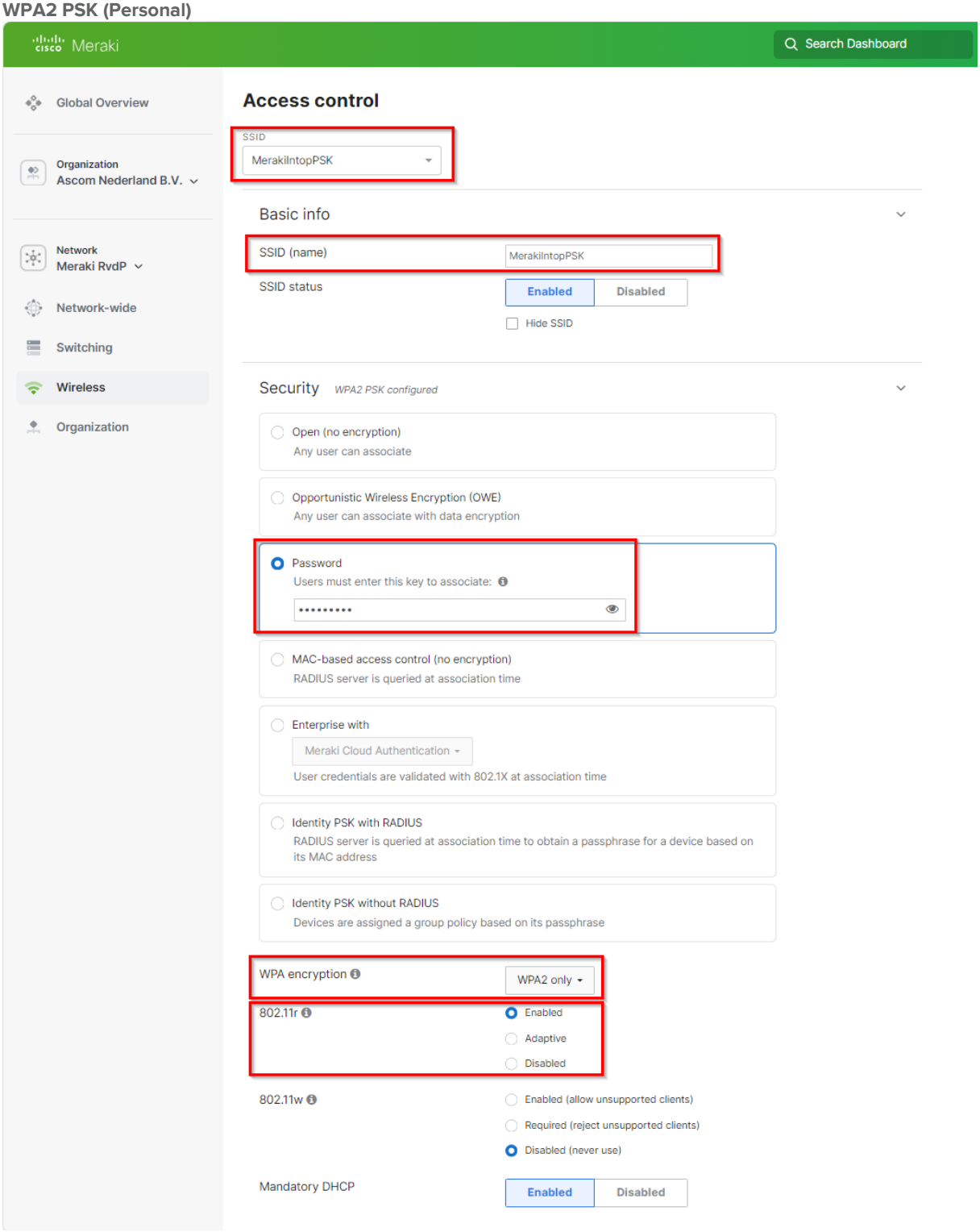
- Add AP's to the network (if not already done when creating network)

