INTEROPERABILITY REPORT

Ascom i62

Avaya WLAN 8180 controller and 8120/8120-E access points

Avaya WLAN version 1.1.0.133

Ascom i62 and OEM derivatives version 3.4.6

Ascom, Gothenburg

September 2012

TABLE OF CONTENT:

INTRODUCTION

This document describes necessary steps and guidelines to optimally configure the Avaya WLAN platform with Ascom i62 VoWiFi handsets.

The guide should be used in conjunction with both Avaya's and Ascom's configuration guide(s).

About Ascom

Ascom Wireless Solutions (www.ascom.com/ws) is a leading provider of on-site wireless communications for key segments such as hospitals, manufacturing industries, retail and hotels. More than 75,000 systems are installed at major companies all over the world. The company offers a broad range of voice and professional messaging solutions, creating value for customers by supporting and optimizing their Mission-Critical processes. The solutions are based on VoWiFi, IP-DECT, DECT, Nurse Call and paging technologies, smartly integrated into existing enterprise systems. The company has subsidiaries in 10 countries and 1,200 employees worldwide. Founded in the 1950s and based in Göteborg, Sweden, Ascom Wireless Solutions is part of the Ascom Group, listed on the Swiss Stock Exchange.

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, data solutions and related services to companies of all sizes around the world.

SITE INFORMATION

Test Site(s):

Ascom US
598 Airport Blvd
Morrisville 27560 NC

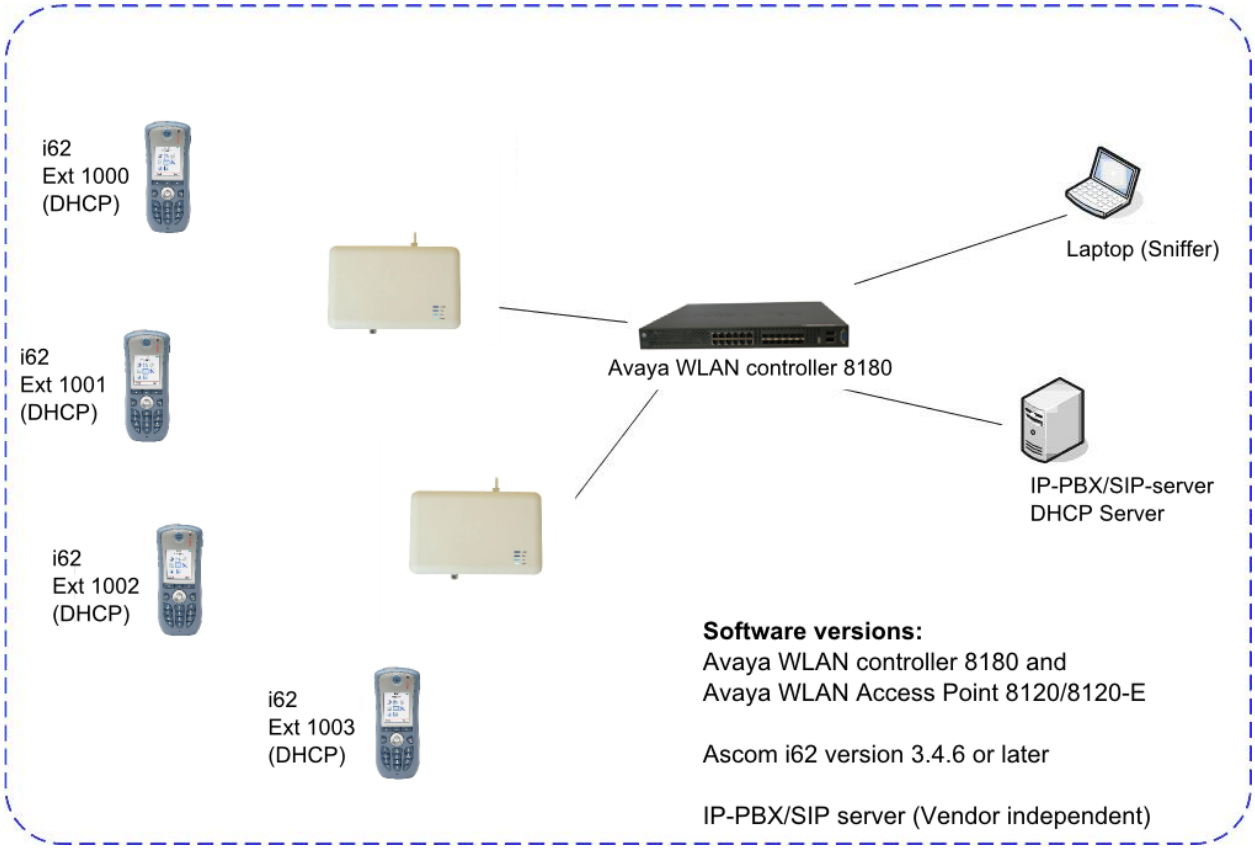
Avaya
4655 Great America Parkway
Santa Clara, CA 95054

Participants:

Karl-Magnus Olsson, Ascom HQ, Gothenburg
Vamshi Doma, Avaya, Santa Clara *

*) Roaming tests including multiple controllers was made by Vamshi Doma, Avaya

TEST TOPOLOGY



SUMMARY

Please refer to Appendix B for detailed results for respective access point.

WLAN Controller Features

High Level Functionality	Result
Association, Open with No Encryption	OK
Association, Open with Static WEP64/128	Not tested
Association, WPA-PSK, TKIP	N/A *
Association, WPA2-PSK, AES Encryption	OK
Association, PEAP-MSCHAPv2 Auth., AES Encryption	OK
Association, EAP-TLS Auth	OK
Association, Multiple ESSIDs	OK
Beacon Interval and DTIM Period	OK
PMKSA Caching	OK **
WPA2-opportunistic/proactive Key Caching	OK **
WMM Prioritization	OK
Active Mode (load test)	OK
802.11 Power-save mode	OK
802.11 Power-save mode (load test)	OK
802.11e U-APSD	OK
802.11e U-APSD (load test)	OK

*) WPA can only be used in “mixed mode”
**) Enabled by default

Roaming

High Level Functionality	Result
Roaming, Open with No Encryption	OK *
Roaming, Open with Static WEP64	Not tested
Roaming, WPA-PSK, TKIP Encryption	N/A
Roaming, WPA2-PSK, AES Encryption	OK **
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK ***

*) Average roaming time: 28ms

**) Average roaming time: 62ms

***) Average roaming time: 48ms

Note: Roaming times are valid for 802.11bg(n). Refer to appendix B for detailed test records.

Known issues

- Having pre-authentication enabled in the systems does affect the stability of the i62 handset. It is therefore strongly recommend to disable pre-authentication and use opportunistic key caching instead (enabled by default)

For additional information regarding known issues please contact intop@ascom.se

Compatibility information

All tests were carried out on an 8180 Avaya WLAN controller and 8120 series access points. This report is applicable also to the chipset (8120-E) with external antennas.

Compatible controllers.
8180 controller

Compatible access points
8120 access points
8120-E access point

General conclusion

The result of the verified test areas, such as authentication/association, handover and load tests was in general very good.

Average roaming times both when PSK and 802.1X authentication was measured to around 50ms.

Performance tests showed that it was possible to keep up 18 simultaneously calls per AP one single access point. Note that this was limited by available phones and not capacity.

Authentication method WPA is available only in combination with WPA2 (WPA2andWPA). Likewise TKIP is only available together with support of CCMP (CCMPandTKIP). Due to configuration constraints in the handset together with the fact that the handset always will utilise the strongest available authentication and encryption method gives two possible PSK combinations; WPA-CCMP and WPA2-CCMP. Recommended setting is WPA2 only and CCMP only.

