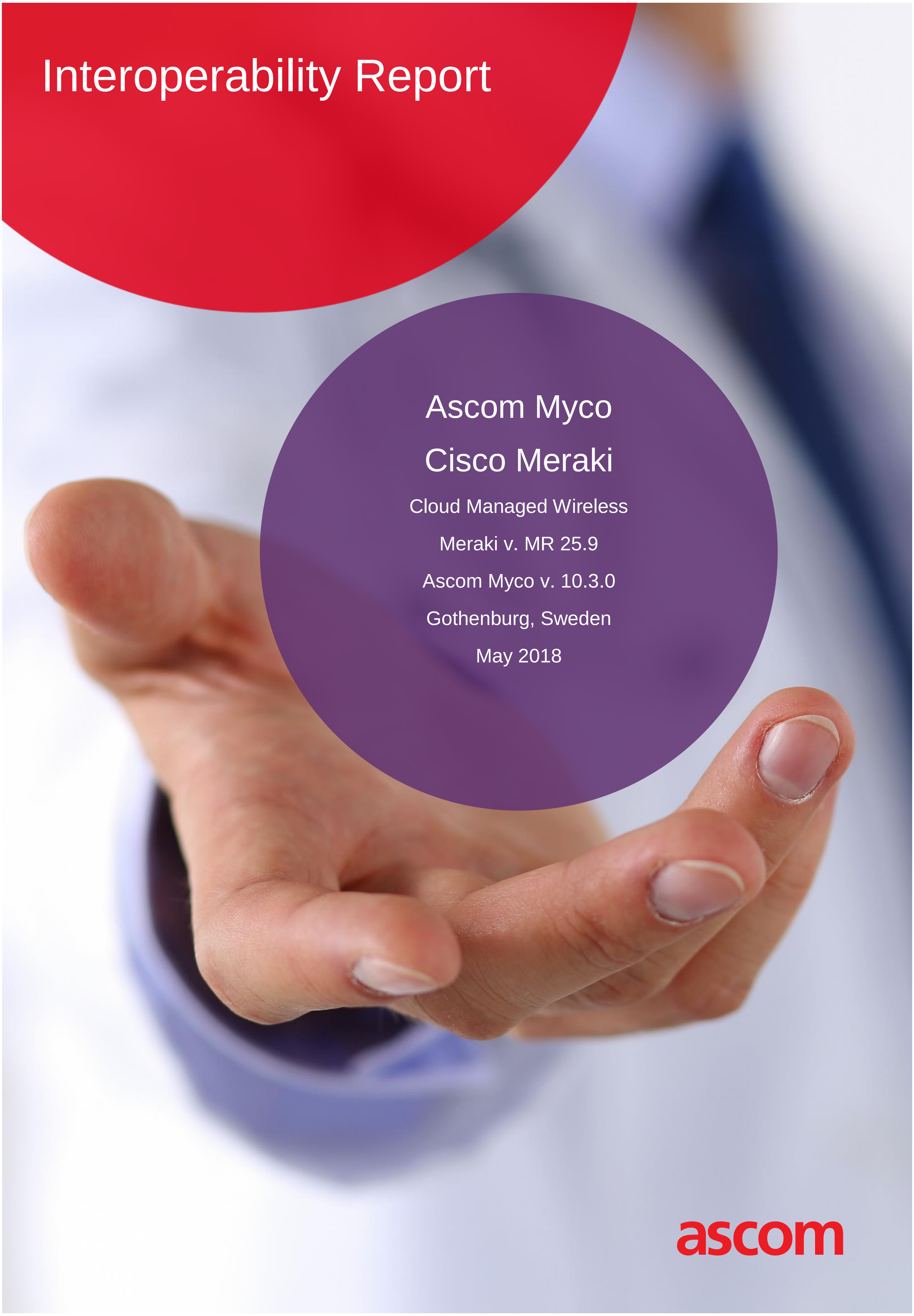


Interoperability Report

Ascom Myco

Cisco Meraki

Cloud Managed Wireless

Meraki v. MR 25.9

Ascom Myco v. 10.3.0

Gothenburg, Sweden

May 2018

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

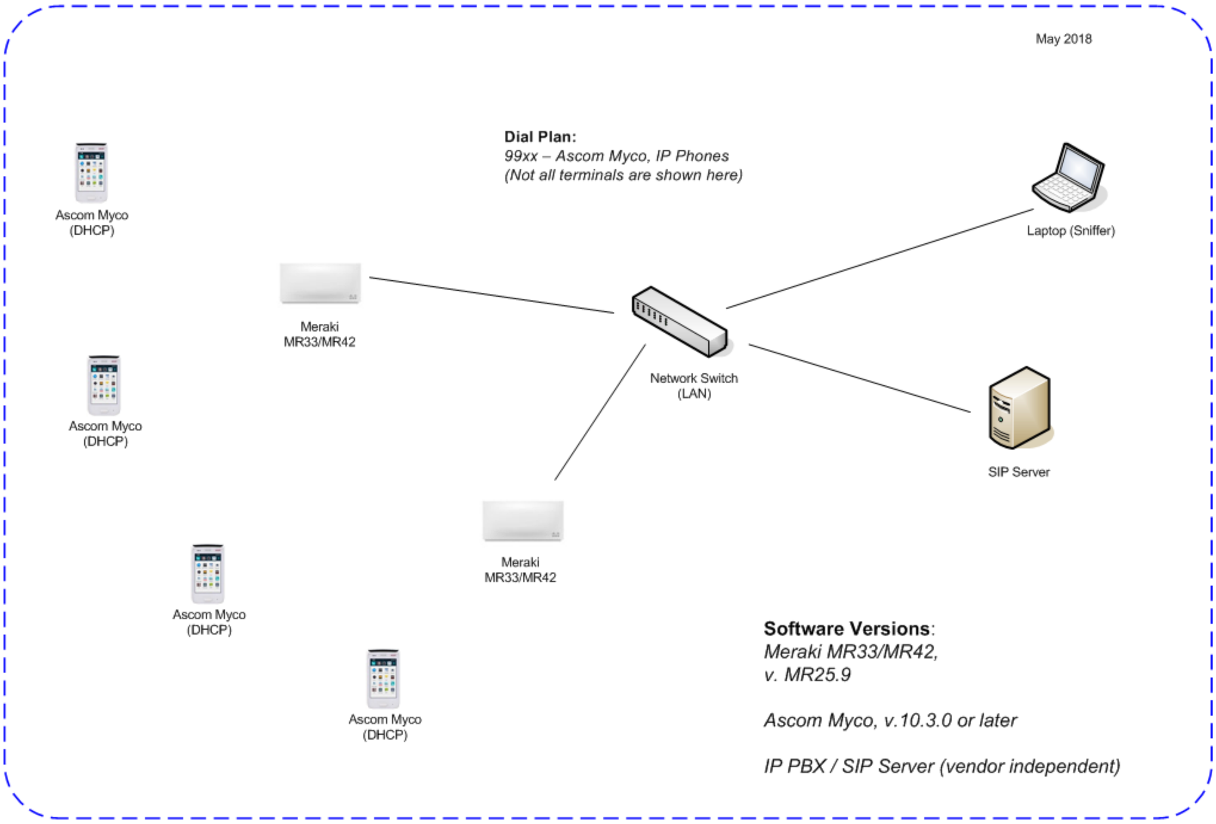
Interoperability Verification Site

Ascom,
Gothenburg,
Sweden

Participants

Matthew Williams, Ascom, Gothenburg

Test Topology



May 2018

Dial Plan:
99xx – Ascom Myco, IP Phones
(Not all terminals are shown here)

Software Versions:
Meraki MR33/MR42,
v. MR25.9

Ascom Myco, v.10.3.0 or later

IP PBX / SIP Server (vendor independent)

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 Myco 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 Myco, version 10.3.0
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 requires 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 Myco in idle mode (observed standby time with Ascom Myco 2: >40 hours (avg.)).	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.