List of all configured SSIDs



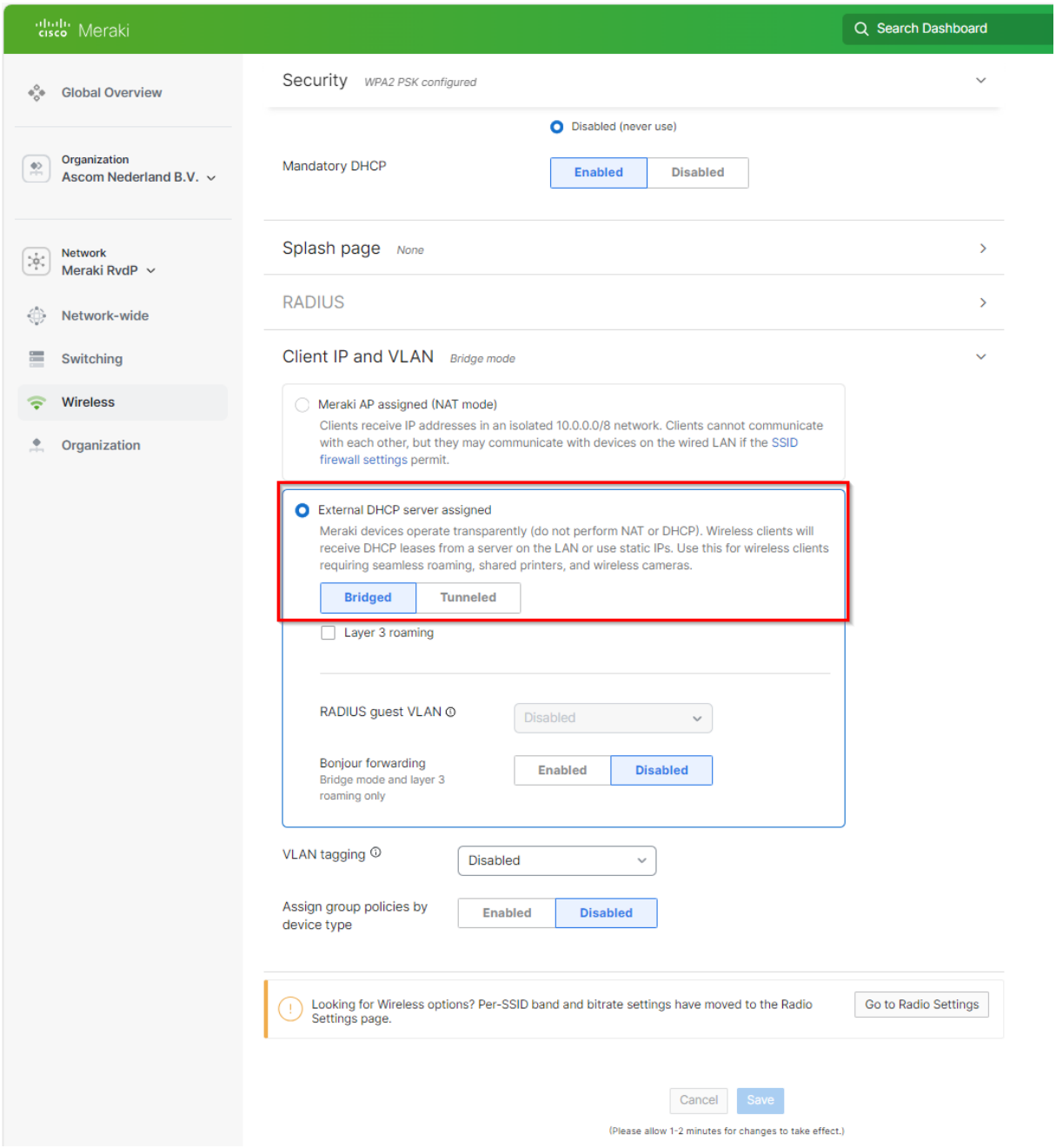
Wireless > SSIDs

WPA2 PSK (Personal)



Wireless > Configure > Access Control

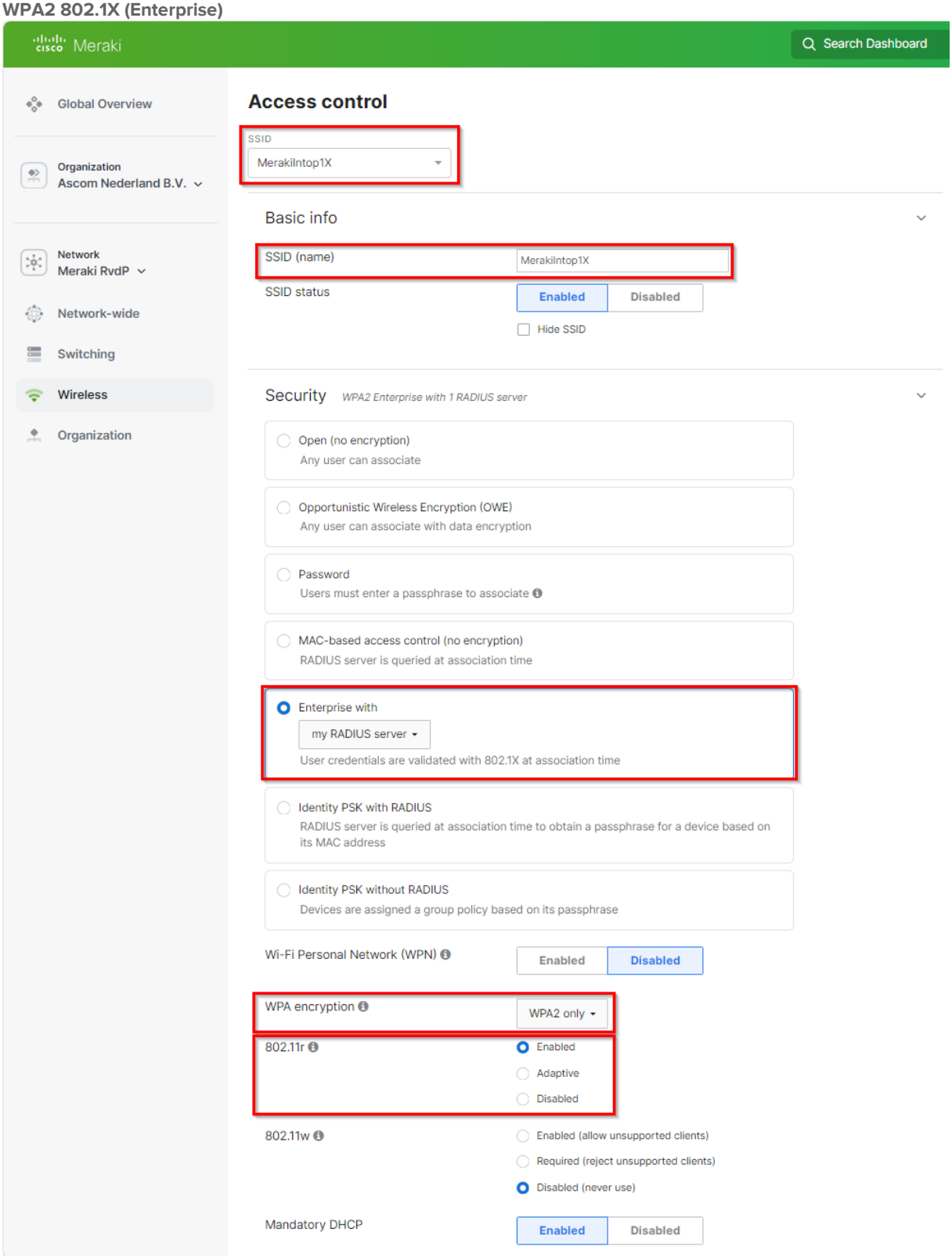
- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security Select Password and enter WPA2 Pre-shared Key (PSK)
- Remember to enable SSID.



