INTEROPERABILITY REPORT

Ascom i62

Enterasys WLAN

(C20/C25/C2110/C2400/C4110/C5110 and AP 3605/3610/3620/3630/3640 & 3705/3710/3715/3765/3767)

i62 and OEM derivatives version 4.3.12

Enterasys software version 08.31.02

Ascom, November 2013

TABLE OF CONTENT:

INTRODUCTION 3
Ascom solution 3
Enterasys solution 3
SITE INFORMATION 4
SUMMARY 5
General conclusion 6
Compatibility information 6
Known issues 6
TEST RESULTS 7
Ascom WLAN Infrastructure Verification – VoWiFi 7
APPENDIX A: TEST CONFIGURATIONS 8
Enterasys Wireless C20 Controller v. 08.31.02 8
Overview 8
Enterasys controller overview. 8
Security settings (PSK) 9
Security settings (802.1X / PEAP-MSCHAPv2) 10
General settings (SSID, QoS, Radio) 13
APPENDIX B: DETAILED TEST RECORDS 23

INTRODUCTION

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

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

Ascom solution

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.

Enterasys solution

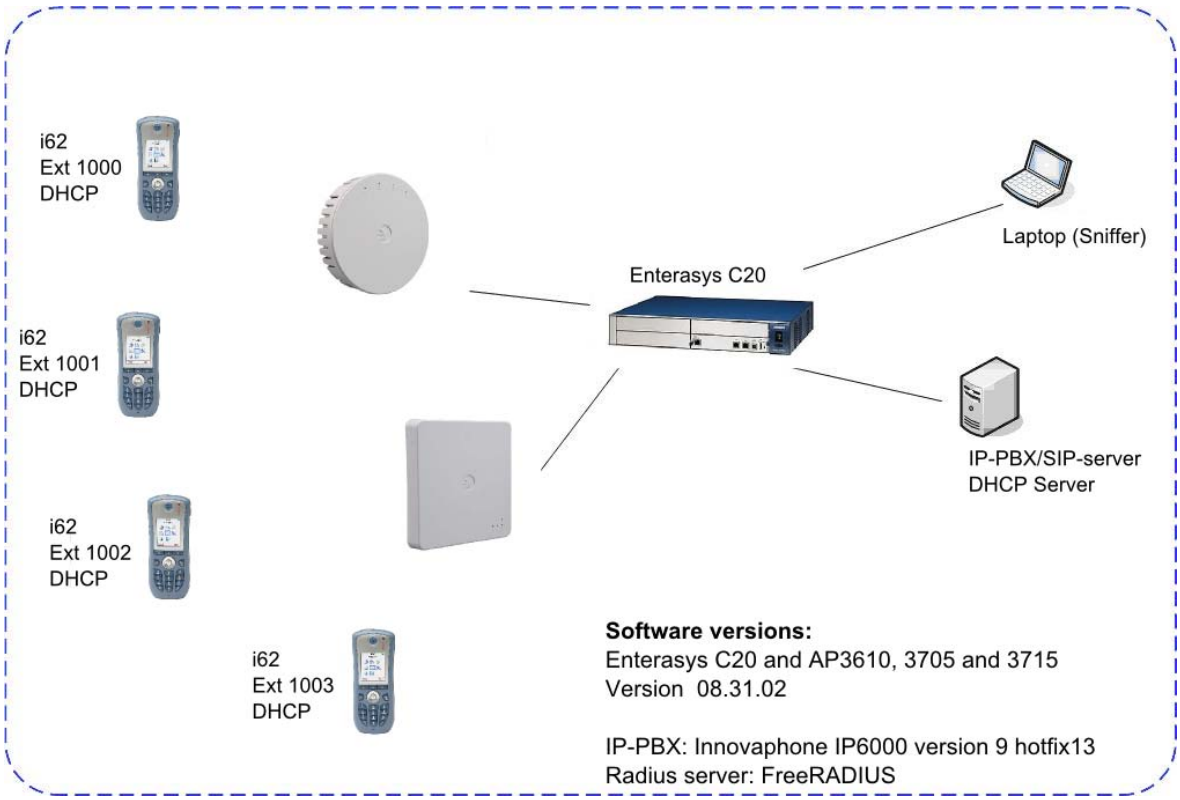
Enterasys Networks is one of the fastest growing companies in the networking industry, providing patented and differentiated wired and wireless network infrastructure, as well as security and management solutions. Enterasys OneFabric is the industry's first fabric-based networking solution to extend visibility and control from virtual servers to mobile devices for cloud computing, software-defined networking, and data center environments. OneFabric enables our customers to provision the network from the data center to the mobile edge with consistent performance to deliver a positive end user experience through enhanced application analytics, all managed from a single pane of glass. With over 20,000 customers and sales in over 90 countries, Enterasys addresses the complexities of today's mega-trends around Mobile, Social, Cloud and Big Data, serving customers across major verticals including education (K-12 and higher education), healthcare, government, manufacturing and hospitality. For more information about Enterasys please visit www.enterasys.com.

SITE INFORMATION

Test Site:
Ascom US
598 Airport Blvd, Suite 300
Morrisville, NC, US-27560
USA

Participants:
Karl-Magnus Olsson, Ascom Sweden, Gothenburg

TEST TOPOLOGY



SUMMARY

Please refer to Appendix B for detailed results.

WLAN Controller Features

High Level Functionality	Result
Association, Open with No Encryption	OK
Association, WPA-PSK, TKIP	OK
Association, WPA2-PSK, TKIP	Not supported by controller
Association, WPA2-PSK / AES Encryption	OK
Association, PEAP-MSCHAPv2 Auth, AES Encryption	OK
Association with EAP-FAST authentication	OK
Association with EAP-TLS authentication	OK
Association, Multiple ESSIDs	OK
Beacon Interval and DTIM Period	OK
Preauthentication	Not recommended
PMKSA Caching	OK
WPA2-opportunistic/proactive Key Caching	OK
WMM Prioritization	OK
Active Mode (load test)	OK
802.11 Power-save mode	OK
802.11e U-APSD	OK
802.11e U-APSD (load test)	OK

Roaming

High Level Functionality	Result
Roaming, Open with No Encryption	OK (typical roaming time 23ms)
Roaming, WPA-PSK, TKIP Encryption	OK (typical roaming time 40ms)
Roaming, WPA2-PSK, AES Encryption	OK (typical roaming time 45ms)
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK (typical roaming time 35ms)*
Roaming, EAP-TLS, AES Encryption	OK(typical roaming time 35ms) *

*) Measured times is with opportunistic key caching enabled.