TEST RESULTS

Ascom WLAN Infrastructure Verification – VoWiFi

Software Versions:

- Avaya WLAN controller 8180 version 1.1.0.133
- Avaya WLAN access point 8120/8120-E
- Ascom i62, version 3.4.6

Signaling Protocol:

- SIP, Innovaphone IP6000 used as SIP server. Version 7 hotfix 15

Configuration of WLAN System:

- Beacon Interval: 100ms
- DTIM Period: 5
- 802.11bg(n)
- 802.11a(n)
- WMM/ U-APSD Enabled (See appendix A for QoS profiles)
- 802.11d Regulatory Domain: World mode

Ascom i62 Configuration:

- World Mode Regulatory Domain set to World mode (802.11d).
- IP DSCP for Voice: 0x2E (46) – Expedited Forwarding
- IP DSCP for Signaling: 0x1A (26) – Assured Forwarding 31
- Transmit Gratuitous ARP: Enable

Keep in mind that security options and power save modes were adjusted according to requirements in individual test cases. Please refer to appendix A for information regarding device configuration.

Test Areas

Association and Authentication: 100% pass (6/6)

- WPA possible to configure only together with support of WPA2
- TKIP can only be selected together with CCMP.
- FreeRadius was used in the test cases where an authentication server was needed.

Power Save and QoS: 100 % pass (4/4)

- QoS mode has to be set to WMM and U-APSD must be enabled.
- Load test done with iPerf. No noticeable degeneration of voice quality.

Performance, “Maximum Number of Calls”: 100% pass (2/2)

- 18 active calls per single radio verified in active mode and U-APSD.

Roaming and Handover Times: 100% pass (4/4)

- PMKSA caching and Opportunistic/Proactive Key Caching verified (enabled by default)
- Pre-Authentication not recommended
- FreeRadius was used in the test cases where an authentication server was needed.

Stability: 100% Pass (2/2)

- Stable call for the duration of >24 hours in none Power Save Mode.
- Stable call for the duration of >24 hours in U-APSD mode.
- Stability test done in both 802.11an and 802.11bgn mode.

Please keep in mind that metrics do NOT account for untested cases.

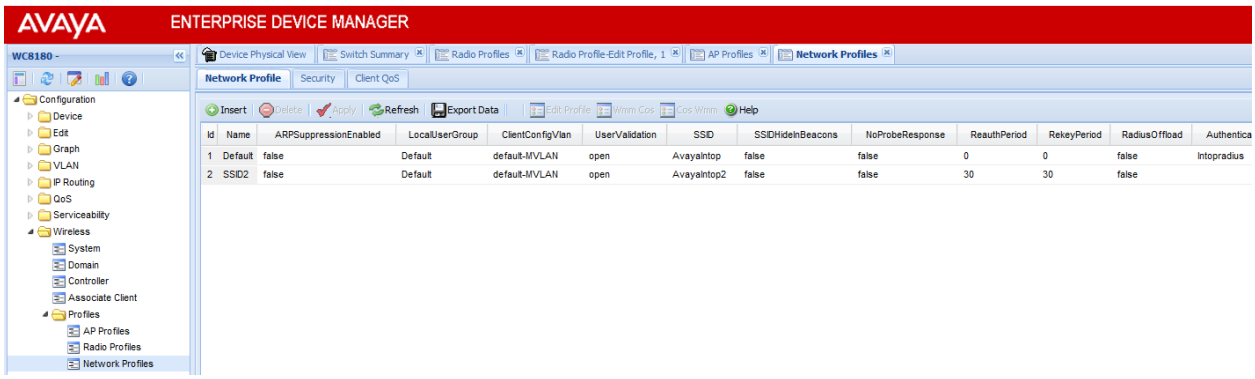
APPENDIX A: TEST CONFIGURATIONS

Avaya WLAN 8180 controller and 8120/8120-E access points

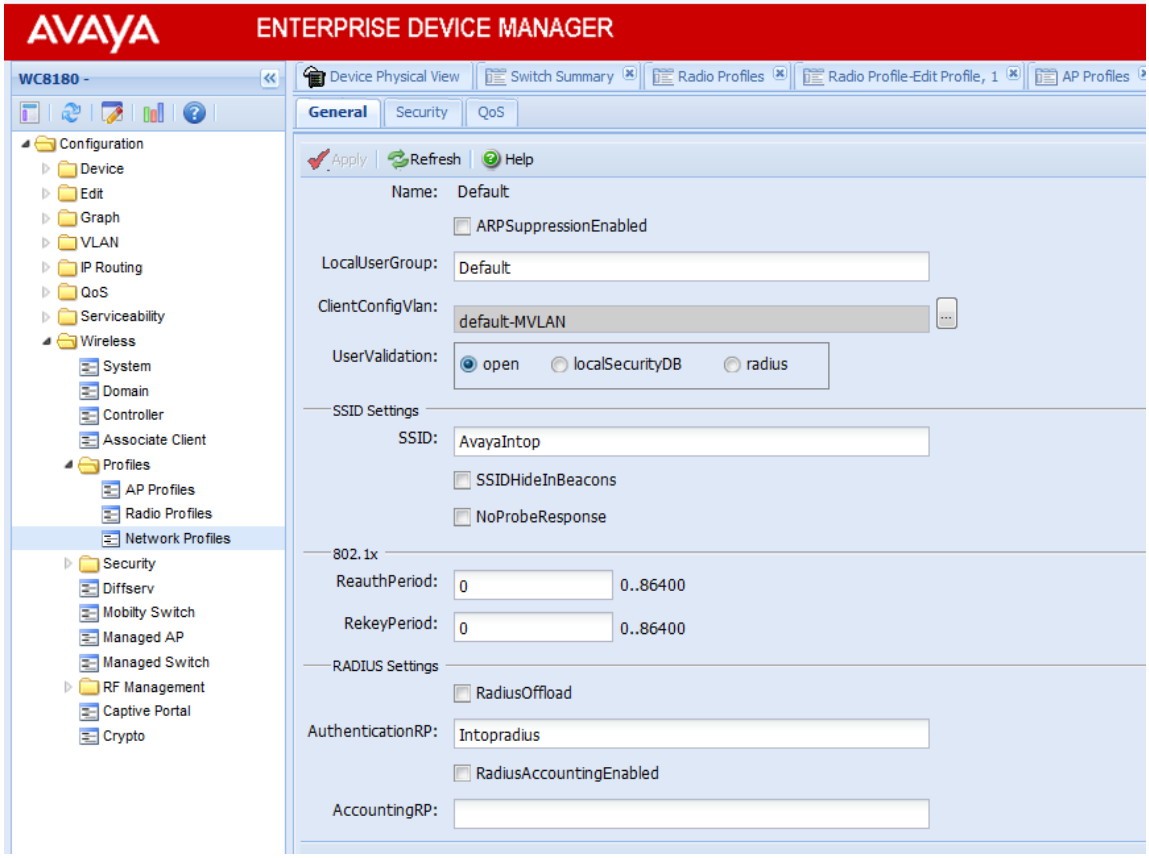
In the following chapter you will find screenshots and explanations of basic settings in order to get the Avaya WLAN operational with Ascom i62. Please note that security settings were modified according to requirements in individual test cases.

The configuration file is found at the bottom of this chapter.