Wireless > Configure > Access Control (step 2)

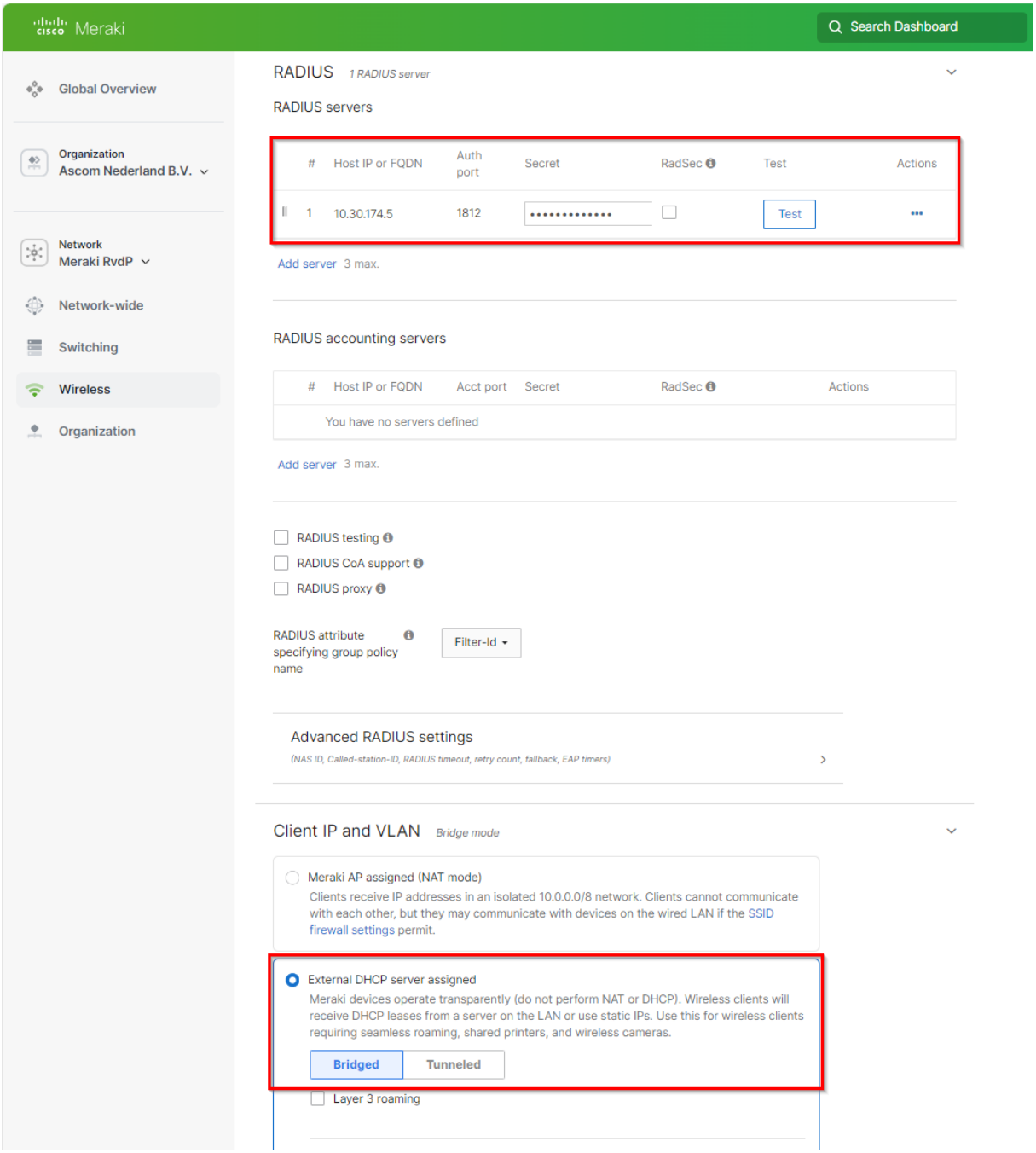
- Select External DHCP server and Bridge Mode, should clients need to receive leases from a DHCP server on the LAN.