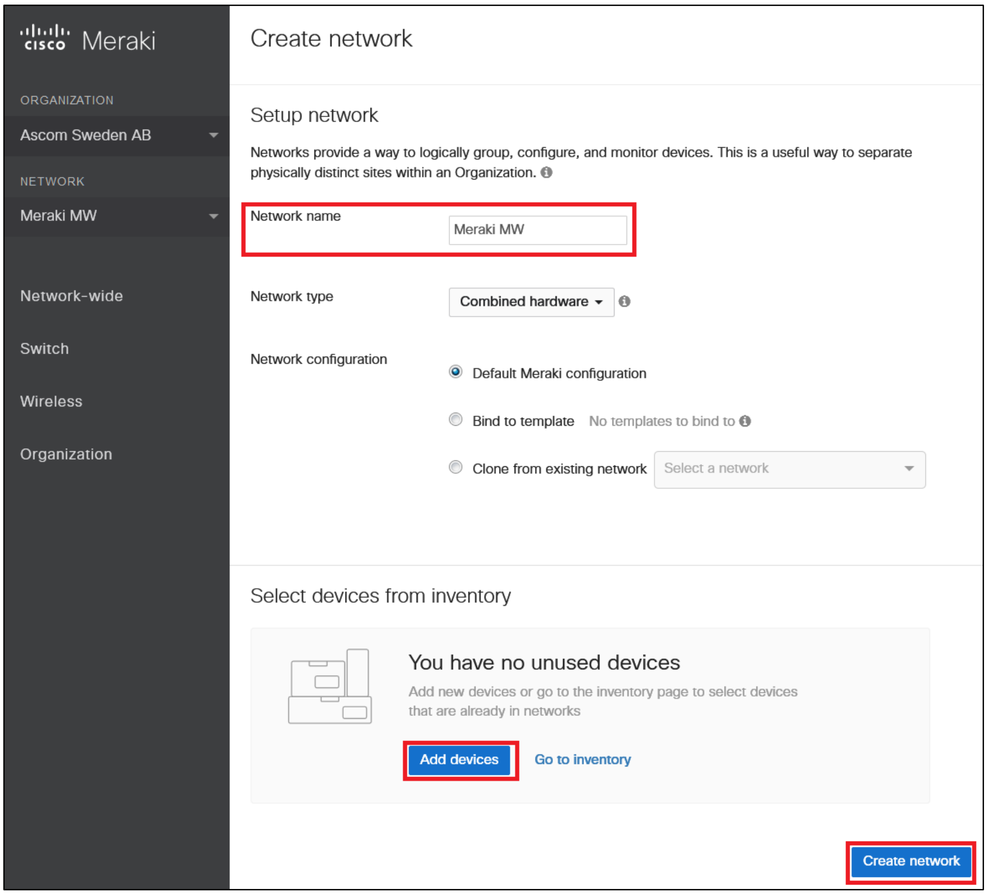
Appendix A: Interoperability Verification Configurations

Meraki MR33/MR42, v. MR 25.9

This section includes screenshots and explanations of basic settings required to use Ascom Myco 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)



Create network

Setup network

Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization.

Network name: Meraki MW

Network type: Combined hardware

Network configuration:
- ● Default Meraki configuration
- ○ Bind to template   No templates to bind to
- ○ Clone from existing network   Select a network

Select devices from inventory

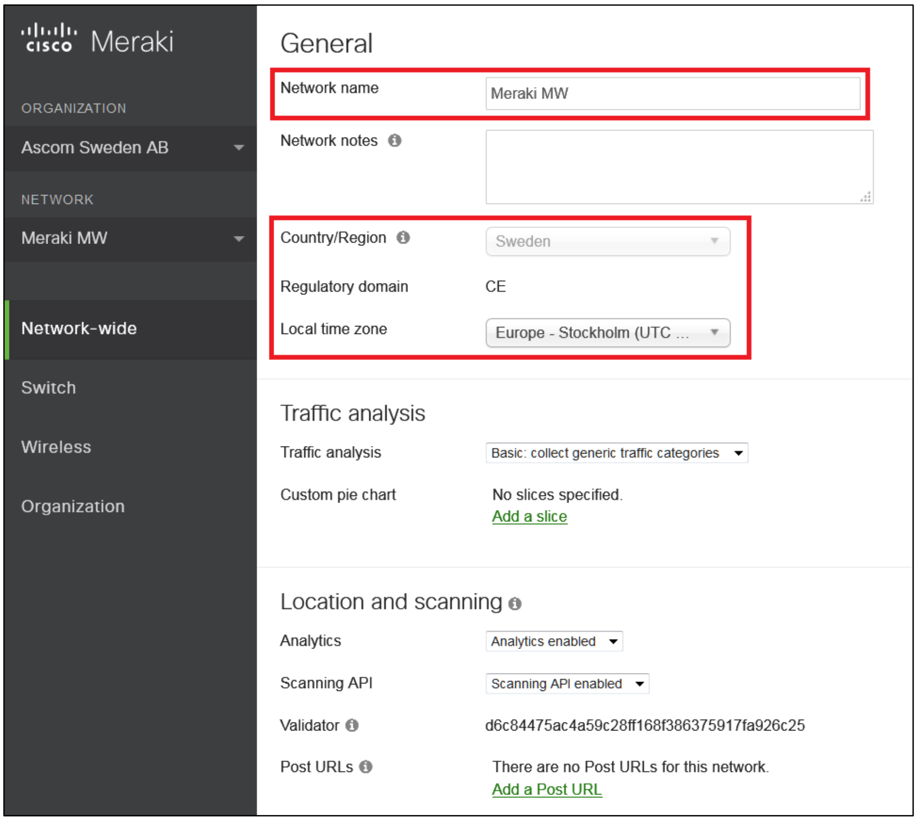
You have no unused devices

Add new devices or go to the inventory page to select devices that are already in networks

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.



General

Network name	Meraki MW
Network notes	
Country/Region	Sweden
Regulatory domain	CE
Local time zone	Europe - Stockholm (UTC ...

Traffic analysis

Traffic analysis	Basic: collect generic traffic categories
Custom pie chart	No slices specified. Add a slice