ESS, Radio and QoS settings



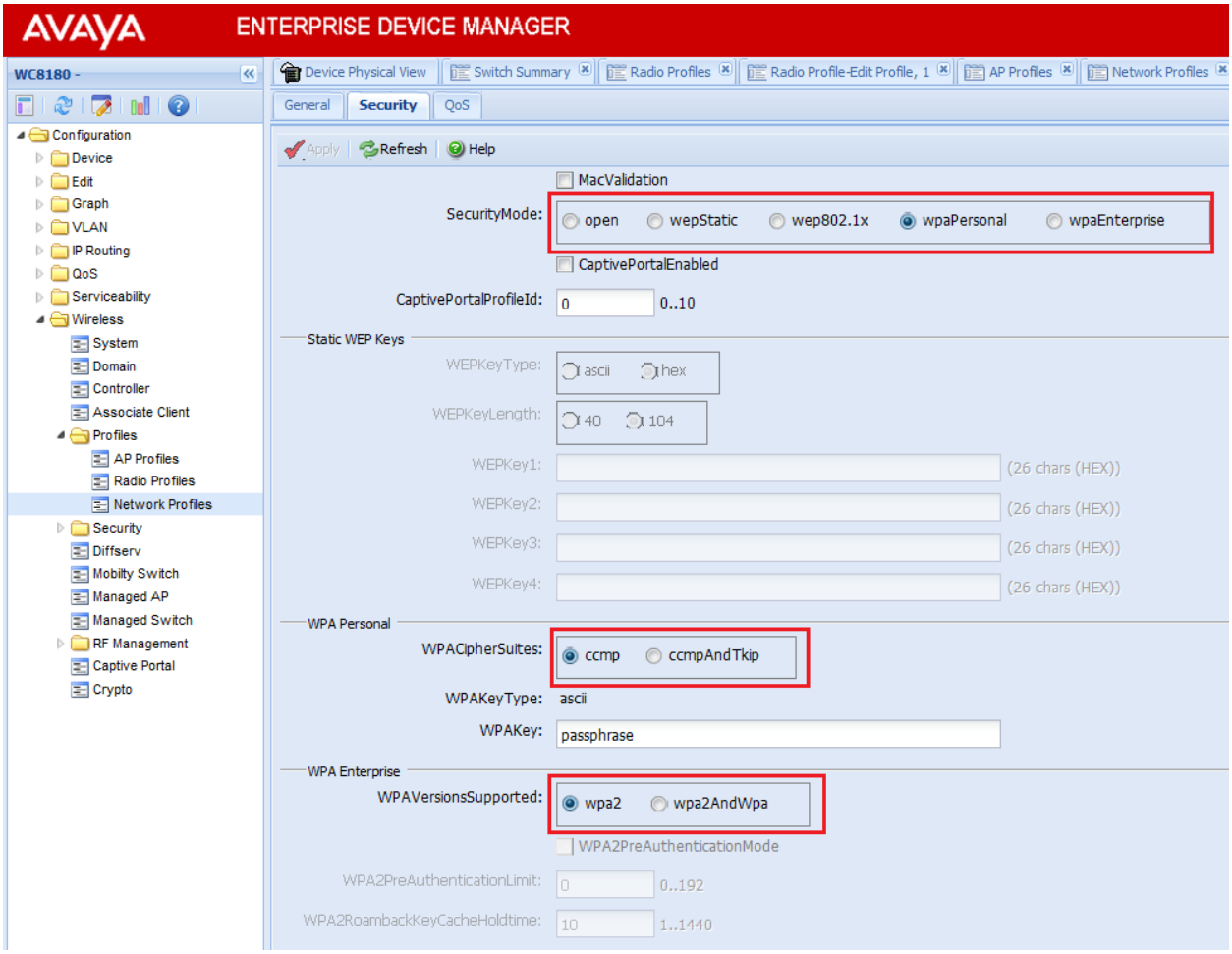
Configuration > Wireless > Network Profiles



Configuration > Wireless > Network Profiles > General

Basic SSID settings.

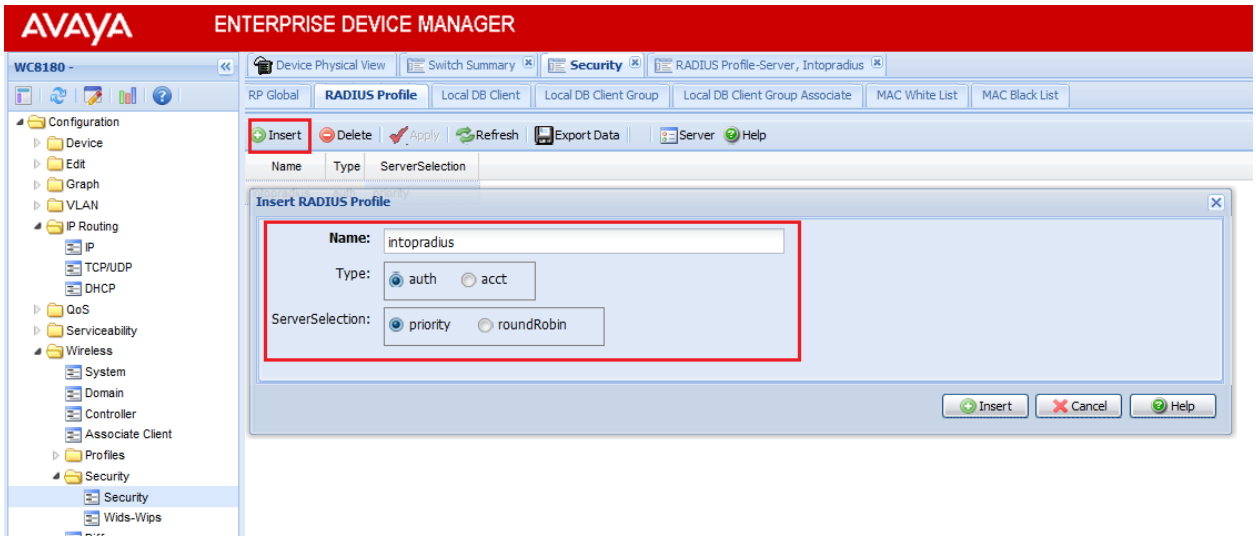
Security settings



Configuration > Wireless > Network Profiles > Security

- Select Security profile WPA2-PSK, AES-CCMP encryption.