WPA2 802.1X (Enterprise)



Wireless > Configure > Access Control

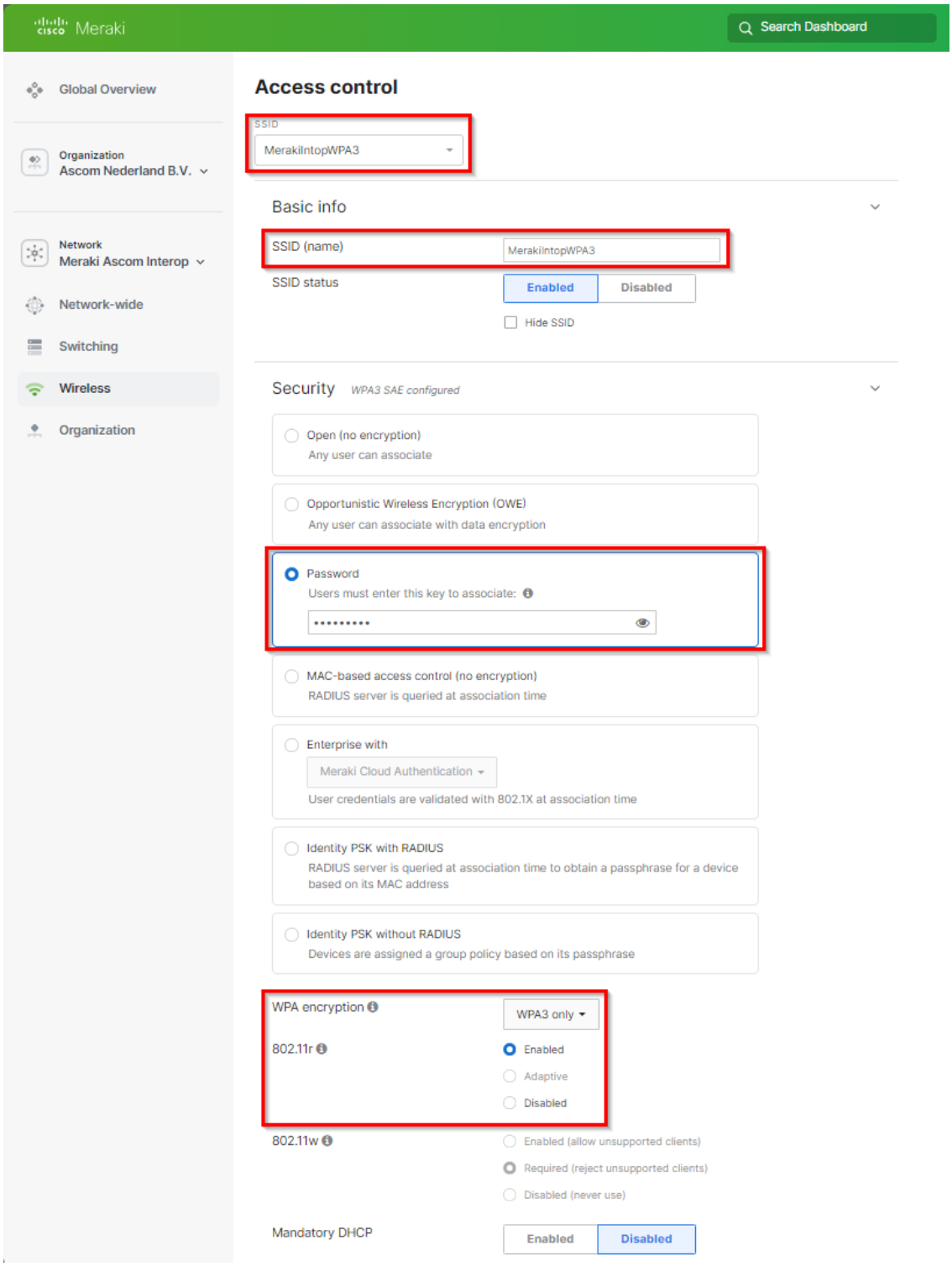
- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security Select “Enterprise with” and select “my RADIUS server” (unless the internal server is used)
- Remember to enable SSID.



Wireless > Configure > Access Control (step 2)