Results reflect outcome of AP3715. See appendix B for detailed results for the other AP models.

General conclusion

The verification, including association, authentication and call stability tests generated in general very good results. Roaming times were measured in the range of 35ms and 55ms when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

Load tests showed that it was possible to maintain 18 simultaneous calls on one access point when using the minimum basic rate set to 11Mbps for 802.11bgn and. The same number of simulations calls could be maintained also for 802.11an.

The majority of the test cases were performed in B@HWC mode. Several tests were however verified also in B@AP mode. No difference in functionality or performance was noticed. Inter controller roaming was verified with B@AP, B@HWC and Routed topology.

Compatibility information

All tests were done on AP3705, 3715 and AP3610 (Internal antennas) and a C20 controller. Due to the fact that AP3605, AP3610, AP3620, AP3630 and AP3640 share the same WLAN chipset, their behavior can be considered to be identical. AP3710 share the same chipset as AP3715. We therefore ensure compatibility/interoperability according to the list below. All Enterasys controller s are considered to be covered based on testing towards C20.

i62 version 4.3.12 is using WLAN driver version 2.4.e

Supported access points with Enterasys Wireless version 08.31.02 or above:

AP3605, AP3610, AP3620
AP3630 (Converted to Fit Mode), AP3640 (Converted to Fit Mode)

AP3705, AP 3710, AP 3715, AP3765, AP3767

Supported controller platforms with Enterasys Wireless version 08.31.06 or above:

C20/C20N
C25
C2110
C2400
C4110
C5110

Known issues

- Upon hold/retrieve (SIP) towards some PBX platform it has been noticed that the packet queue in the access point overflow, which may cause dropped SIP packets. Symptom: unable to retrieve call after hold. Workaround: lower DTIM value or remap the call signaling to a higher access category.

For additional information regarding the known issues please contact interop@ascom.se or support@ascom.se

TEST RESULTS

Ascom WLAN Infrastructure Verification – VoWiFi

Software Versions:

- Enterasys C20 Version 08.31.02
- AP3610, 3705 and 3715
- Ascom i62, v4.3.12 (WLAN driver 2.4.e)

Signaling Protocol:

- SIP

Configuration of WLAN System:

- Beacon Interval: 100ms
- DTIM Period: 5
- 802.11bgn
- 802.11an
- WMM/ U-APSD Enabled
- 802.11d Regulatory Domain: World mode
- Minimum basic rate set to 11Mbps

Ascom i62 Configuration:

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

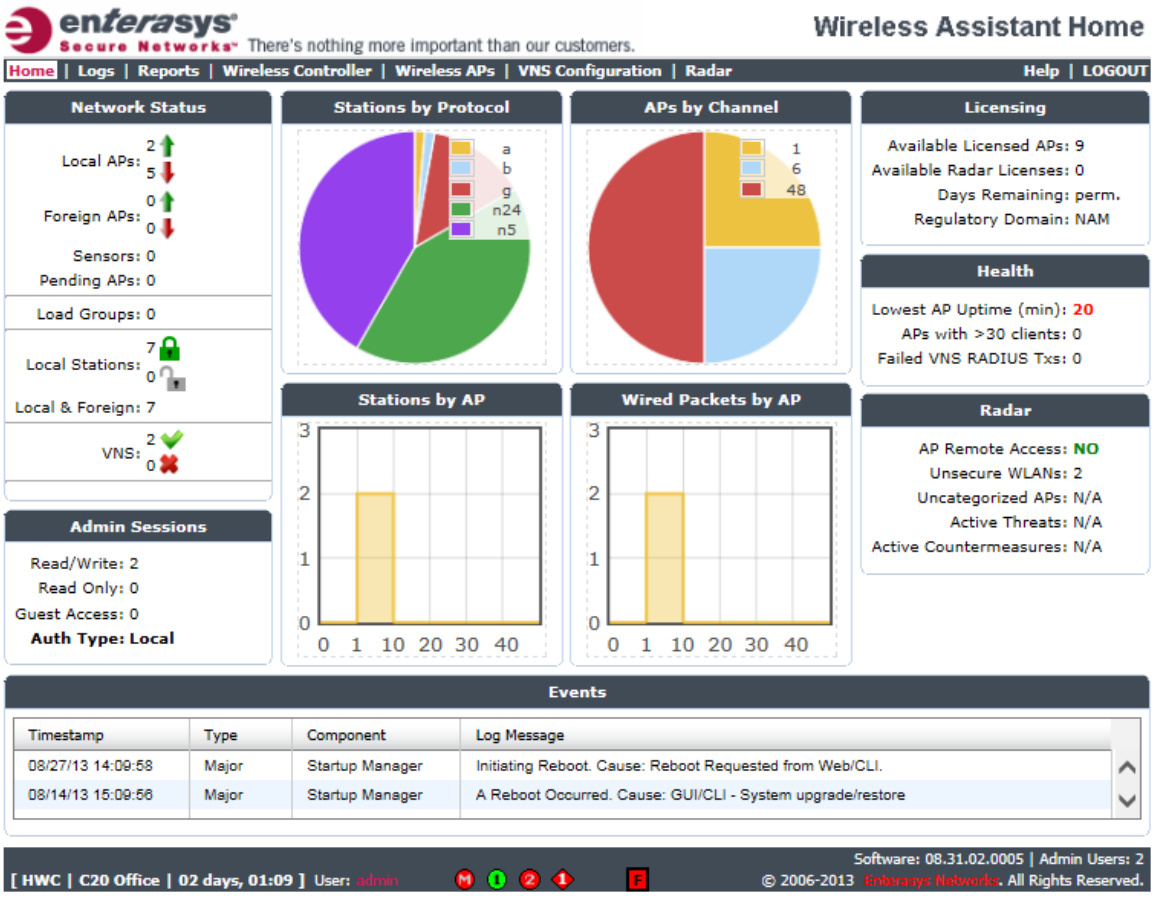
Keep in mind that security options and power save modes were adjusted according to requirements in individual test cases. Please refer to appendix A for information regarding device configuration.