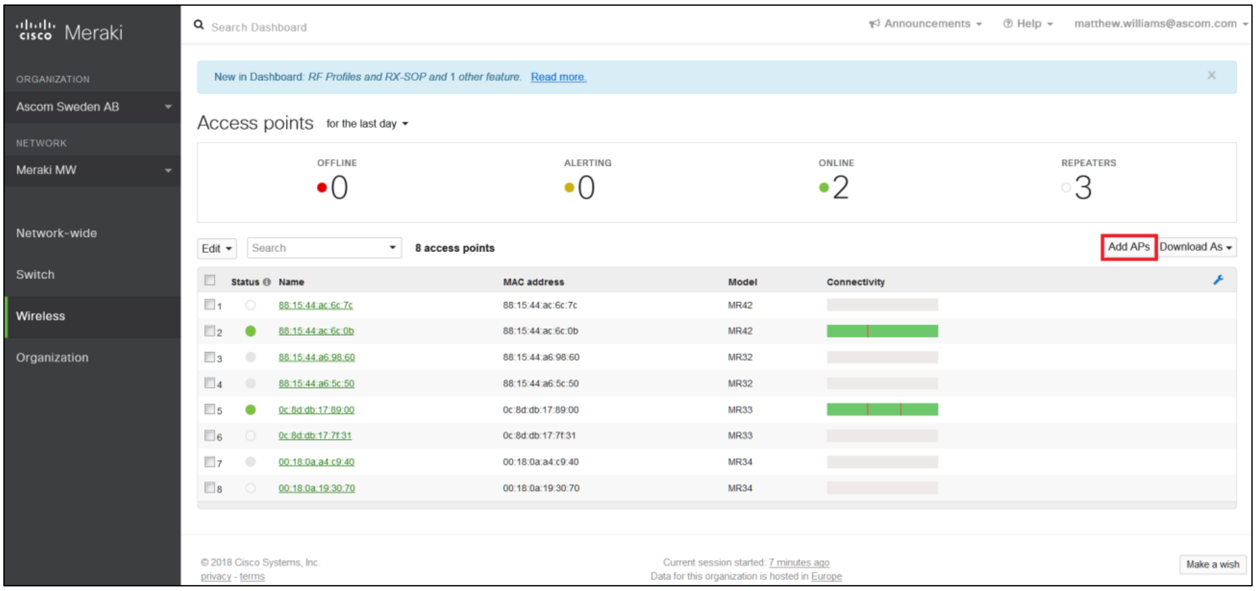
Location and scanning

Analytics	Analytics enabled
Scanning API	Scanning API enabled
Validator	d6c84475ac4a59c28ff168f386375917fa926c25
Post URLs	There are no Post URLs for this network. Add a Post URL

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.



New in Dashboard: *RF Profiles and RX-SOP and 1 other feature.* Read more.

Access points for the last day

OFFLINE	ALERTING	ONLINE	REPEATERS
0	0	2	3

8 access points

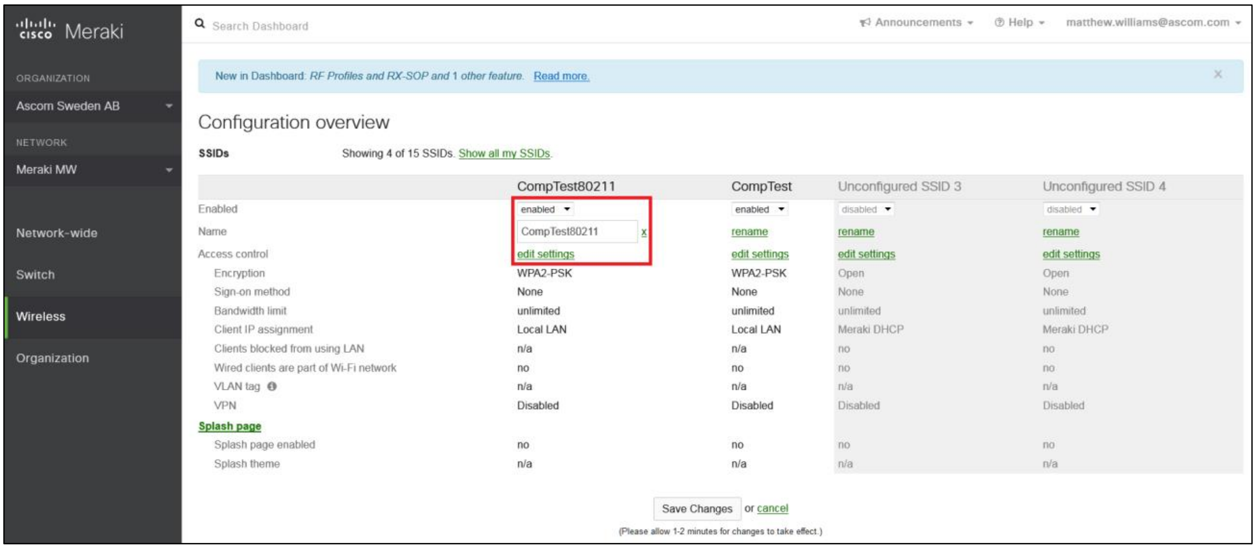
	Status	Name	MAC address	Model	Connectivity
□ 1	○	88:15:44:ac:6c:7c	88:15:44:ac:6c:7c	MR42	
□ 2	●	88:15:44:ac:6c:0b	88:15:44:ac:6c:0b	MR42	🟩
□ 3	●	88:15:44:a6:98:60	88:15:44:a6:98:60	MR32	
□ 4	●	88:15:44:a6:5c:50	88:15:44:a6:5c:50	MR32	
□ 5	●	0c:8d:db:17:89:00	0c:8d:db:17:89:00	MR33	🟩
□ 6	○	0c:8d:db:17:7f:31	0c:8d:db:17:7f:31	MR33	
□ 7	●	00:18:0a:a4:c9:40	00:18:0a:a4:c9:40	MR34	
□ 8	○	00:18:0a:19:30:70	00:18:0a:19:30:70	MR34	

© 2018 Cisco Systems, Inc.
privacy - terms

Current session started: 7 minutes ago
Data for this organization is hosted in Europe

Wireless > Monitor > Access Points

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



New in Dashboard: *RF Profiles and RX-SOP and 1 other feature.* Read more.

Configuration overview

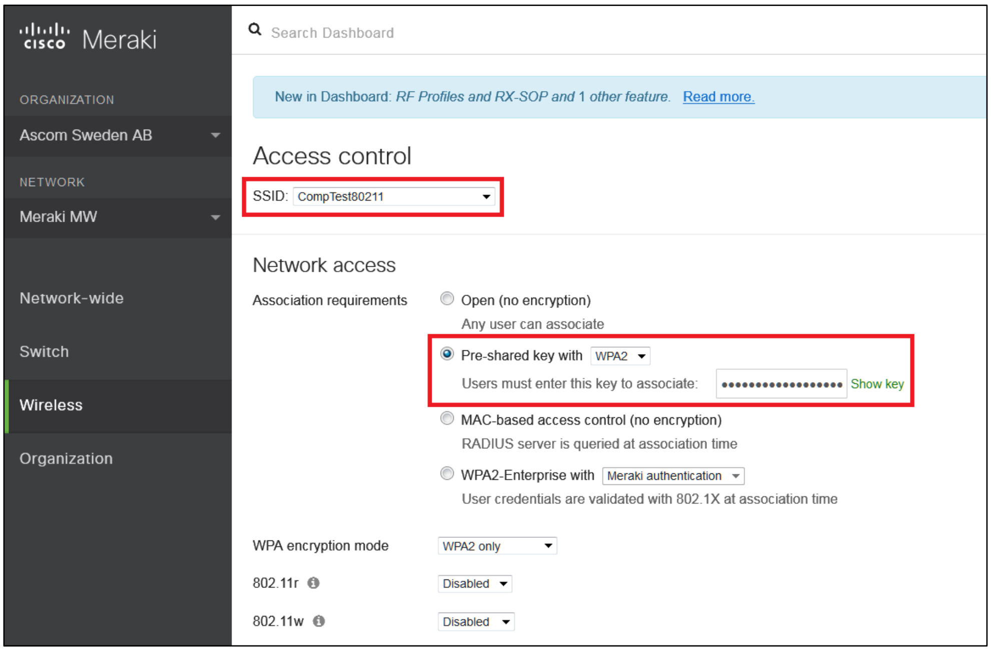
SSIDs Showing 4 of 15 SSIDs. Show all my SSIDs.