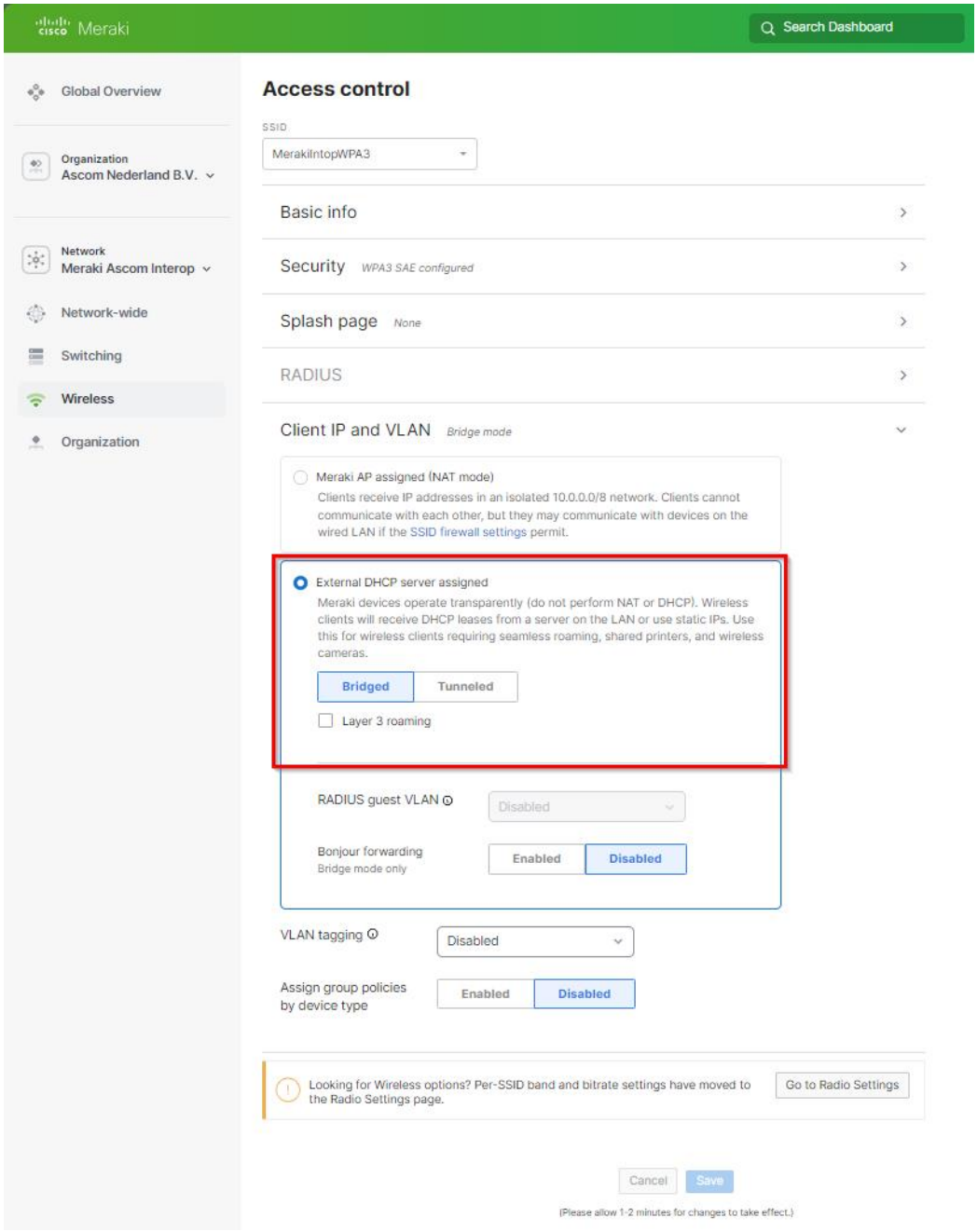
- Define a RADIUS server
- Select External DHCP server and Bridge Mode, should clients need to receive leases from a DHCP server on the LAN.

WPA3 PSK (Personal)



Wireless > Configure > Access Control

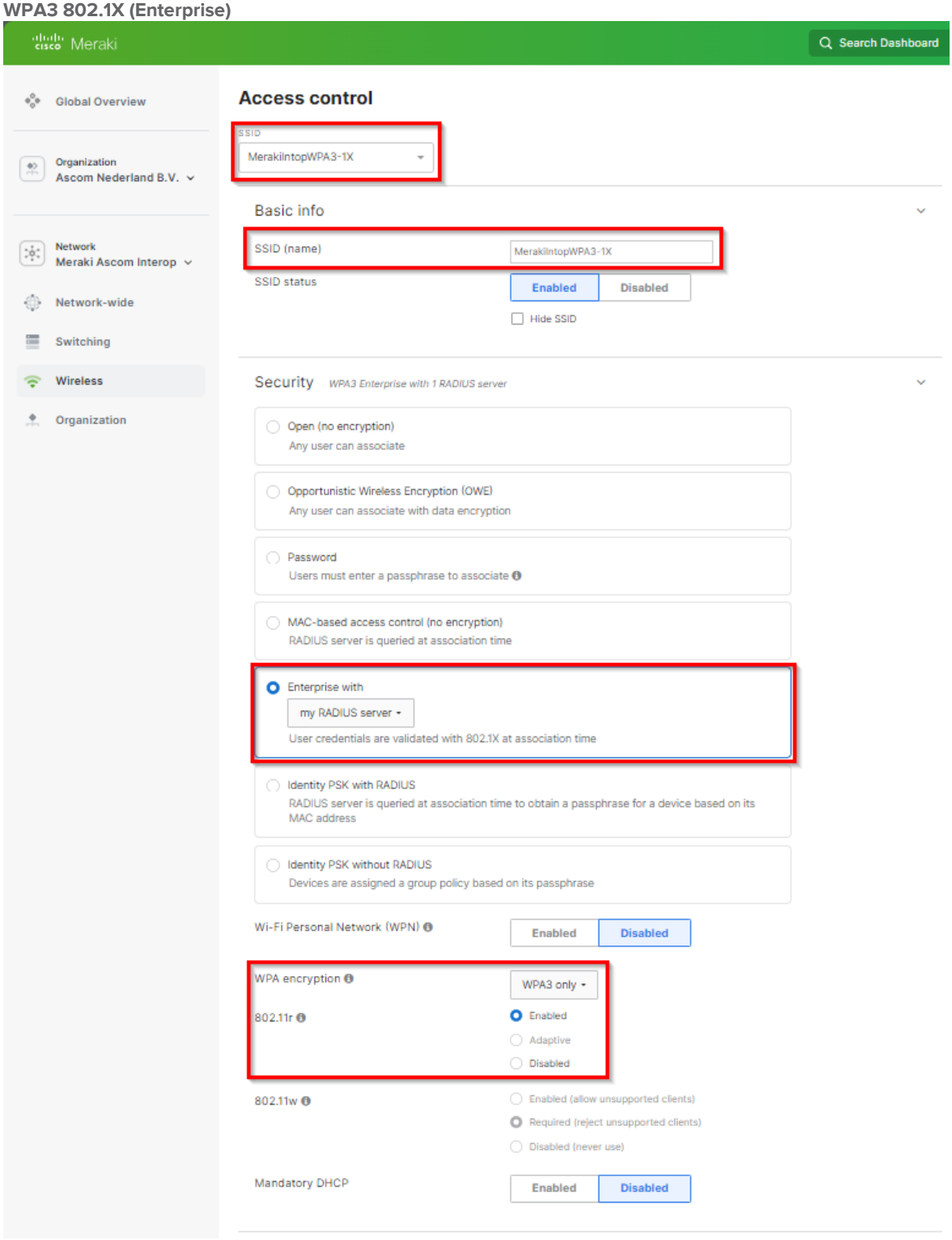
- Select SSID from the drop-down
- Enter the SSID (name)
- Under Security select Password and enter a password.
- Select WPA3 only as WPA encryption method
- Select Enabled for 802.11r to enable Fast Transition.
- Remember to enable SSID.