APPENDIX A: TEST CONFIGURATIONS

Enterasys Wireless C20 Controller v. 08.31.02

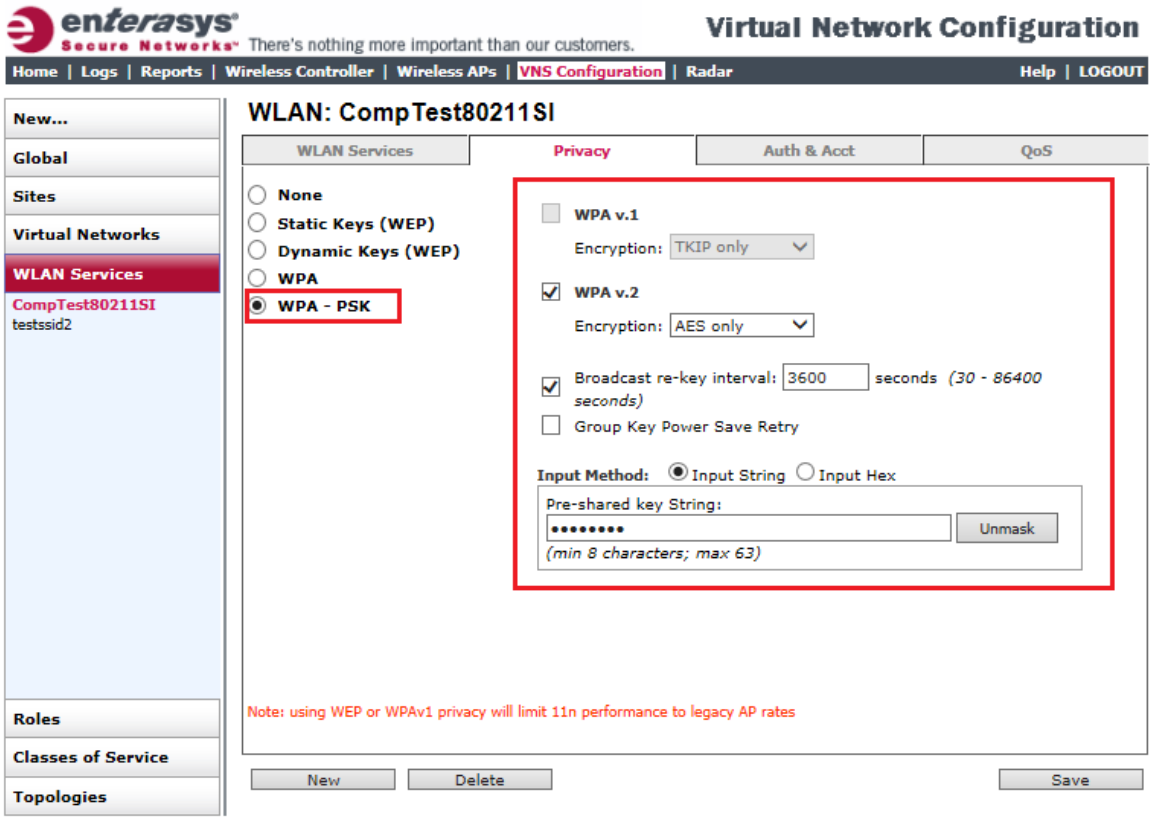
In the following chapter you will find screenshots and explanations of basic settings in order to get an Enterasys Wireless system to operate with an Ascom i62. Please note that security settings were modified according to requirements in individual test cases.

Overview



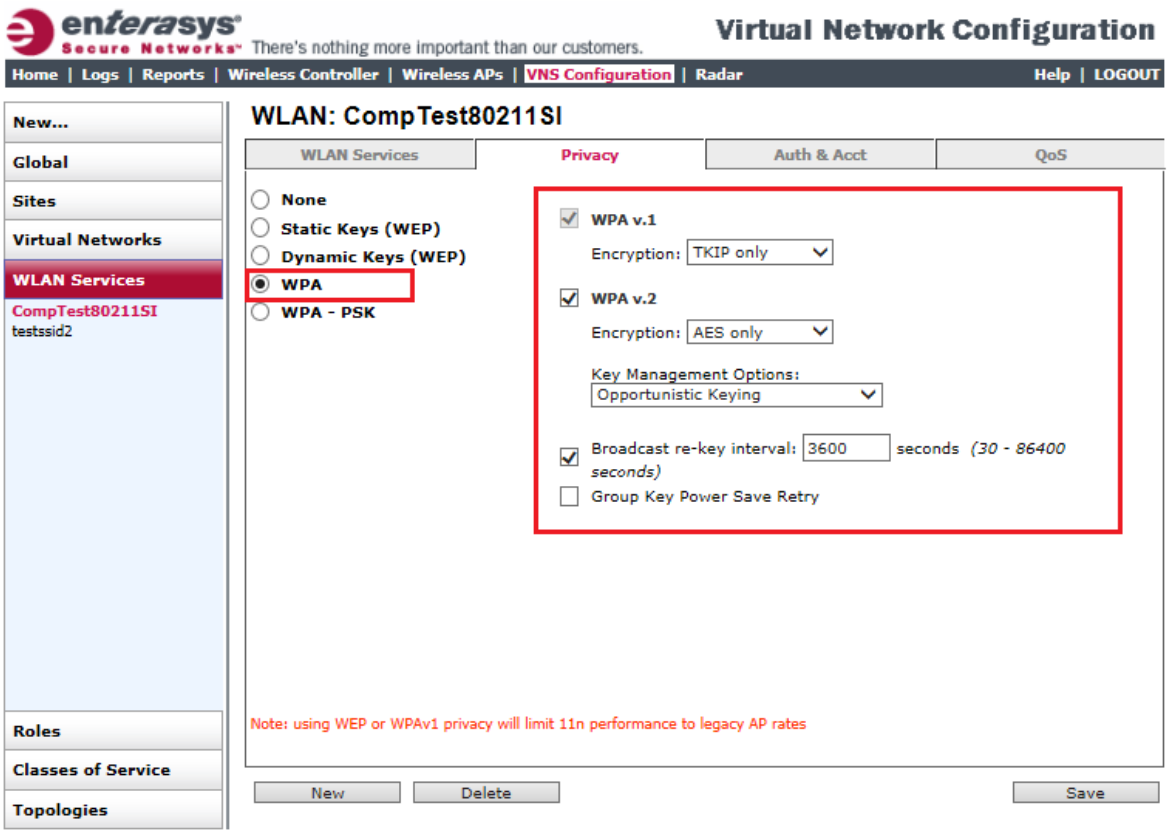
Enterasys controller overview.