	CompTest80211	CompTest	Unconfigured SSID 3	Unconfigured SSID 4
Enabled	enabled	enabled	disabled	disabled
Name	CompTest80211 x	rename	rename	rename
Access control	edit settings	edit settings	edit settings	edit settings
Encryption	WPA2-PSK	WPA2-PSK	Open	Open
Sign-on method	None	None	None	None
Bandwidth limit	unlimited	unlimited	unlimited	unlimited
Client IP assignment	Local LAN	Local LAN	Meraki DHCP	Meraki DHCP
Clients blocked from using LAN	n/a	n/a	no	no
Wired clients are part of Wi-Fi network	no	no	no	no
VLAN tag	n/a	n/a	n/a	n/a
VPN	Disabled	Disabled	Disabled	Disabled
Splash page				
Splash page enabled	no	no	no	no
Splash theme	n/a	n/a	n/a	n/a

(Please allow 1-2 minutes for changes to take effect.)

Wireless > Configure > SSID

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



New in Dashboard: *RF Profiles and RX-SOP and 1 other feature.* Read more.

Access control

SSID: CompTest80211

Network access

Association requirements

○ Open (no encryption)
Any user can associate

● Pre-shared key with WPA2
Users must enter this key to associate: ••••••••••••••••••

○ MAC-based access control (no encryption)
RADIUS server is queried at association time

○ WPA2-Enterprise with Meraki authentication
User credentials are validated with 802.1X at association time

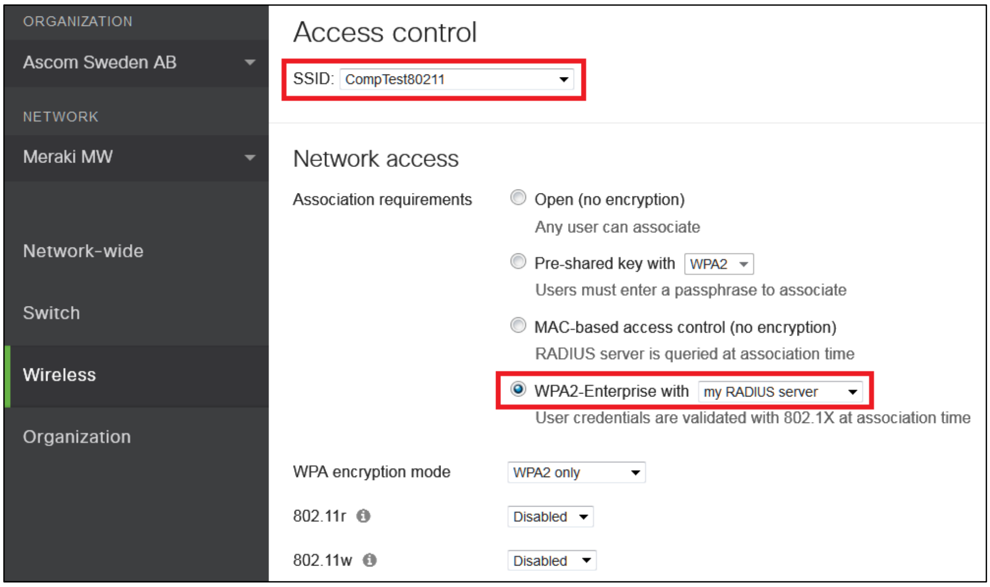
WPA encryption mode: WPA2 only

802.11r: Disabled

802.11w: Disabled

Wireless > Configure > Access Control (WPA2-PSK)

- Select SSID
- Enter WPA2 Pre-shared Key



Access control

SSID: CompTest80211

Network access

Association requirements

○ Open (no encryption)
Any user can associate

○ Pre-shared key with WPA2
Users must enter a passphrase to associate

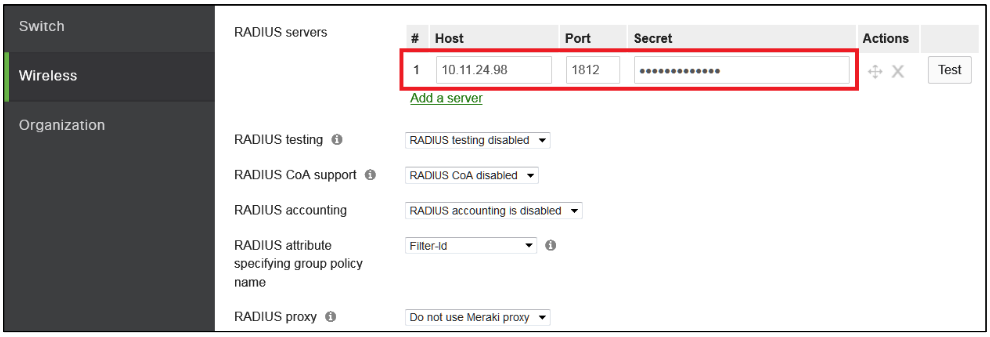
○ MAC-based access control (no encryption)
RADIUS server is queried at association time

● WPA2-Enterprise with my RADIUS server
User credentials are validated with 802.1X at association time

WPA encryption mode: WPA2 only

802.11r: Disabled

802.11w: Disabled



RADIUS servers

#	Host	Port	Secret	Actions
1	10.11.24.98	1812	•••••••••••••	

RADIUS testing: RADIUS testing disabled

RADIUS CoA support: RADIUS CoA disabled

RADIUS accounting: RADIUS accounting is disabled

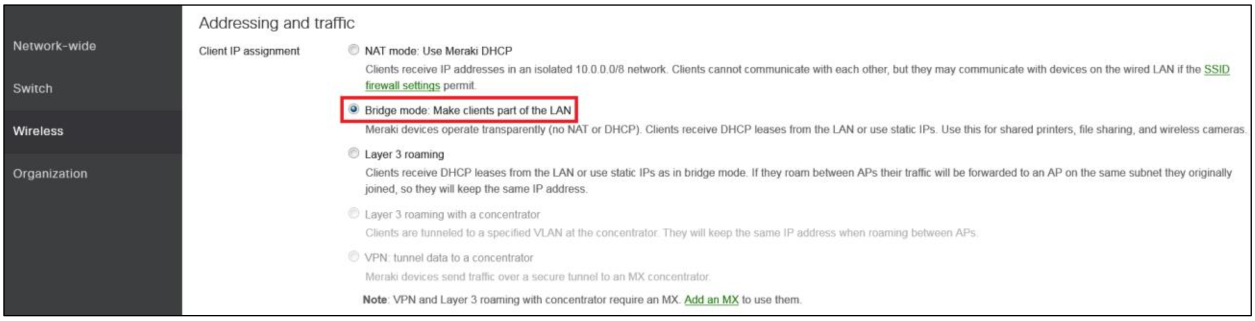
RADIUS attribute specifying group policy name: Filter-Id

RADIUS proxy: Do not use Meraki proxy

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).



Addressing and traffic

Client IP assignment

○ NAT mode: Use Meraki DHCP

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.

● Bridge mode: Make clients part of the LAN

Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.

○ Layer 3 roaming

Clients receive DHCP leases from the LAN or use static IPs as in bridge mode. If they roam between APs their traffic will be forwarded to an AP on the same subnet they originally joined, so they will keep the same IP address.

○ Layer 3 roaming with a concentrator

Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.

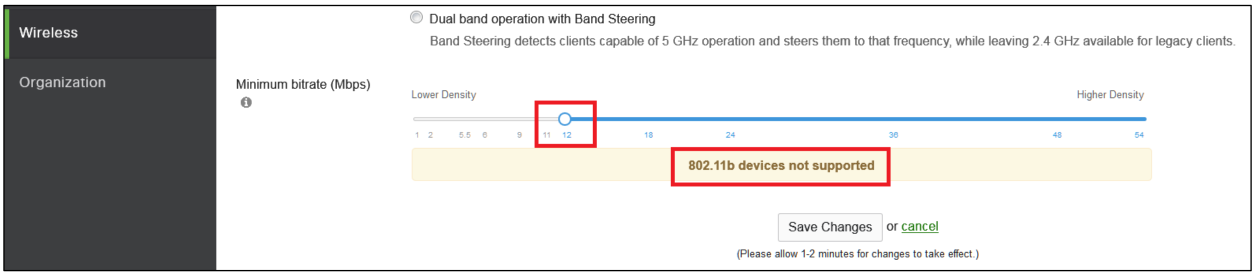
○ VPN: tunnel data to a concentrator

Meraki devices send traffic over a secure tunnel to an MX concentrator.