Wireless > Configure > Access Control (step 2)

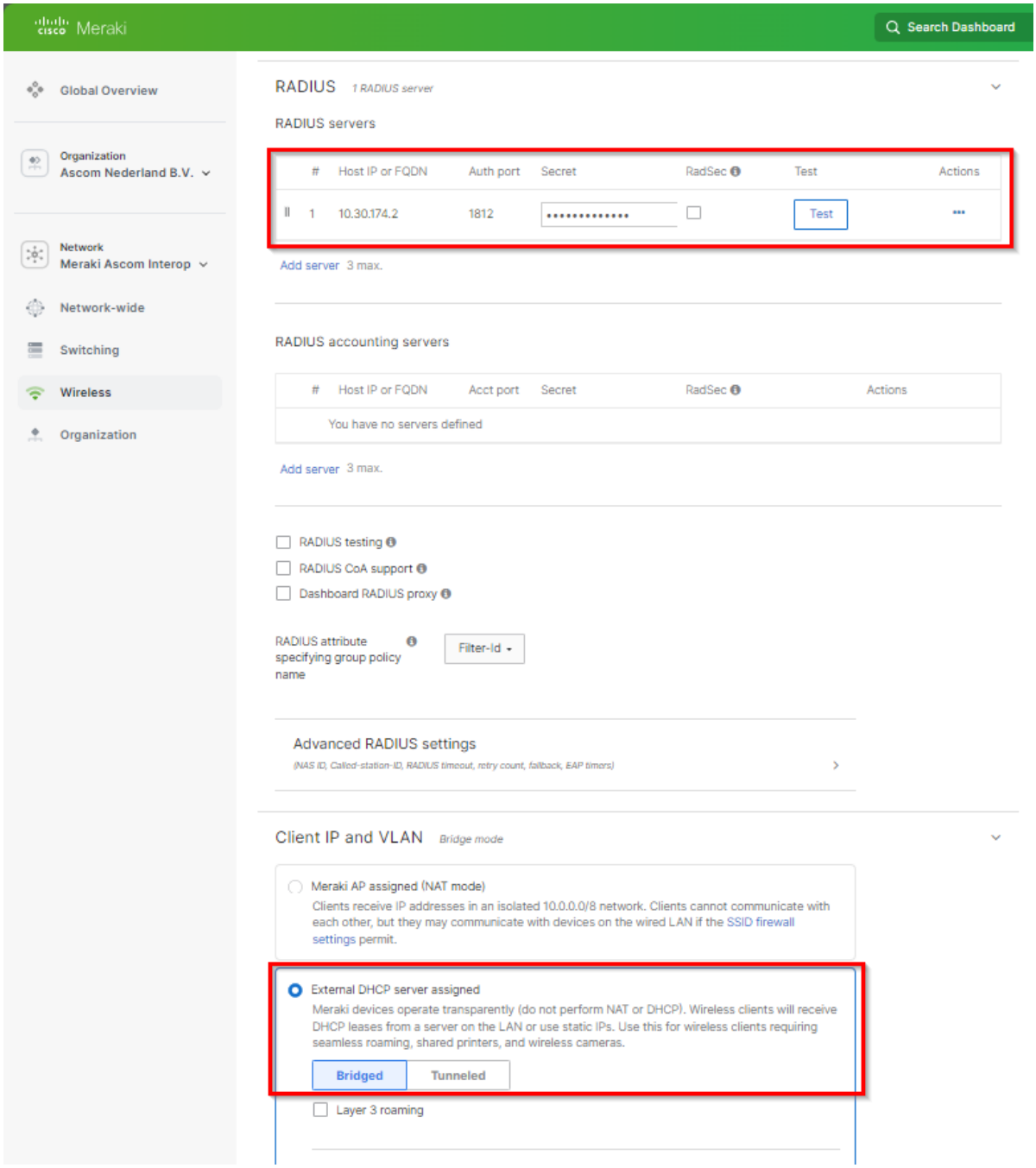
- Select External DHCP server and Bridge Mode, should clients need to receive leases from a DHCP server on the LAN.

WPA3 802.1X (Enterprise)



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.