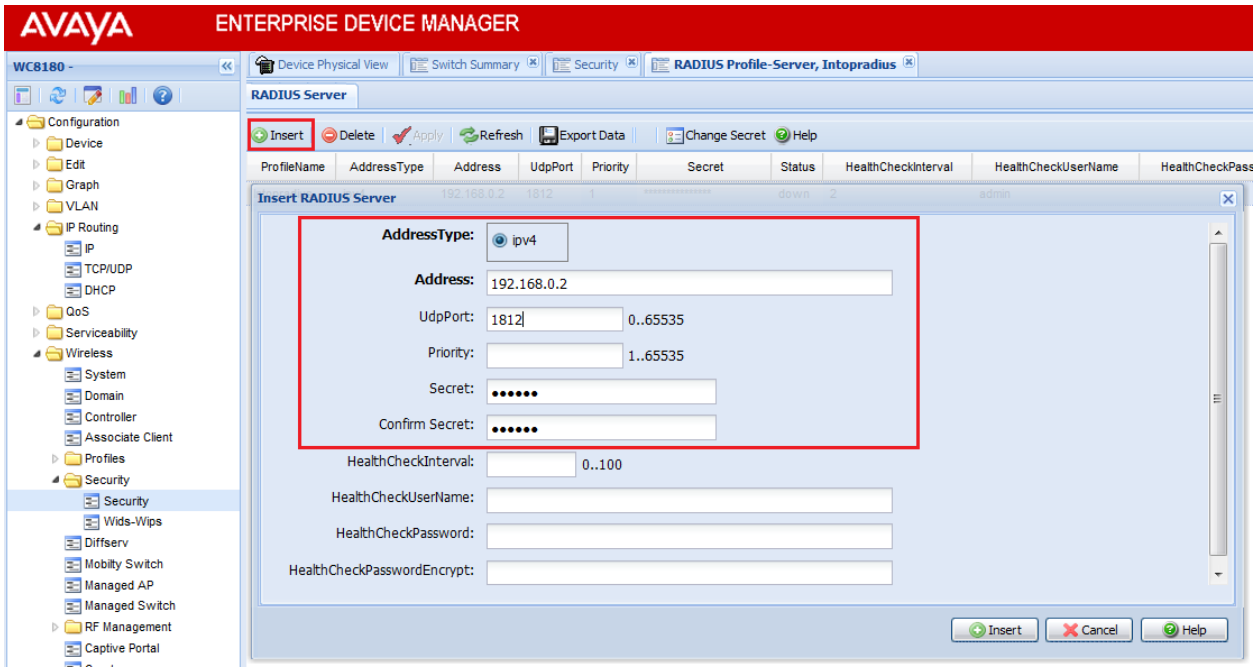
Setting up a WPA2-Enterprise/802.1X



Configuration > Wireless > Security > Security

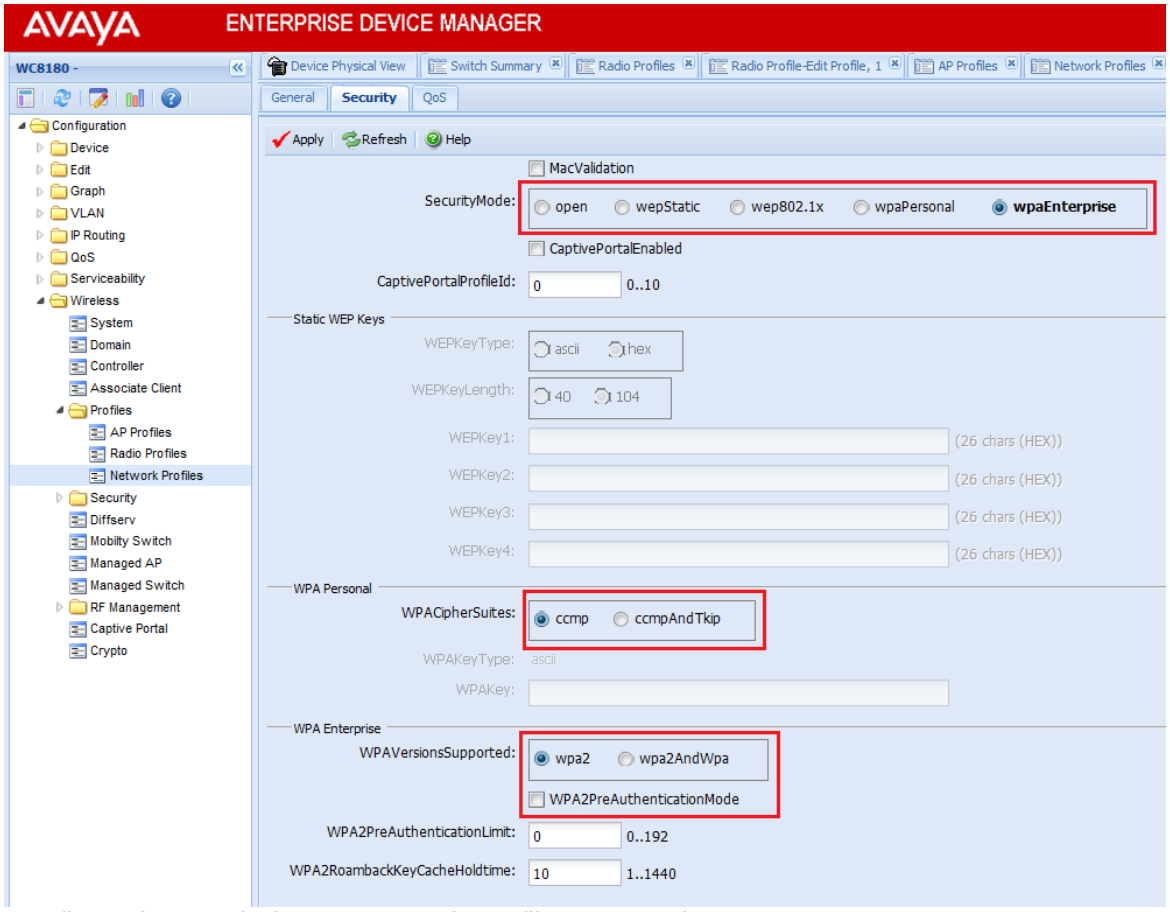
- Add a new RADIUS profile by clicking “Insert”
- Select Type: auth
- Select ServerSelection: Priority.

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



Configuration > Wireless > Security > Security

- Create a new server by clicking “Insert”
- Add the address to the RADIUS server, port to use and fill in the secret.

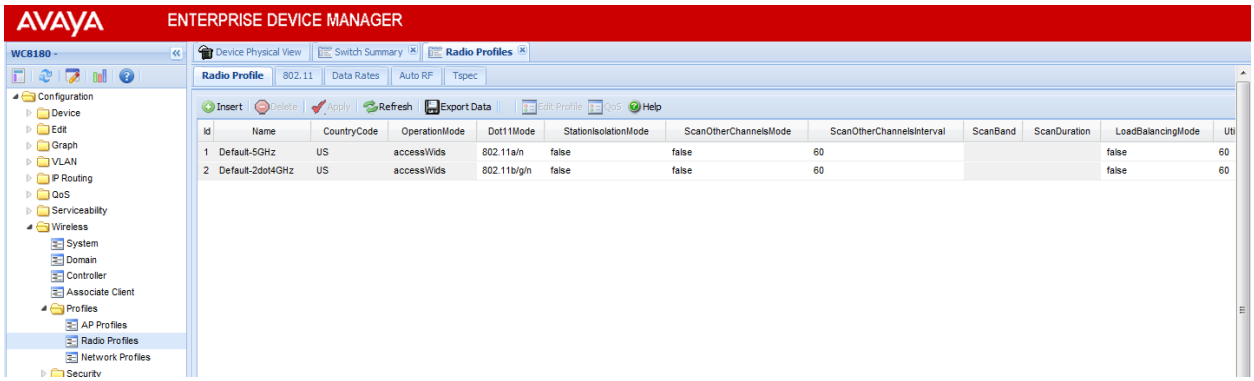


Configuration > Wireless > Network Profiles > Security

- Select wpaEnterprise, ccmp and wp2.
- Unselect the checkbox to disable pre-authentication.

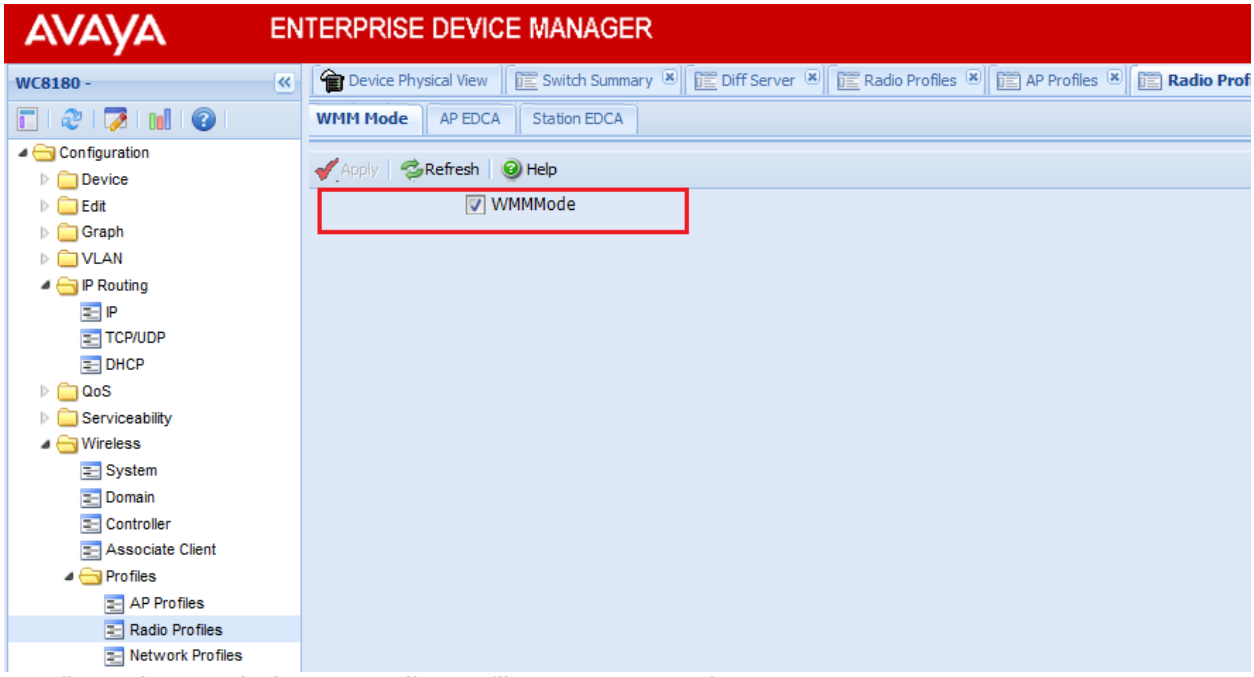
Note. Opportunistic key caching/proactive key caching will work between controllers given that they are in the same domain.