Note: VPN and Layer 3 roaming with concentrator require an MX. Add an MX to use them.

Wireless > Configure > Access Control (step 2)

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



○ Dual band operation with Band Steering

Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

Minimum bitrate (Mbps)

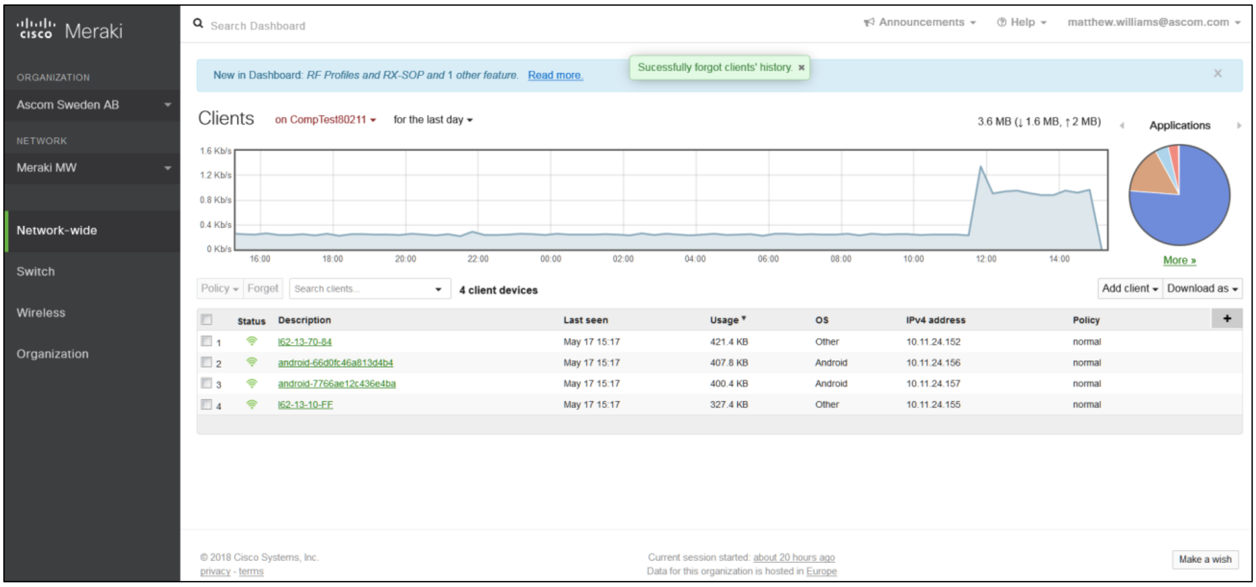
802.11b devices not supported

(Please allow 1-2 minutes for changes to take effect.)

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.



New in Dashboard: *RF Profiles and RX-SOP and 1 other feature.* Read more.

Sucessfully forgot clients' history.

Clients on CompTest80211 for the last day

3.6 MB (↓1.6 MB, ↑2 MB)

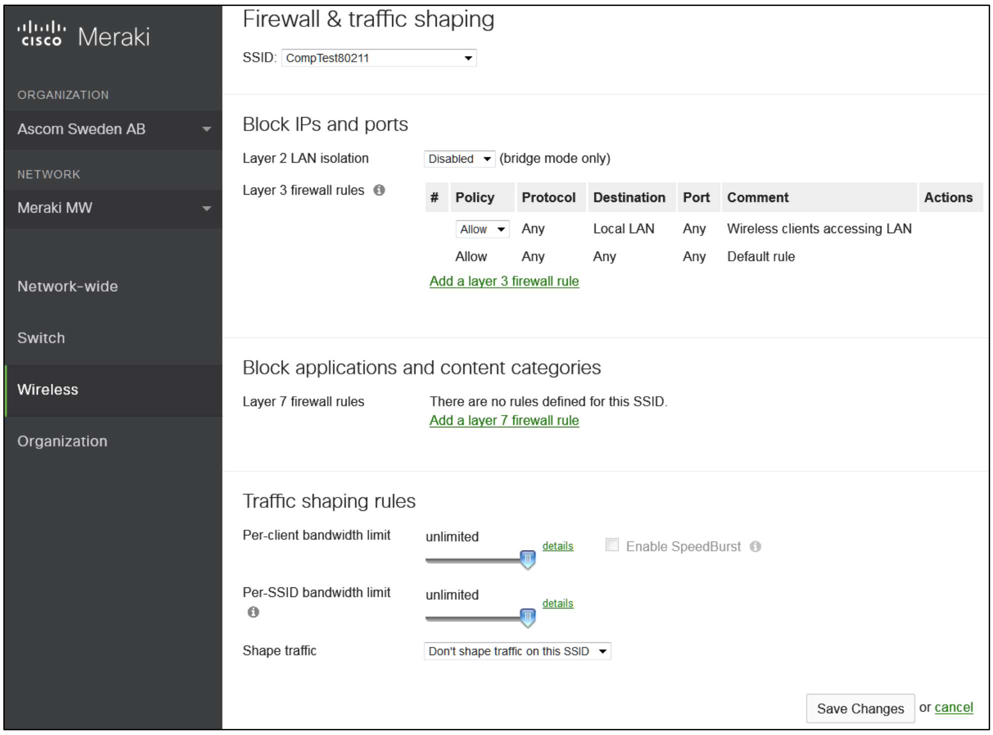
4 client devices

	Status	Description	Last seen	Usage	OS	IPv4 address	Policy
□ 1	ᯤ	l62-13-70-84	May 17 15:17	421.4 KB	Other	10.11.24.152	normal
□ 2	ᯤ	android-66d0fc46a813d4b4	May 17 15:17	407.8 KB	Android	10.11.24.156	normal
□ 3	ᯤ	android-7766ae12c436e4ba	May 17 15:17	400.4 KB	Android	10.11.24.157	normal
□ 4	ᯤ	l62-13-10-FF	May 17 15:17	327.4 KB	Other	10.11.24.155	normal

© 2018 Cisco Systems, Inc.
privacy - terms

Current session started: about 20 hours ago
Data for this organization is hosted in Europe

SSID Overview (Network-Wide > Monitor > Clients)



Firewall & traffic shaping

SSID: CompTest80211

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
	Allow	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Add a layer 3 firewall rule

Block applications and content categories

Layer 7 firewall rules: There are no rules defined for this SSID.
Add a layer 7 firewall rule