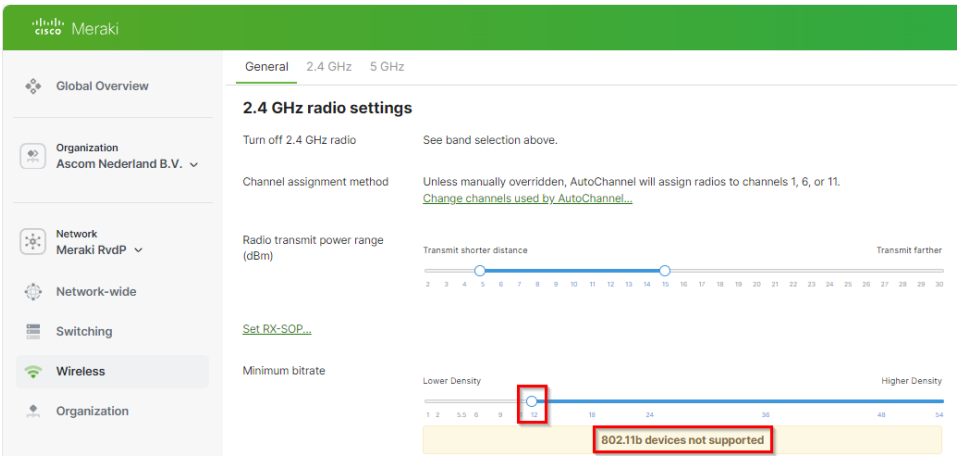


Wireless > Configure > Access Control (step 2)

- 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

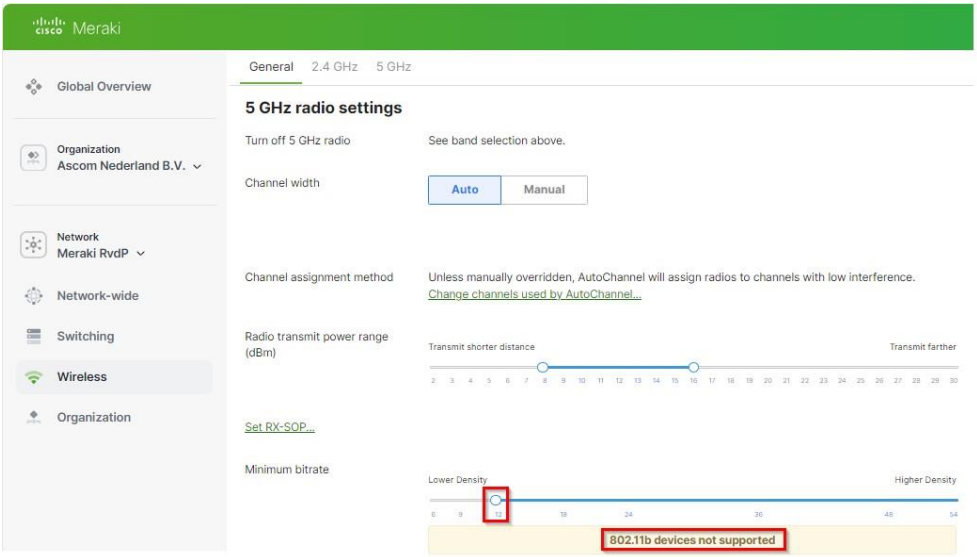
2.4Ghz radio settings



Wireless > Radio settings > RF profiles > Basic Indoor Profile

- Select Minimum bitrate: 12 Mbps

5Ghz radio settings



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.

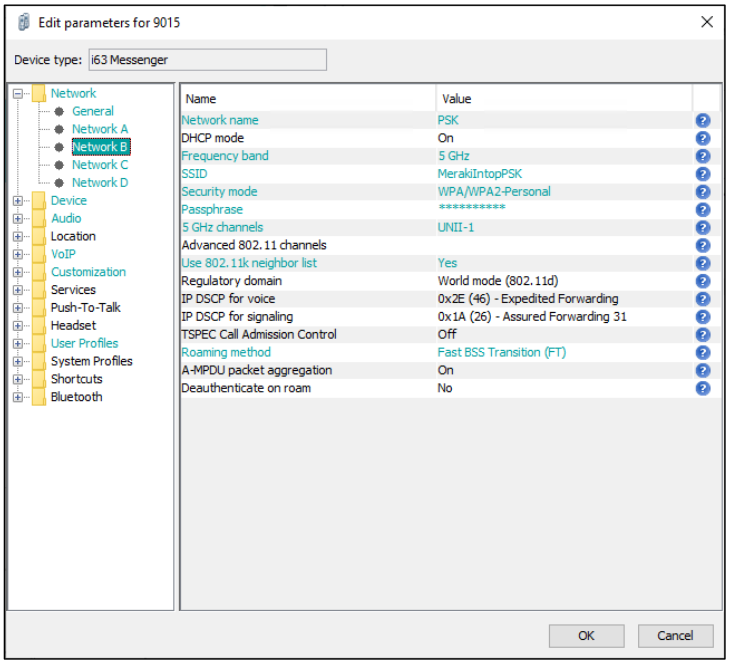
General guidelines when deploying Ascom i63 handsets in 802.11a/n/ac/ax environments:

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

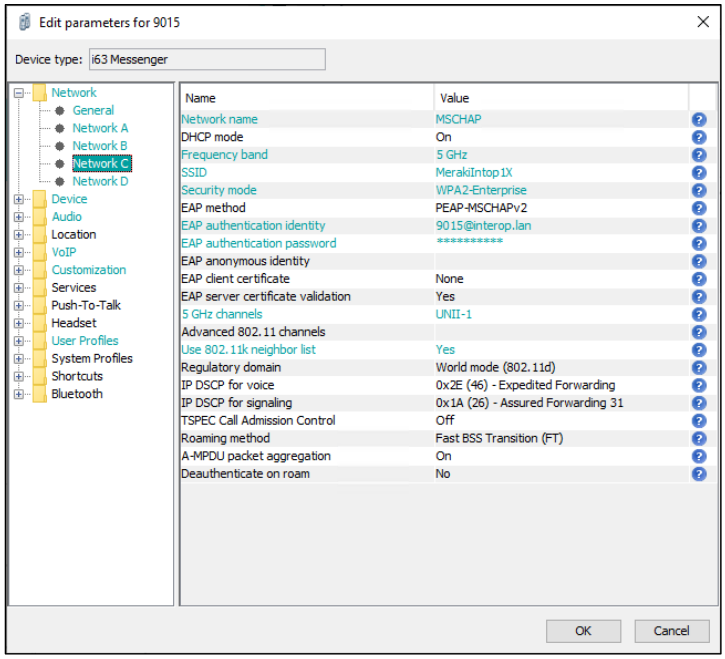


Network settings for WPA2-Personal

- 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”.

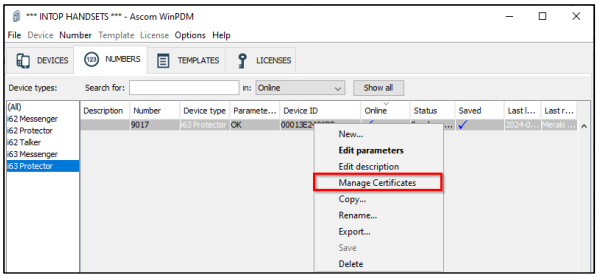
WPA2-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



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

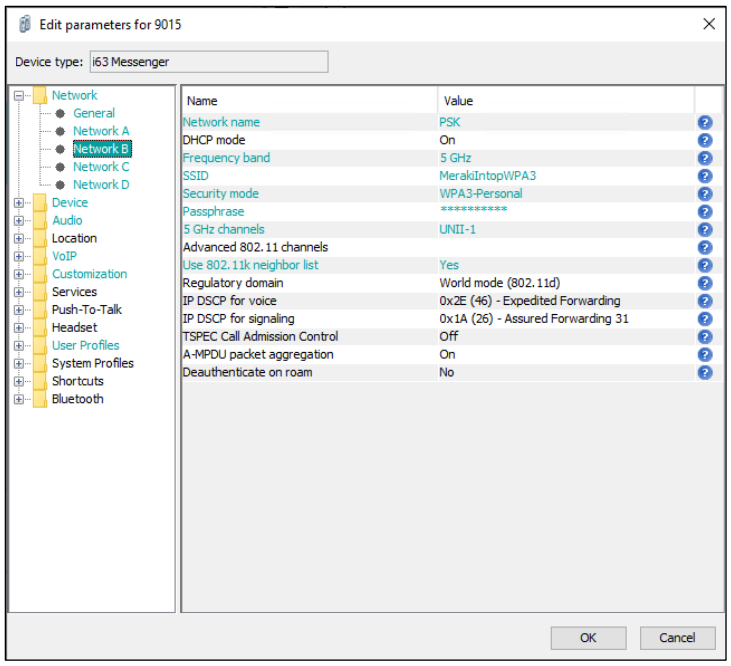
NOTE: The FCC no longer allows 802.11d to determine the regulatory domain. Accordingly, devices deployed in the United States must have the “Regulatory domain” set to “USA”.



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

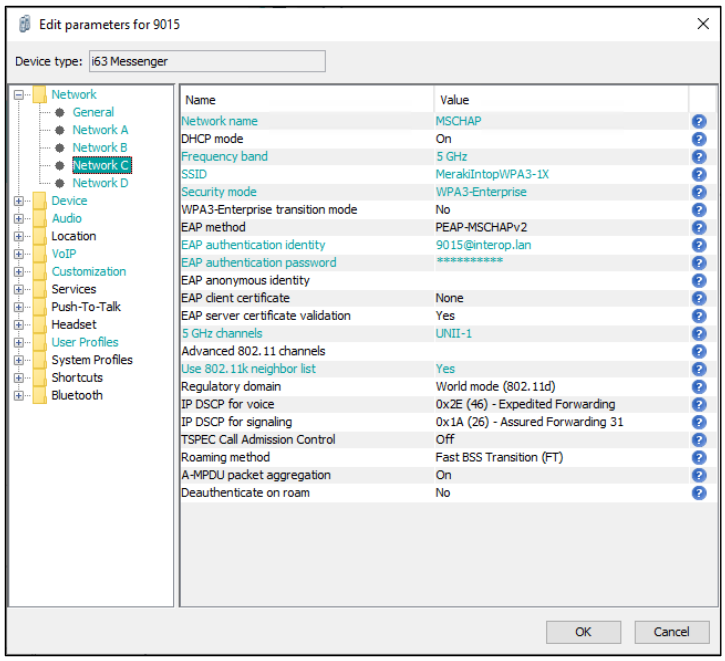


Network settings for WPA3-Personal

- 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”.

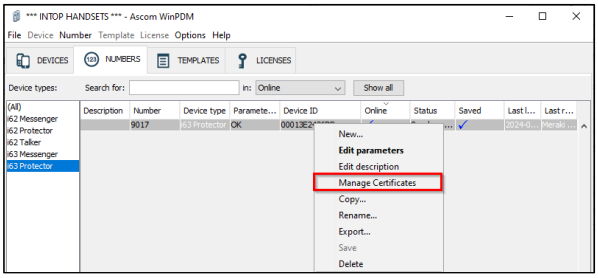
WPA3-Enterprise (802.1X Authentication PEAP-MSCHAPv2)



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