Security settings (PSK)

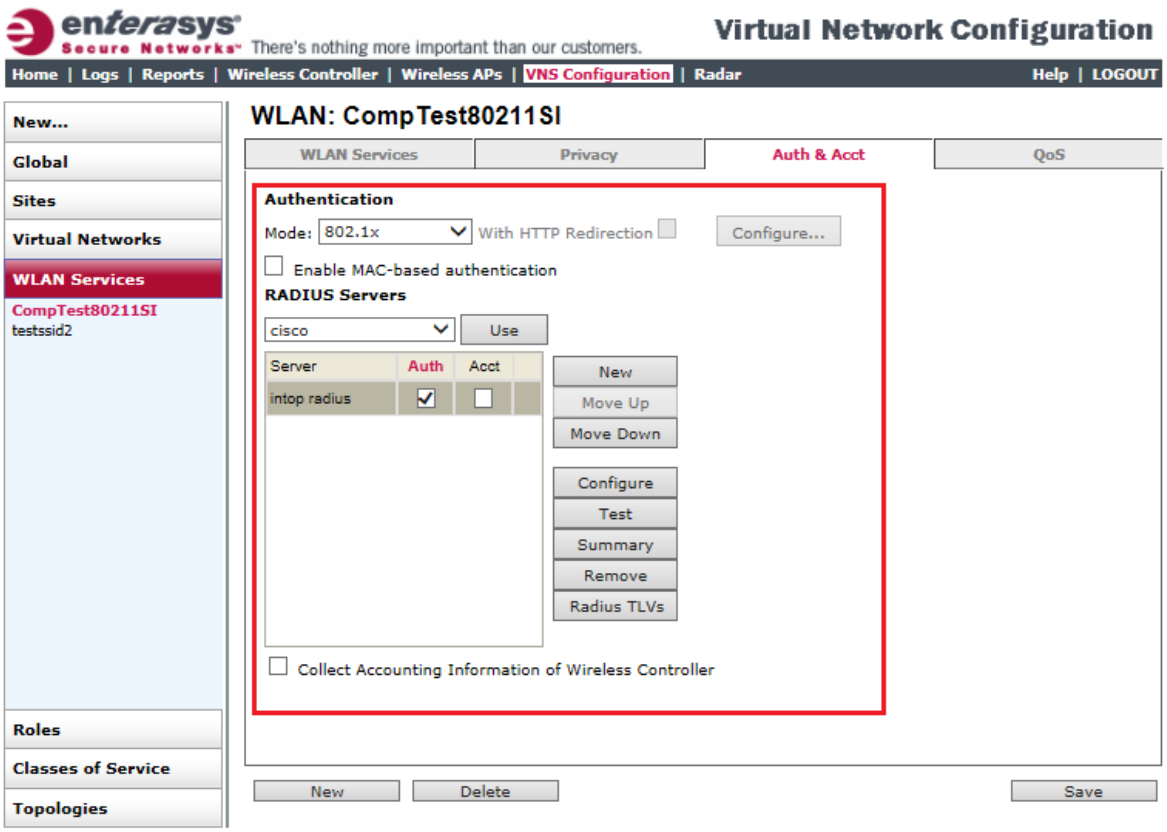


Security profile WPA2-PSK, AES encryption

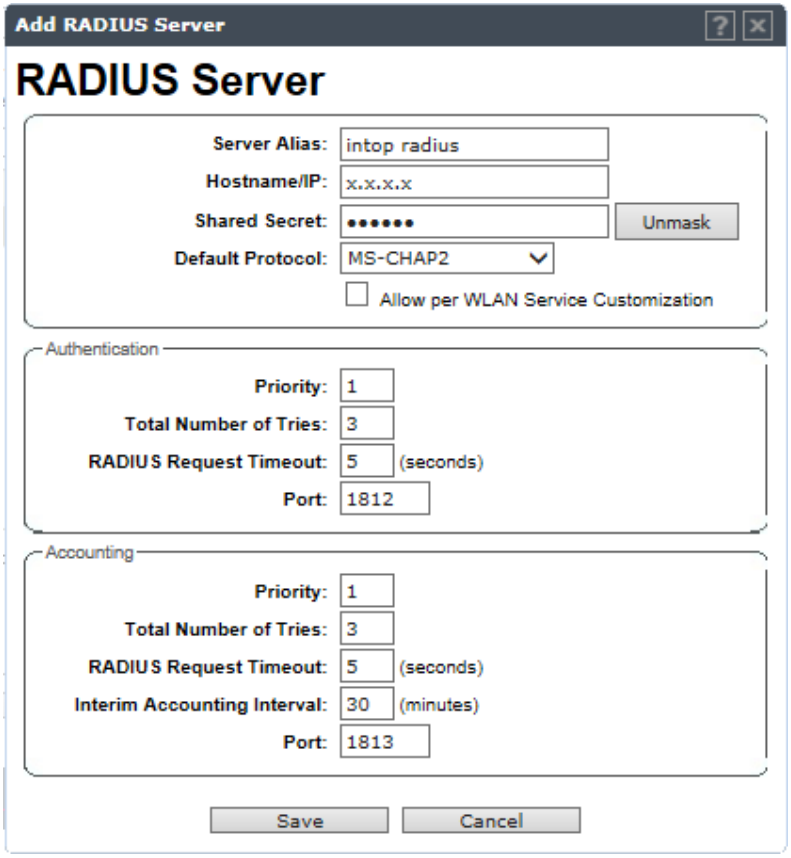
Security settings (802.1X / PEAP-MSCHAPv2)



Configuration of authentication using external Radius sever, 802.1X (Step 1). In this example is WPA2-AES/CCMP used. “Opportunistic Keying” is strongly recommended as Key Management Option in order to allow faster roaming between access points.