Radio Configuration



Configuration > Wireless > Radio Profiles

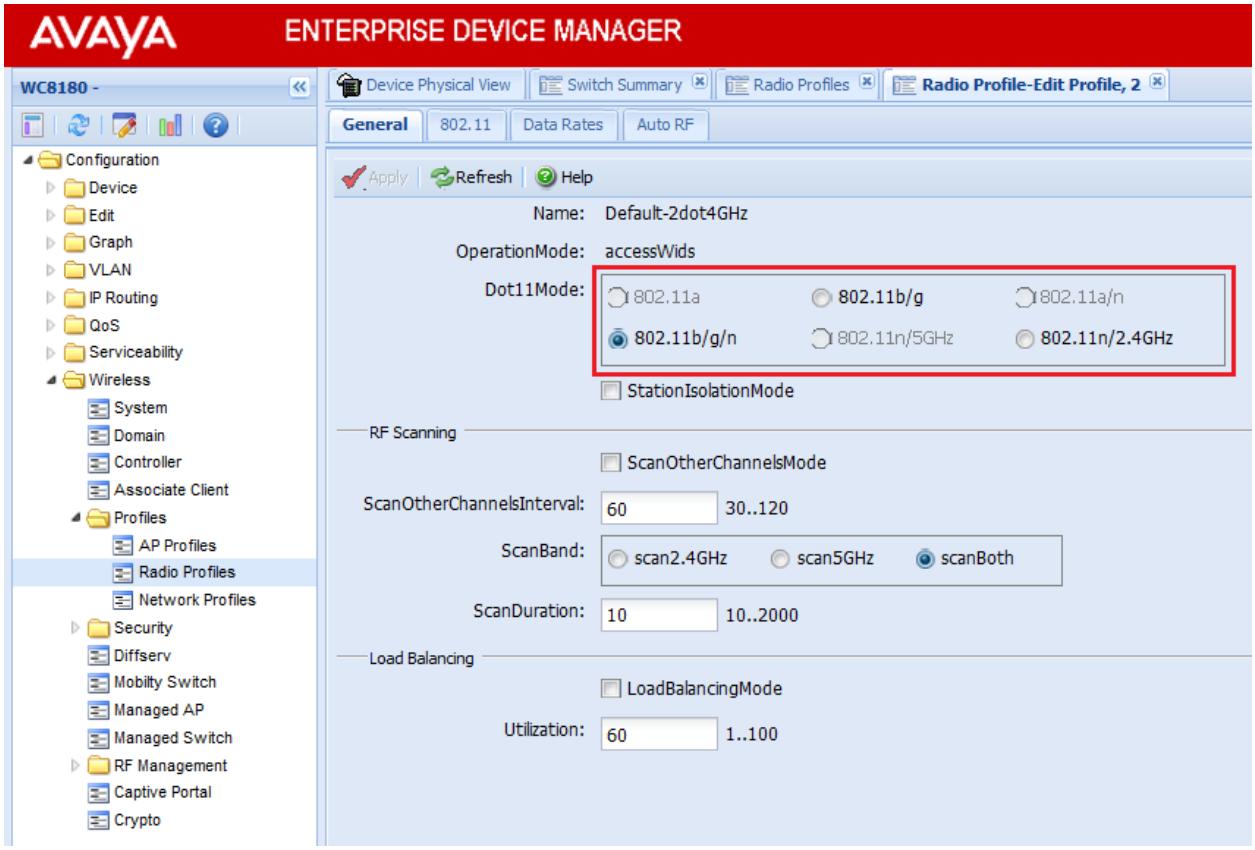
Radio Profiles overview.



Configuration > Wireless > Radio Profiles > WMM Mode

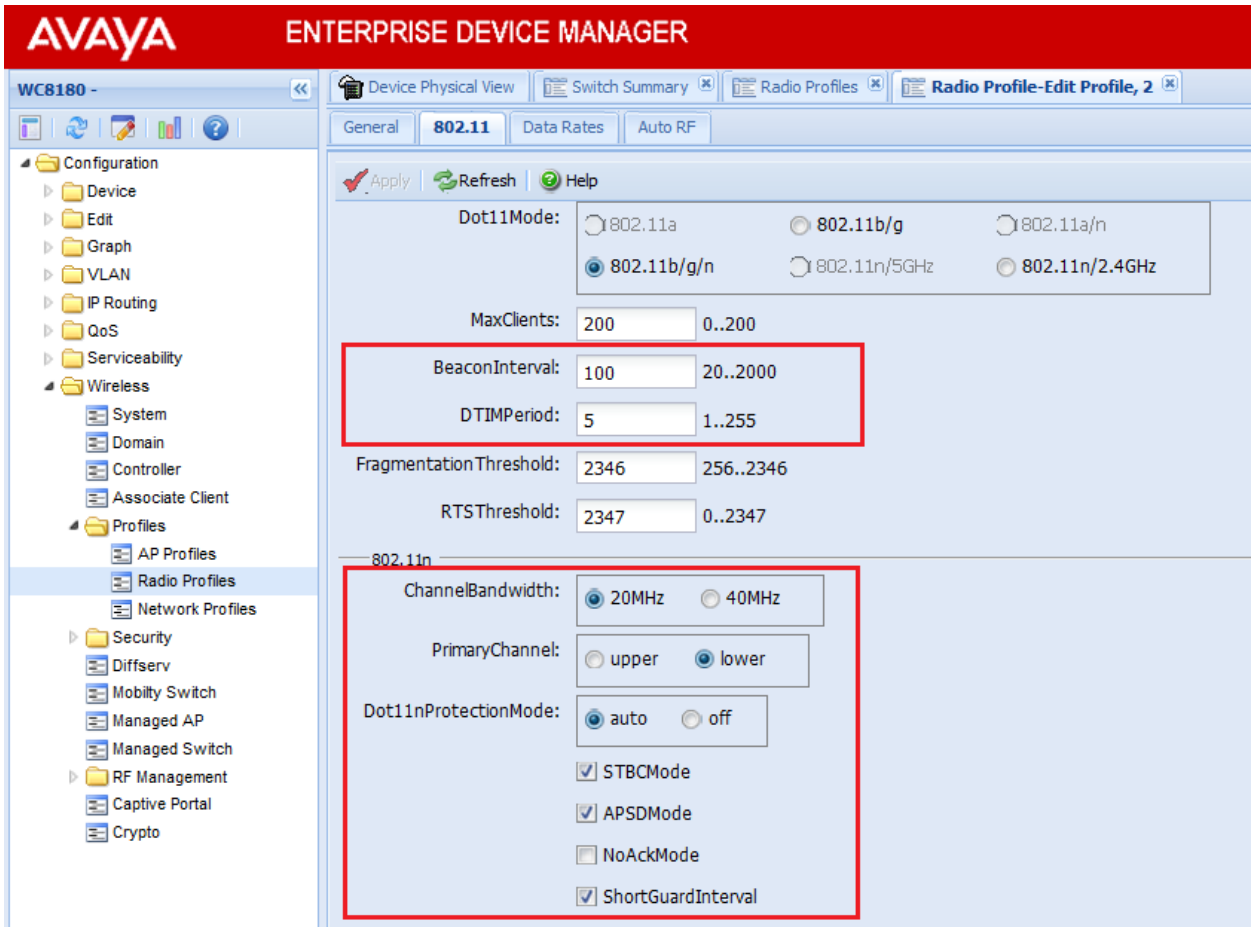
- Secure that WMMMode is enabled. (Enabled by default).