Traffic shaping rules

Per-client bandwidth limit: unlimited details □ Enable SpeedBurst

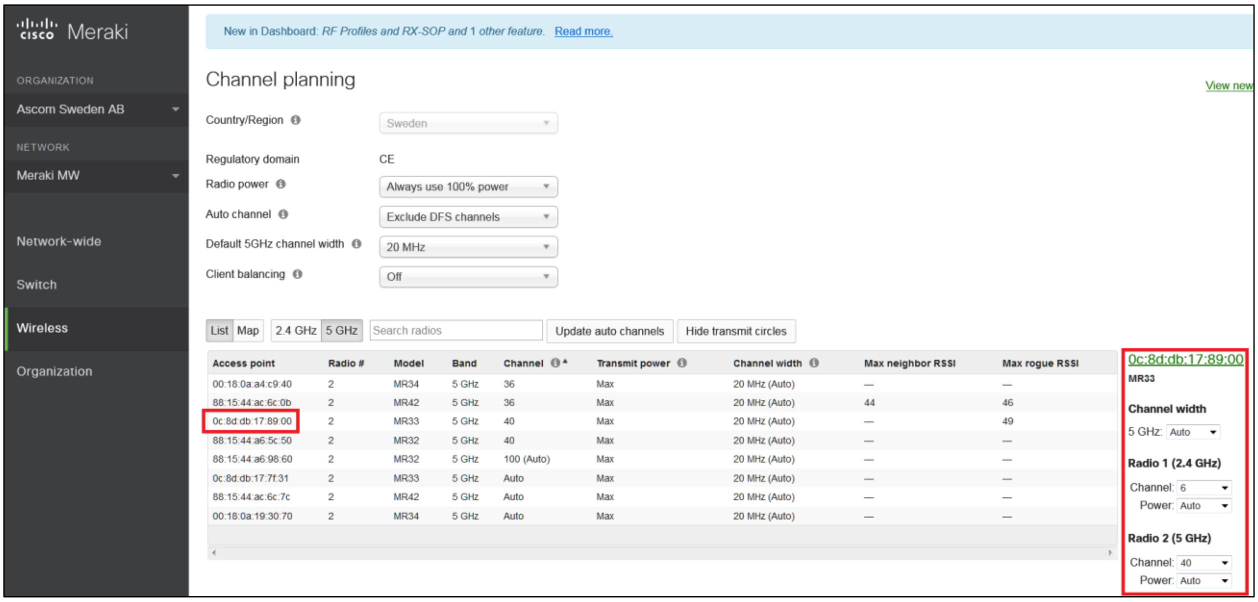
Per-SSID bandwidth limit: unlimited details

Shape traffic: Don't shape traffic on this SSID

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

- No need to modify (included as reference)

NOTE: DSCP values cannot be changed on the Myco.



New in Dashboard: *RF Profiles and RX-SOP and 1 other feature.* Read more.

Channel planning

Country/Region	Sweden
Regulatory domain	CE
Radio power	Always use 100% power
Auto channel	Exclude DFS channels
Default 5GHz channel width	20 MHz
Client balancing	Off

Access point	Radio #	Model	Band	Channel	Transmit power	Channel width	Max neighbor RSSI	Max rogue RSSI
00:18:0a:a4:c9:40	2	MR34	5 GHz	36	Max	20 MHz (Auto)	—	—
88:15:44:ac:6c:0b	2	MR42	5 GHz	36	Max	20 MHz (Auto)	44	46
0c:8d:db:17:89:00	2	MR33	5 GHz	40	Max	20 MHz (Auto)	—	49
88:15:44:a6:5c:50	2	MR32	5 GHz	40	Max	20 MHz (Auto)	—	—
88:15:44:a6:98:60	2	MR32	5 GHz	100 (Auto)	Max	20 MHz (Auto)	—	—
0c:8d:db:17:7f:31	2	MR33	5 GHz	Auto	Max	20 MHz (Auto)	—	—
88:15:44:ac:6c:7c	2	MR42	5 GHz	Auto	Max	20 MHz (Auto)	—	—
00:18:0a:19:30:70	2	MR34	5 GHz	Auto	Max	20 MHz (Auto)	—	—

0c:8d:db:17:89:00
MR33

Channel width
5 GHz: Auto

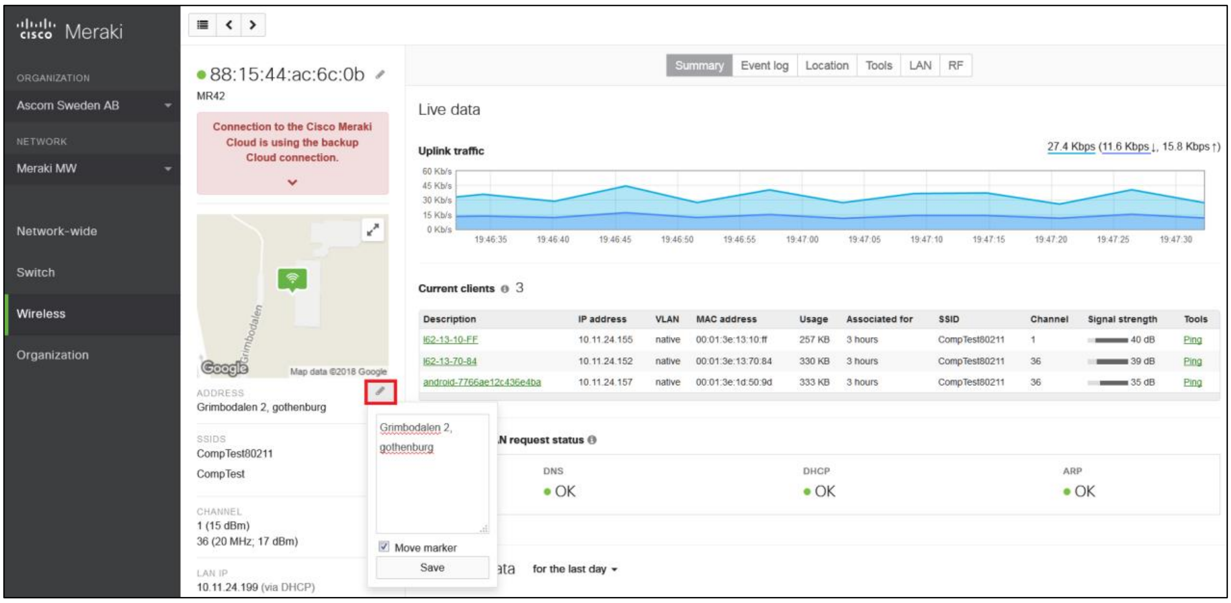
Radio 1 (2.4 GHz)
Channel: 6
Power: Auto

Radio 2 (5 GHz)
Channel: 40
Power: Auto

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.



88:15:44:ac:6c:0b
MR42

Connection to the Cisco Meraki Cloud is using the backup Cloud connection.

ADDRESS
Grimbodalen 2, gothenburg

Grimbodalen 2,
gothenburg

☑ Move marker
Save

SSIDS
CompTest80211
CompTest

CHANNEL
1 (15 dBm)
36 (20 MHz; 17 dBm)

LAN IP
10.11.24.199 (via DHCP)

Live data

Uplink traffic 27.4 Kbps (11.6 Kbps ↓, 15.8 Kbps ↑)

Current clients 3

Description	IP address	VLAN	MAC address	Usage	Associated for	SSID	Channel	Signal strength	Tools
I62-13-10-FF	10.11.24.155	native	00:01:3e:13:10:ff	257 KB	3 hours	CompTest80211	1	40 dB	Ping
I62-13-70-84	10.11.24.152	native	00:01:3e:13:70:84	330 KB	3 hours	CompTest80211	36	39 dB	Ping
android-7766ae12c436e4ba	10.11.24.157	native	00:01:3e:1d:50:9d	333 KB	3 hours	CompTest80211	36	35 dB	Ping

N request status

DNS	DHCP	ARP
● OK	● OK	● OK

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 Myco 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.***