Configuration of authentication using external Radius sever (Step 2). Select the server to use. The server is created/configured in next step.

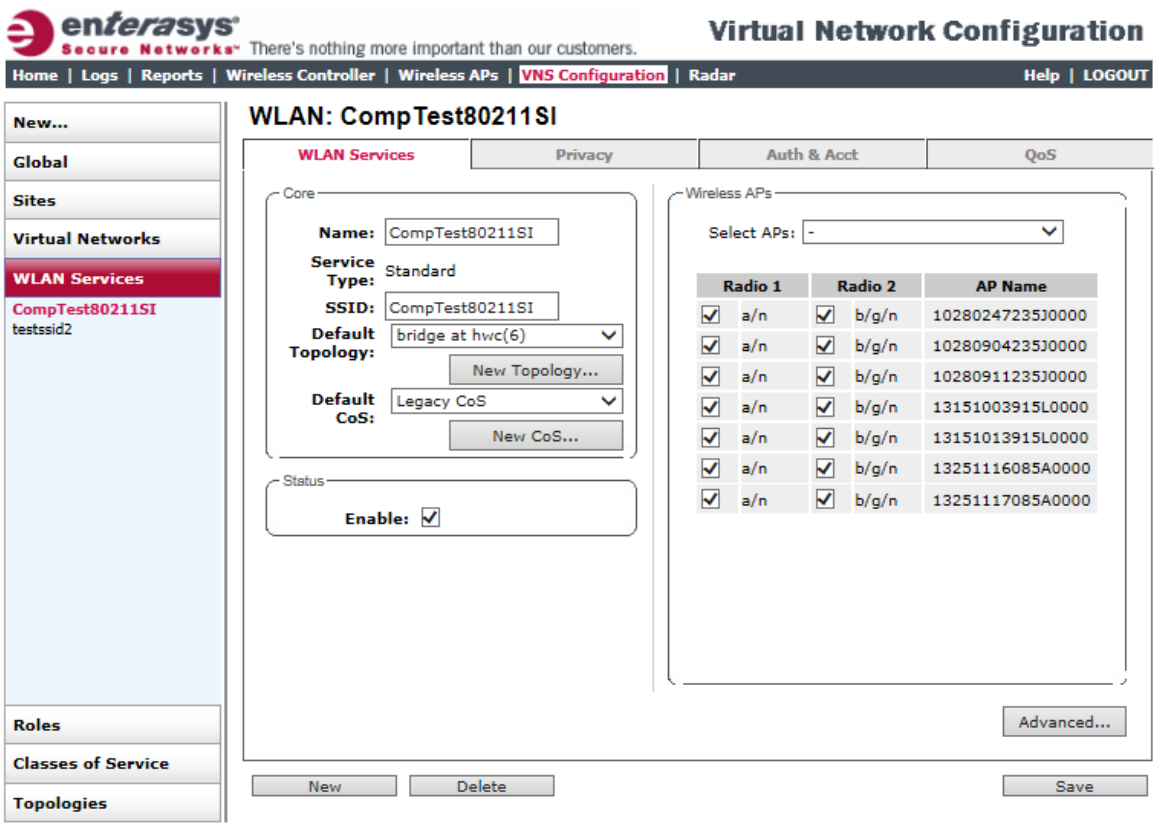


Configuration of authentication using external Radius sever (Step 3). The IP address and the secret must correspond to the IP and the credential used by the Radius server.

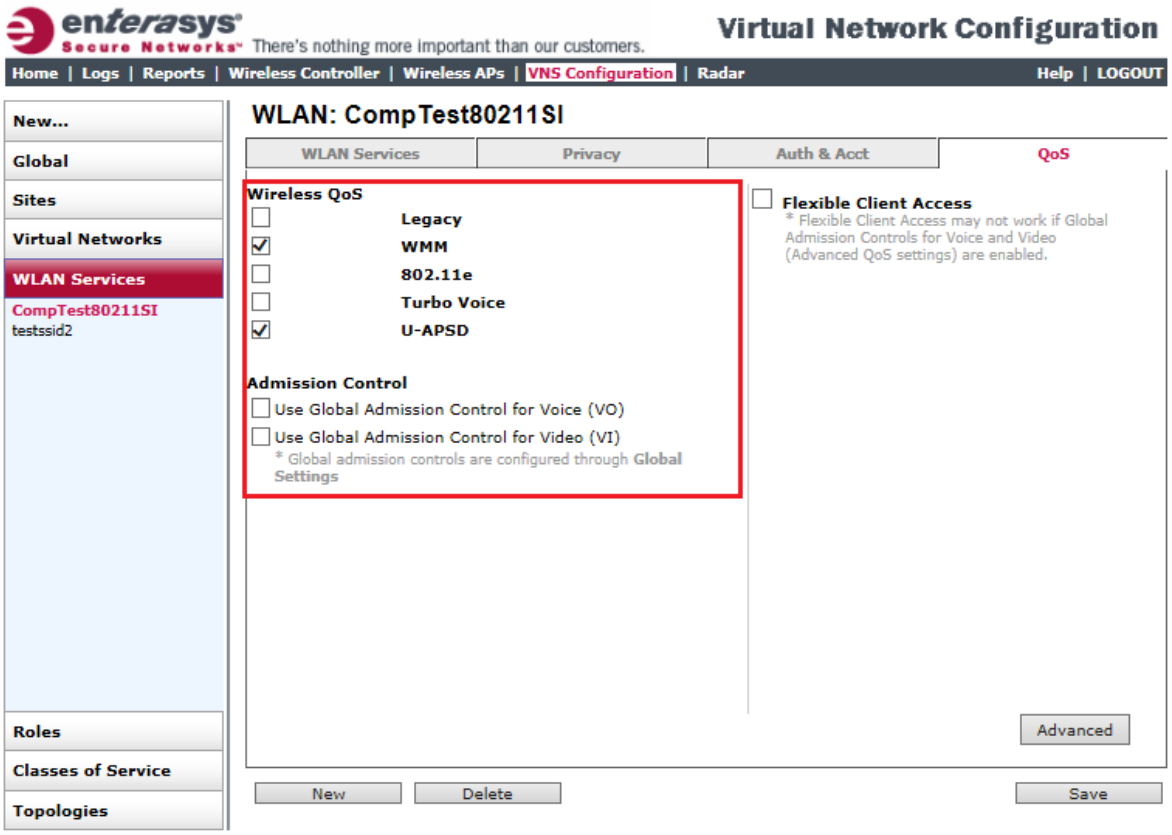
Note that depending on which Authentication method used it might be necessary to add a certificate into the i62. PEAP-MSCHAPv2 requires a Root certificate and EAP-TLS requires both a Root certificate and a client certificate. Server certificate validation can however be overridden in version 4.1.12 and above per handset setting.