802.11b/g/n



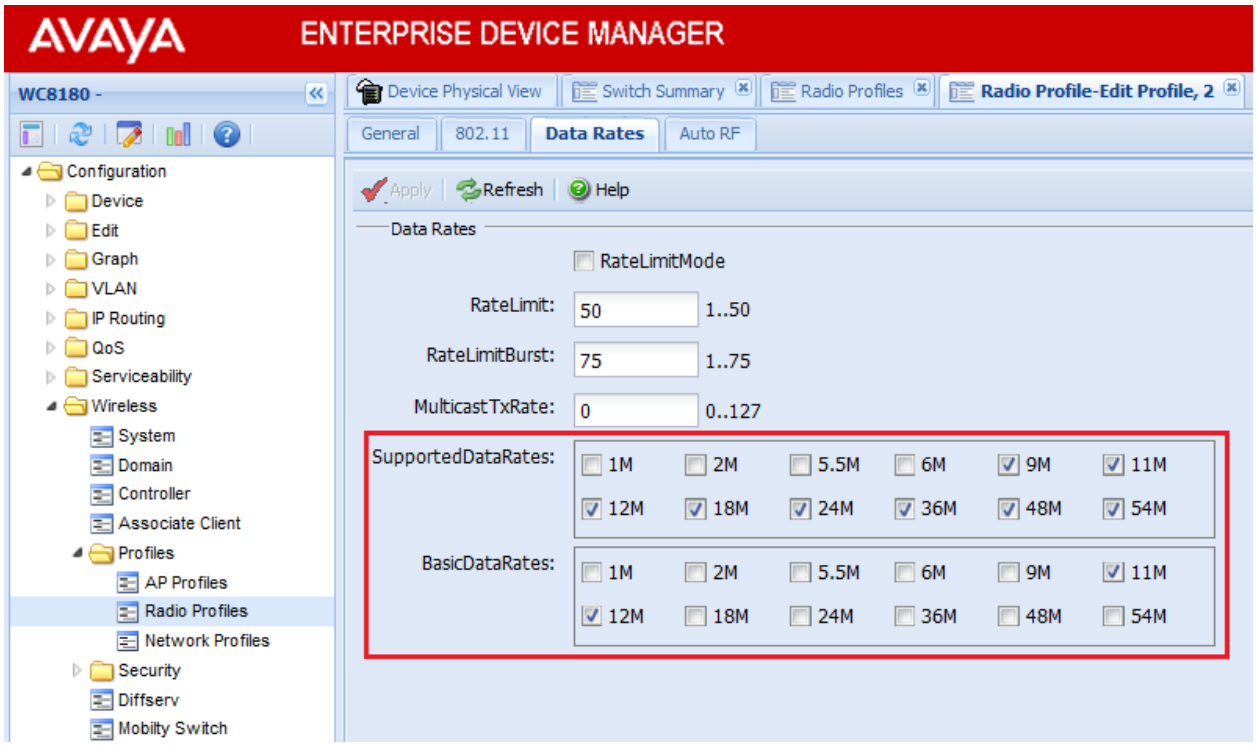
Configuration > Wireless > Radio Profiles > General

- Select 802.11b/g/n.



Configuration > Wireless > Radio Profiles > 802.11

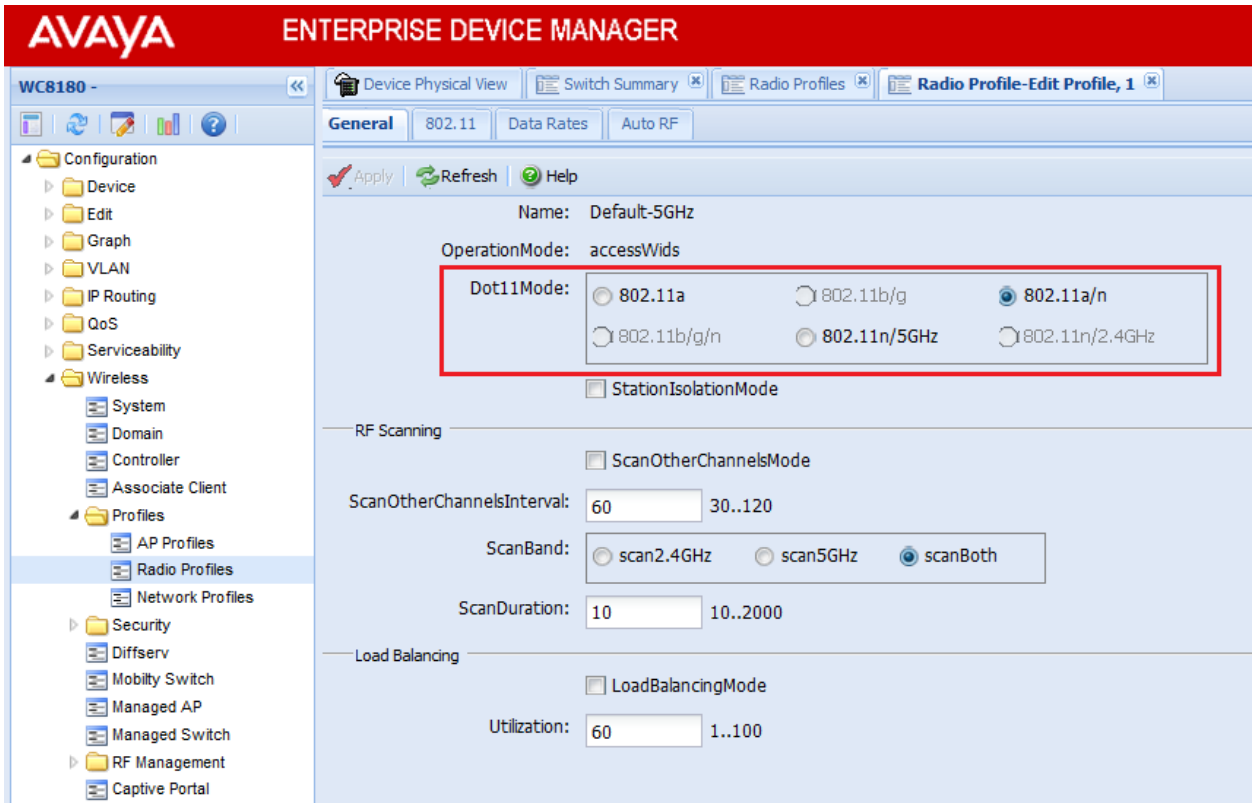
- Ascom recommends a Beacon Interval of 100ms and a DTIM interval of 5. DTIM value 5 is recommended in order to allow maximum battery conservation without impacting the quality. A lower value will negatively impact the standby time.
- Channel bonding is not recommended on the 2.4GHz band.
- Make sure that APSDmode is enabled.



Configuration > Wireless > Radio Profiles > Data Rates

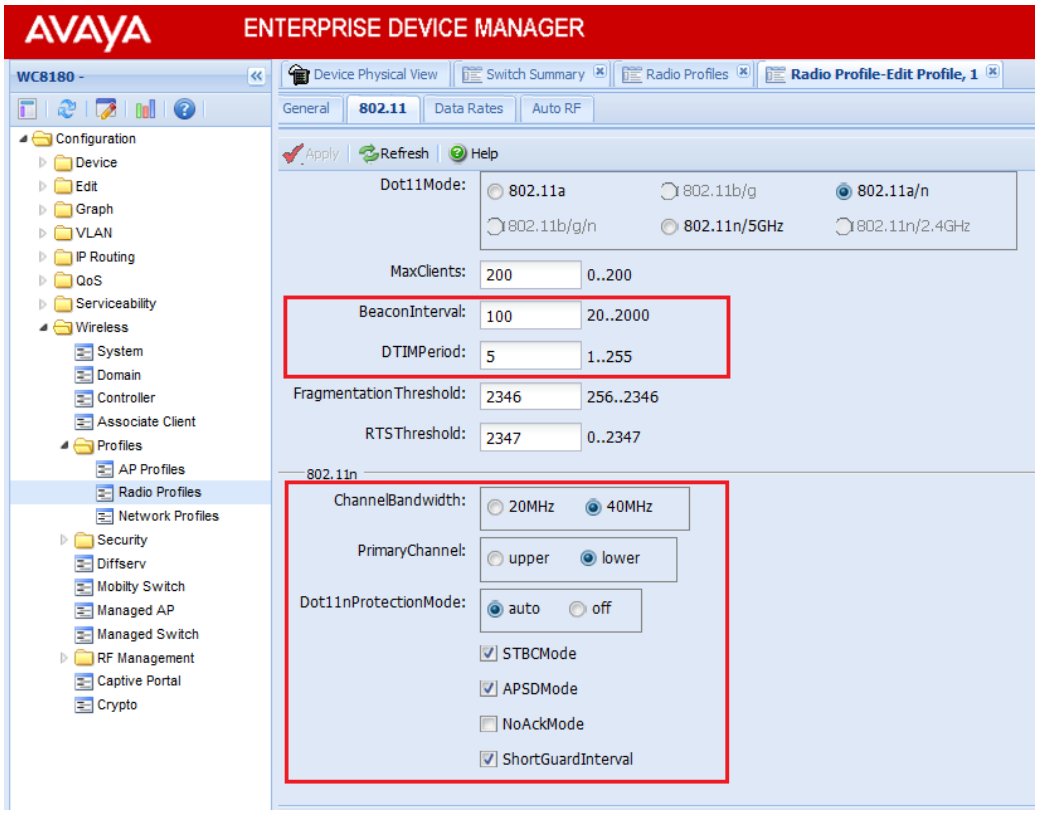
- Ascom recommends that the lowest data rates are disabled. The default data rates set is ok but consider that the performance will decrease.