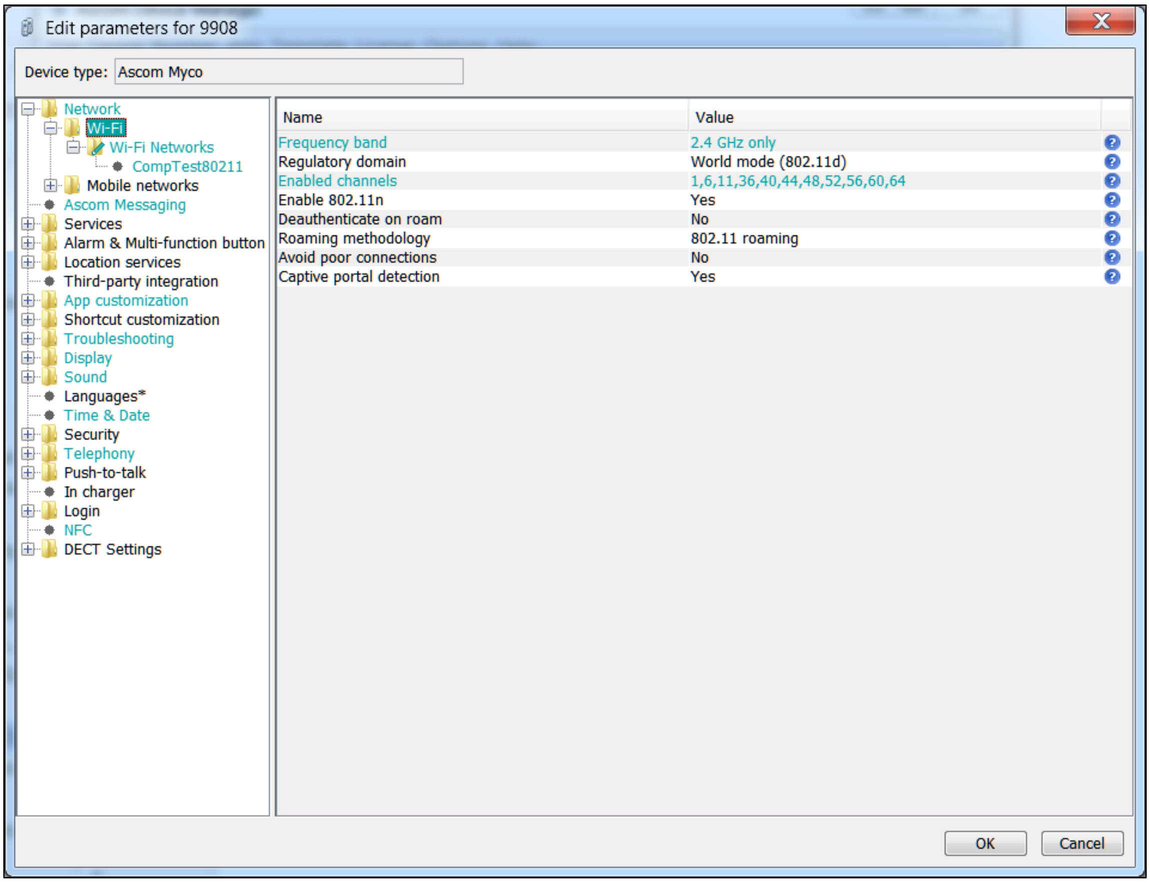
3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***

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 Myco Settings Summary

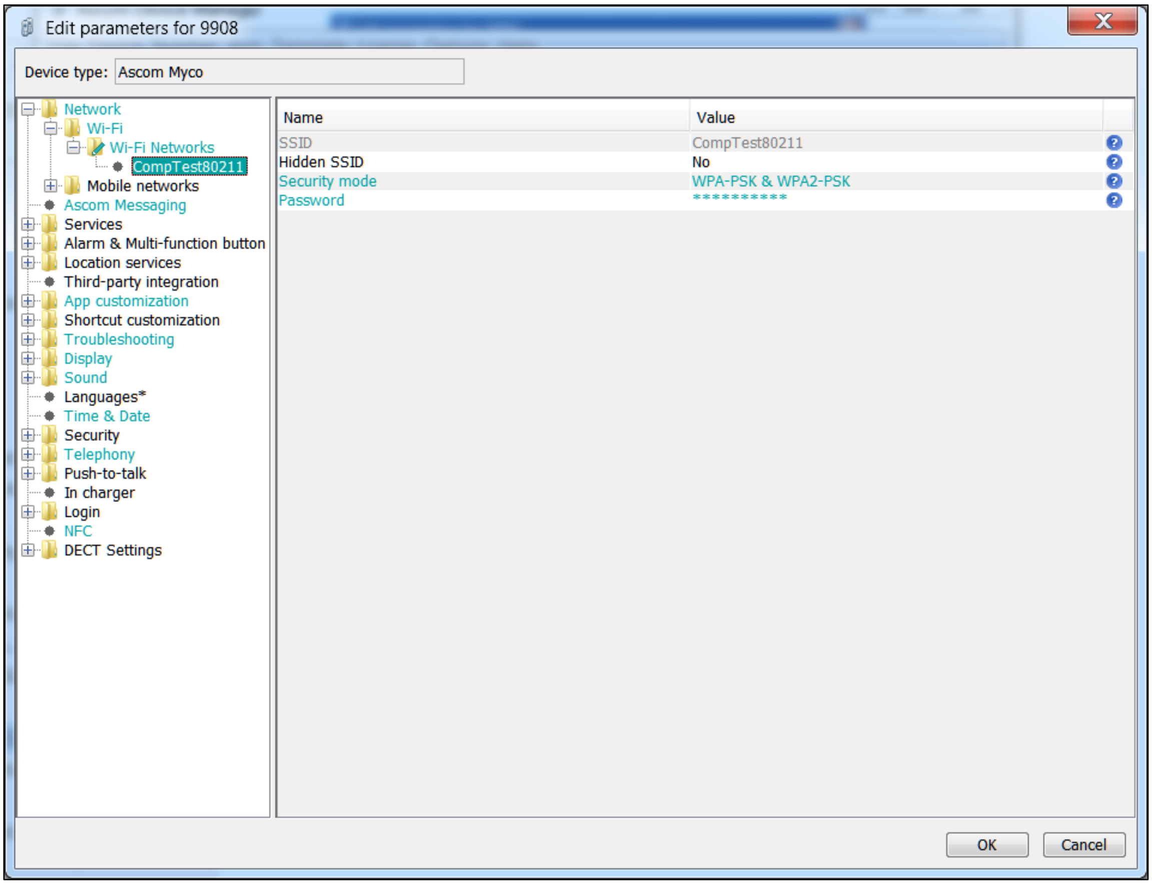


Name	Value
Frequency band	2.4 GHz only
Regulatory domain	World mode (802.11d)
Enabled channels	1,6,11,36,40,44,48,52,56,60,64
Enable 802.11n	Yes
Deauthenticate on roam	No
Roaming methodology	802.11 roaming
Avoid poor connections	No
Captive portal detection	Yes

Network settings for Wi-Fi

- Select Network to be active (In this example “CompTest80211”, created in step below)
- Select frequency band according to system setup.
- Select only the channels used in the system.