Note. To enable fast inter-controller roaming with opportunistic key caching, the “pair” option under “Wireless controller -> availability” has to be enabled. Please consult Enterasys for details.

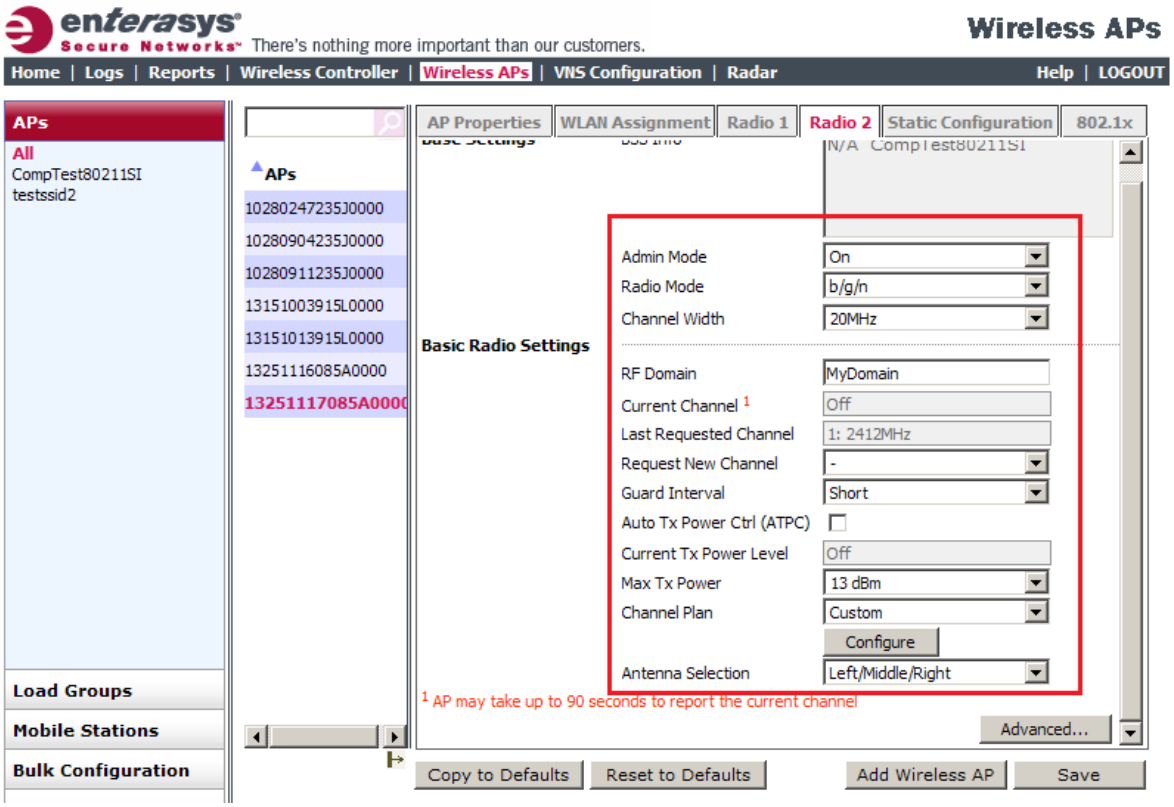
General settings (SSID, QoS, Radio)



General SSID settings.