802.11a/n



Configuration > Wireless > Radio Profiles > General

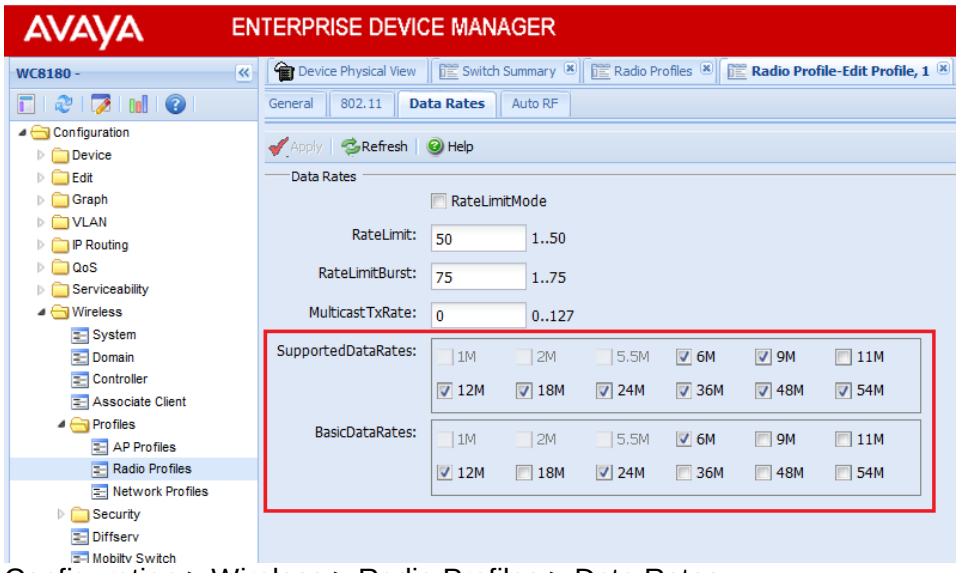
Select 802.11a/n.



Configuration > Wireless > Radio Profiles > 802.11

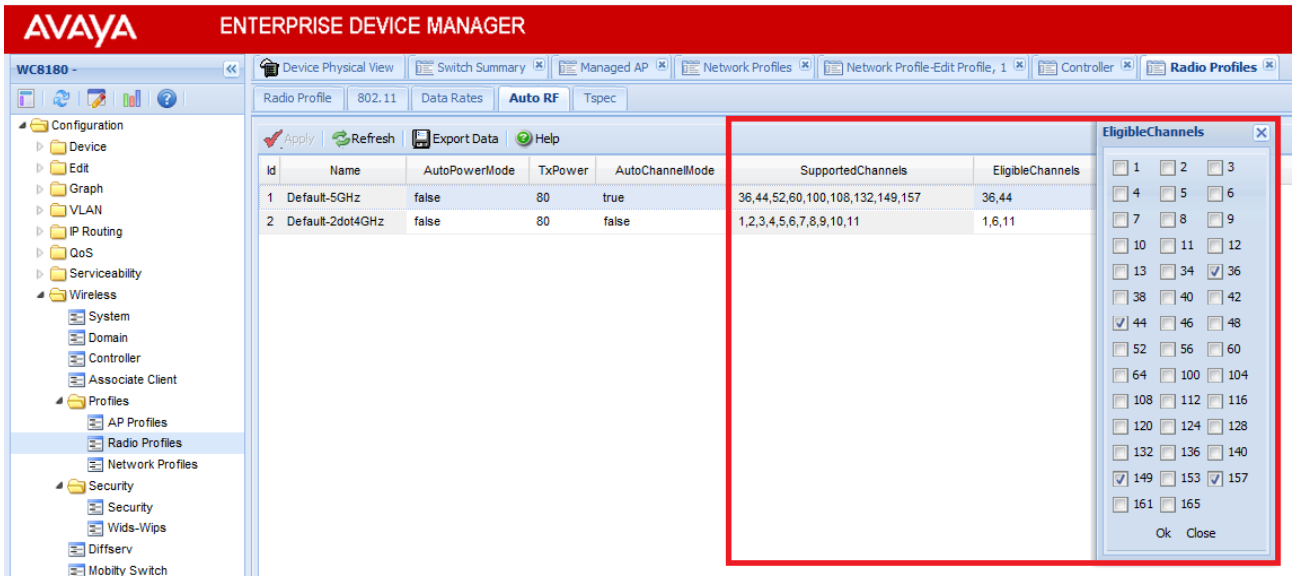
- Ascom recommends a Beacon Interval of 100ms and a DTIM interval of 5. DTIM value 5 is recommended in order to allow maximum battery conservation without impacting the quality. A lower value will negatively impact the standby time.
- Make sure that APSDmode is enabled.

Note. Channel bonding is enabled by default but doesn't have to be used.



Configuration > Wireless > Radio Profiles > Data Rates

- Default data rate set.



Configuration > Wireless > Radio Profiles > Auto RF

Ascom support only 3 channel deployments using channel 1,6 and11. For 802.11a/n use channels according to the infrastructure manufacturer and country regulations.

General guidelines when deploying Ascom i62 handsets (SW version 2.5.7 or later) in 802.11a/n environments:

1. Enabling more than 8 channels will degrade roaming performance. Ascom strongly recommends against going above 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.