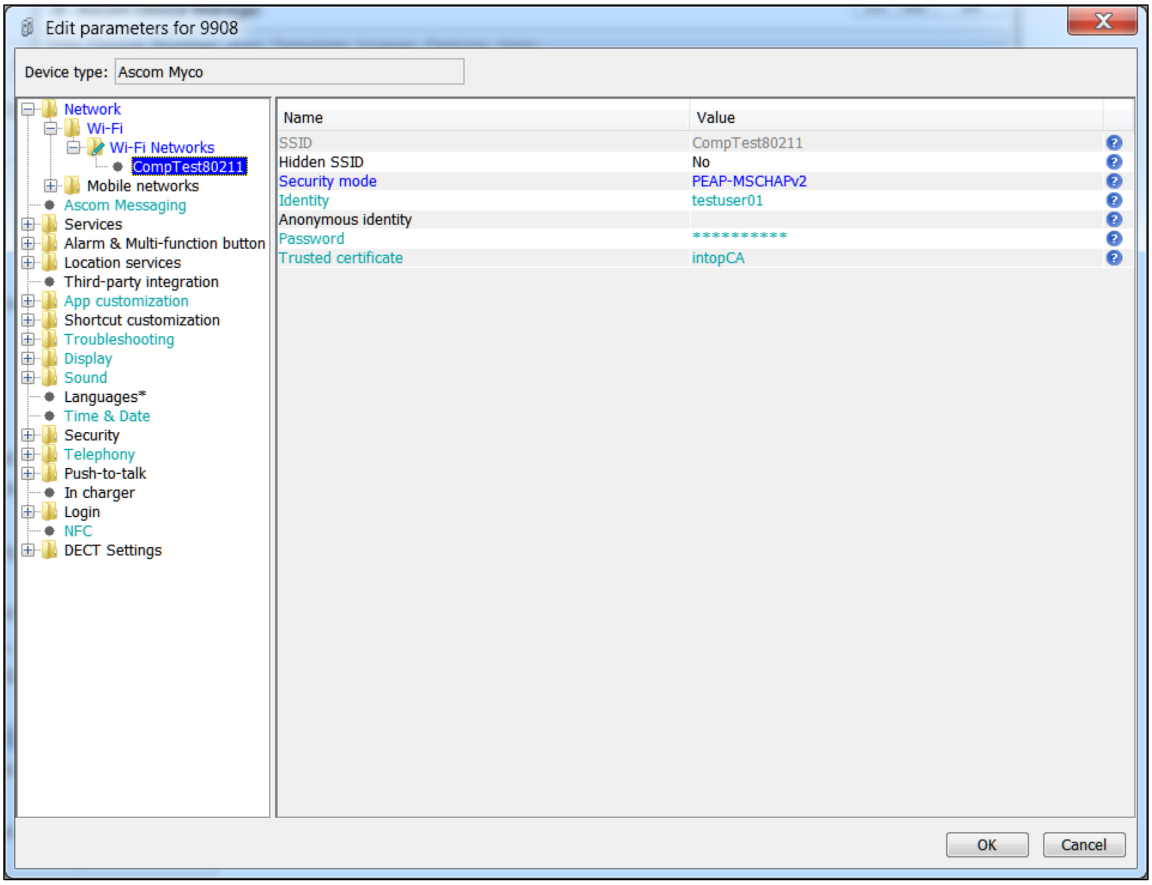
Note: FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in the USA must set Regulatory domain to “US”.



Device type: Ascom Myco

Name	Value
SSID	CompTest80211
Hidden SSID	No
Security mode	WPA-PSK & WPA2-PSK
Password	**********

Network settings for WPA2-PSK

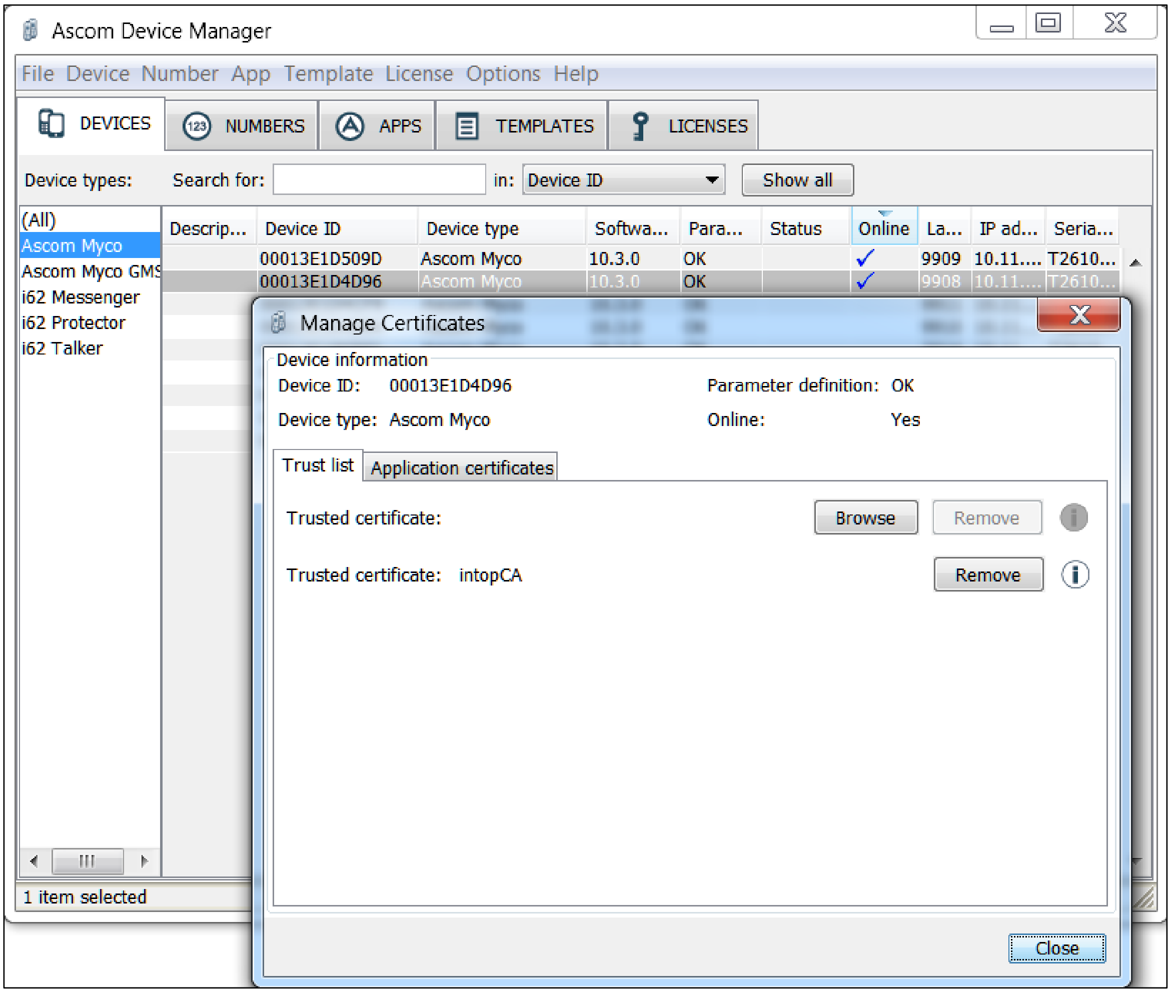


Device type: Ascom Myco

Name	Value
SSID	CompTest80211
Hidden SSID	No
Security mode	PEAP-MSCHAPv2
Identity	testuser01
Anonymous identity	
Password	**********
Trusted certificate	intopCA

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

- Select security mode PEAP-MSCHAPv2.
- Enter User identity and password.
- Select your trusted certificate uploaded to the device (see next page).



Device types: Search for: in: Device ID

(All)
Ascom Myco
Ascom Myco GMS
i62 Messenger
i62 Protector
i62 Talker

Descrip...	Device ID	Device type	Softwa...	Para...	Status	Online	La...	IP ad...	Seria...
	00013E1D509D	Ascom Myco	10.3.0	OK		✓	9909	10.11....	T2610...
	00013E1D4D96	Ascom Myco	10.3.0	OK		✓	9908	10.11....	T2610...

Manage Certificates

Device information

Device ID: 00013E1D4D96 Parameter definition: OK

Device type: Ascom Myco Online: Yes

Trust list | Application certificates

Trusted certificate:

Trusted certificate: intopCA

Ascom Device Manager

- 802.1X Authentication requires a CA certificate to be uploaded to the device. This is done under the “Numbers” tab by “right clicking” the device and selecting “Manage Certificates”.
- Upload the required CA certificate under Trust list.

Note that both a root and a client certificate are needed for TLS. Otherwise only a CA certificate is needed.

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