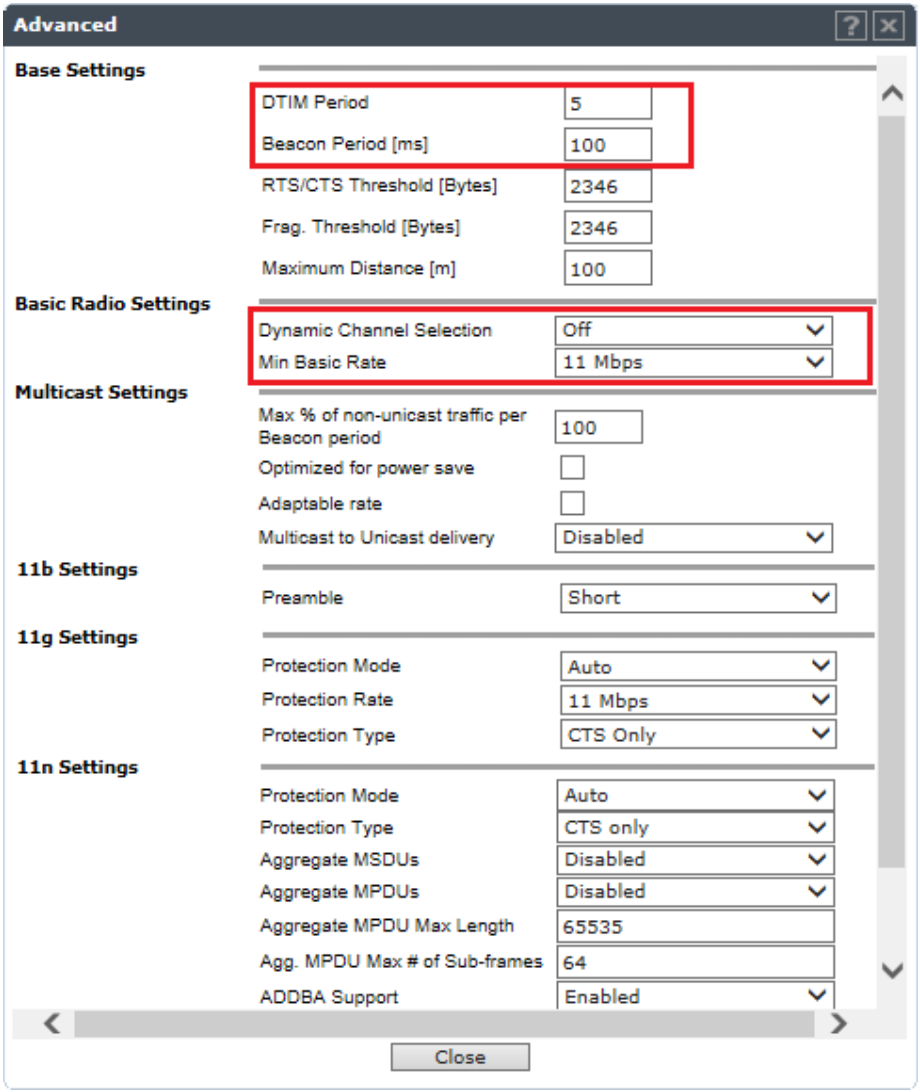


Make sure that WMM. In this example U-APSD is enabled which is strongly recommended in order to increase battery performance.



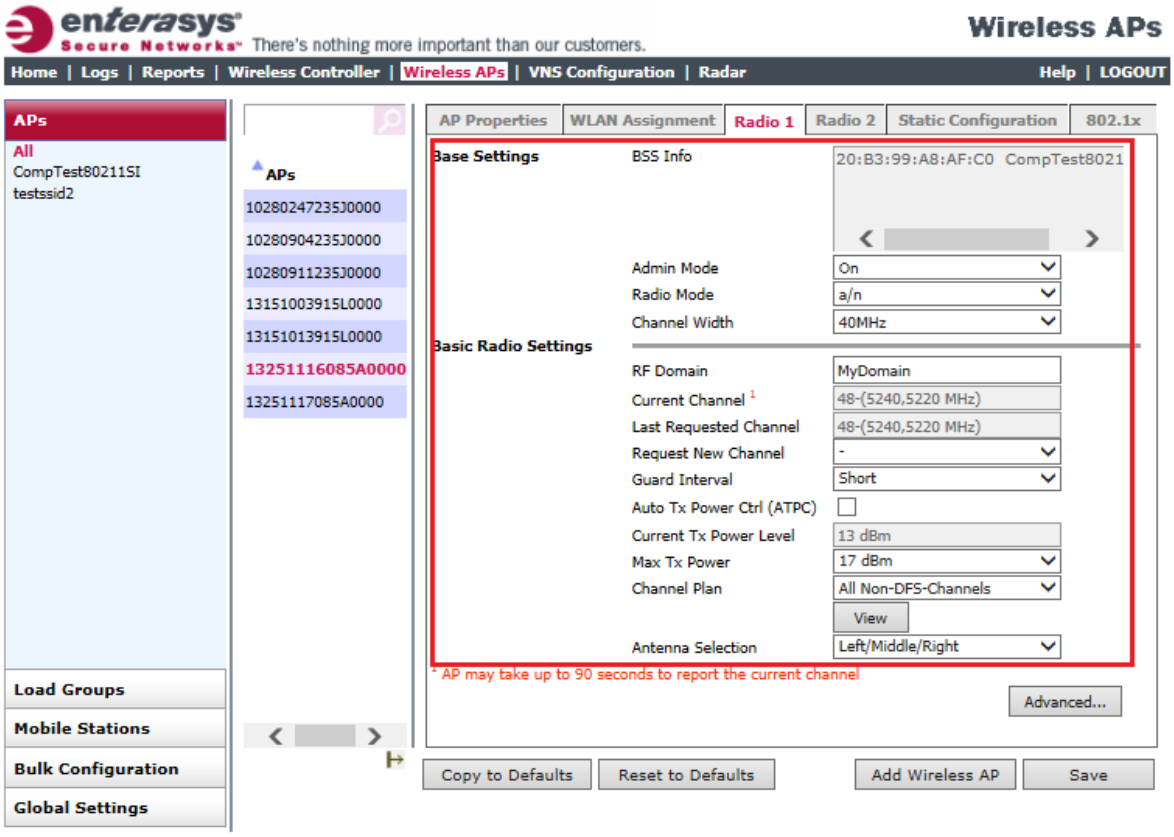
Ascom recommended settings for 802.11bgn are to use Custom channel plan and channel 1, 6 and 11. Due to the limited number of non-overlapping channels using 802.11bgn it is recommended to use 20MHz channel width.

Note that Tx Power was adjusted in order to test roaming.