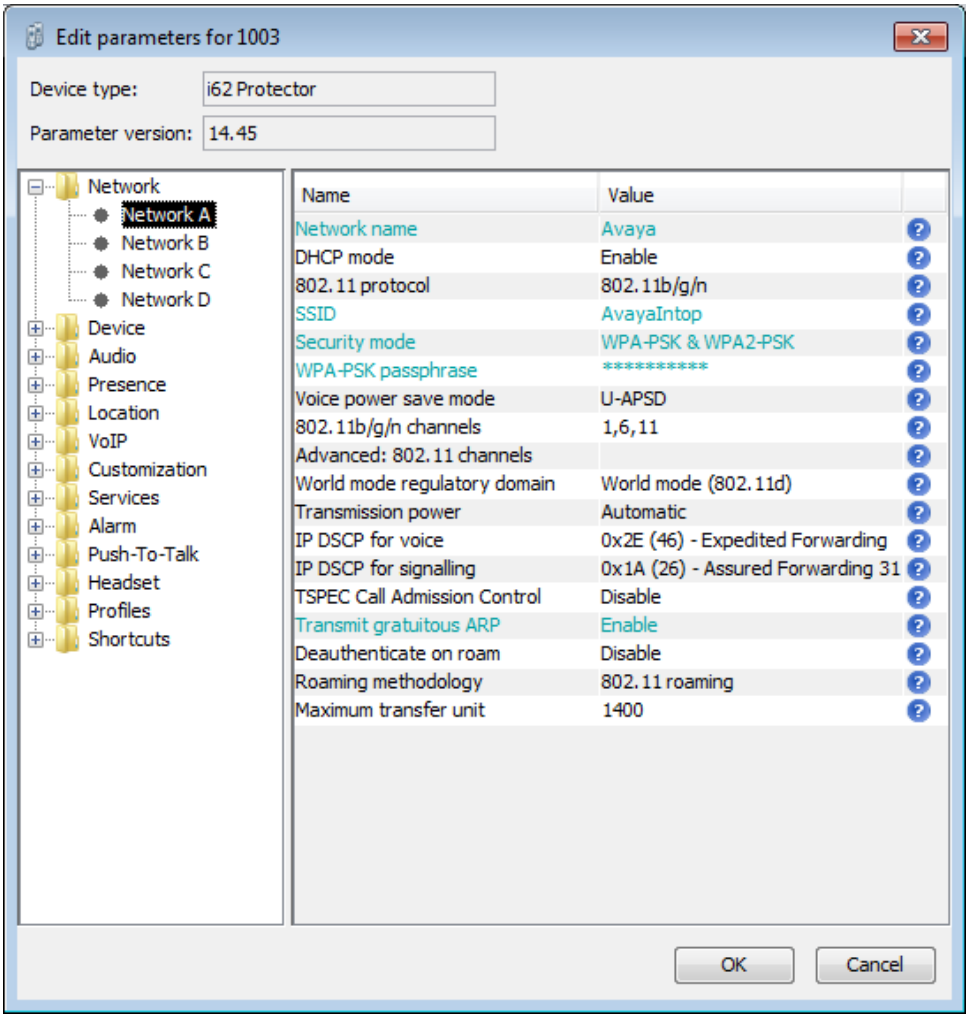
3. Make sure that all non-DFS channel are taken before resorting to DFS channels. The handset can cope in mixed non-DFS and DFS environments; however, due to “unpredictability” introduced by radar detection protocols, voice quality may become distorted and roaming delayed. Hence Ascom recommends avoiding the use of DFS channels in VoWIFI deployments.

Configuration:

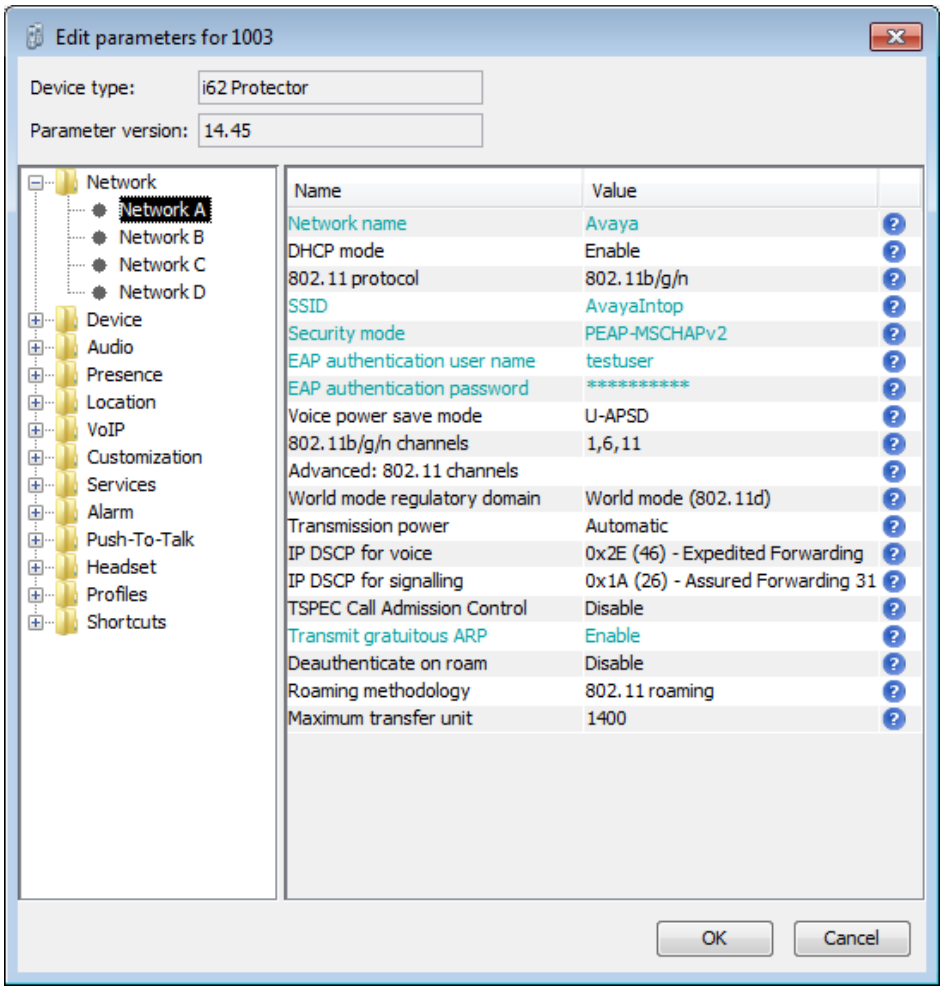
Avaya WLAN configuration

See attached file (config.txt) for the 8180 controller configuration.

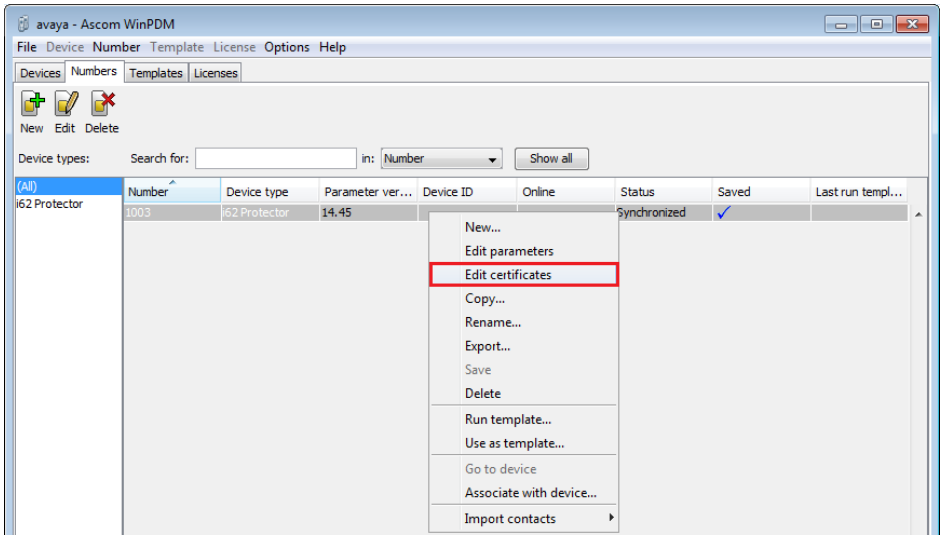
Ascom i62



Ascom i62 Network configurations (WPA2-PSK)



i62 network settings for 802.1X authentication (PEAP-MSCHAPv2)



If 802.1X Authentication is used a root certificate has to be uploaded to the phone by “right clicking” - > Edit certificates. EAP-TLS will require both a root and a client certificate.

Innovaphone IP6000 (IP PBX)

The Innovaphone IP6000 was configured with a static IP address of 192.168.0.50. Signaling is less relevant here since testing homes in on interoperability in relation to the WLAN infrastructure and not features of the IP PBX.

IP6000 configuration:

See attached file (complete-IP6000-08-03-a6.txt) for configuration.

APPENDIX B: DETAILED TEST RECORDS

VoWIFI

Pass	23
Fail	0
Comments	10
Untested	1
Total	34

See attached file (WLANinteroperabilityTestReport_Avaya.xls) for detailed test results.

MISCELLANEOUS

Please refer to the test specification for WLAN systems on Ascom's interoperability web page for explicit information regarding each test case.

See URL (requires login):
https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability

Document History

Rev	Date	Author	Description
P1	2012-01-16	SEKMO	Initial draft
P2	2012-01-19	SEKMO	Corrections to Radio settings chapter (DFS)
P3	2012-01-24	SEKMO	Minor improvements.
R1	2012-02-01	SEKMO	Revision 1
R2	2012-09-18	SEKMO	Revision 2. Changed recommended version to 3.4.6 or later