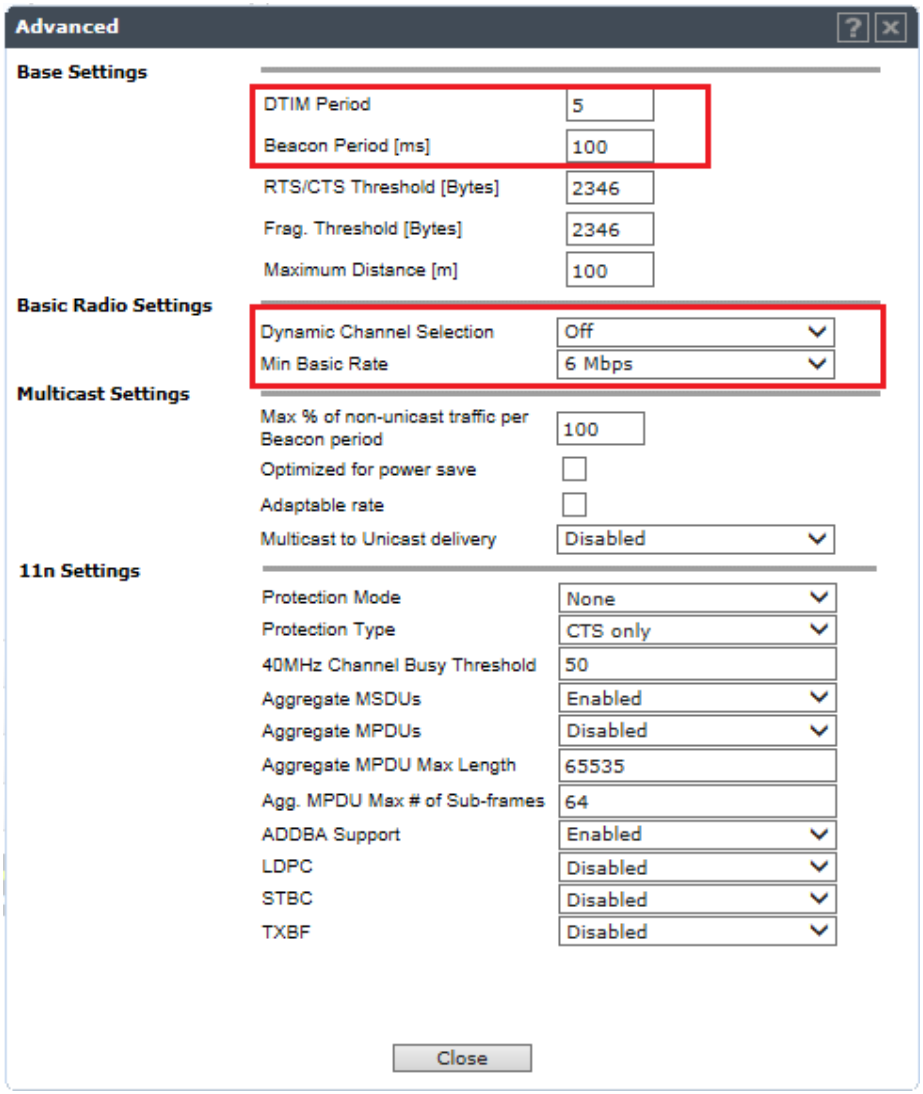


Radio 2 -> Advanced; Set DTIM period to value 5 and beacon period to 100ms. These values are recommended in order to allow maximum battery conservation without impacting the quality. A lower DTIM value is possible but will impact the standby time negatively.

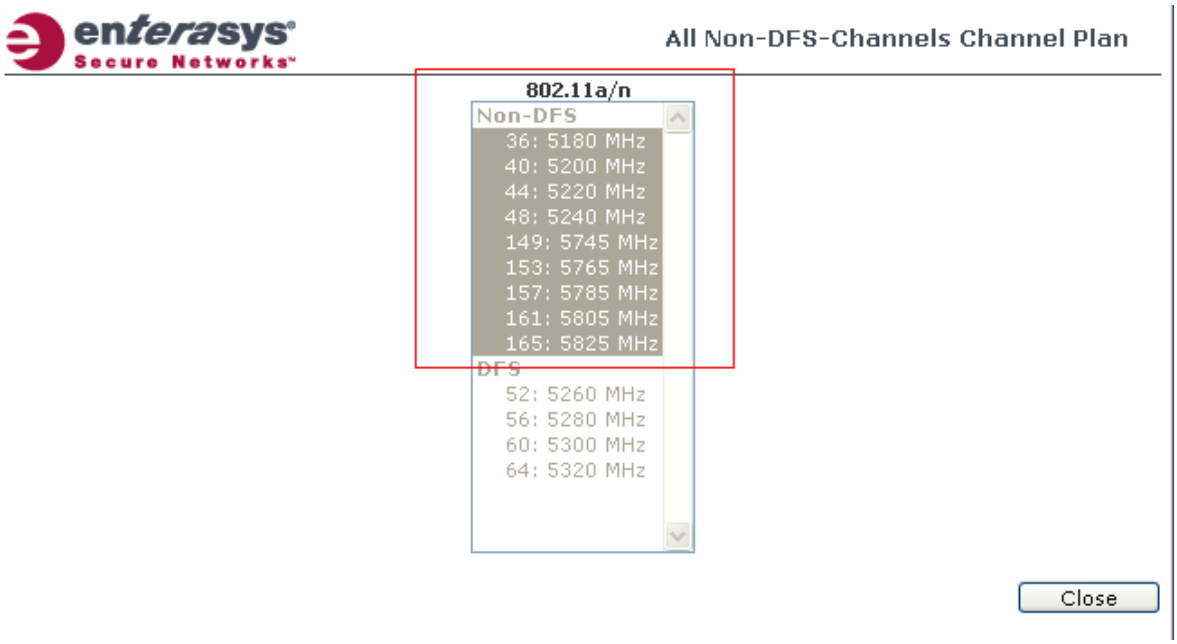
It is recommended to set the Min Basic Rate to 11Mbps to increase the performance.



Configuration of 802.11an: use channels according to the infrastructure manufacturer and country regulations.



Radio 1 -> Advanced; Set DTIM period to value 5 and beacon period to 100ms. These values are recommended in order to allow maximum battery conservation without impacting the quality. A lower DTIM value is possible but will impact the standby time negatively.



General guidelines when deploying Ascom i62 handsets (SW version 4.1.12 or later) in 802.11an 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.

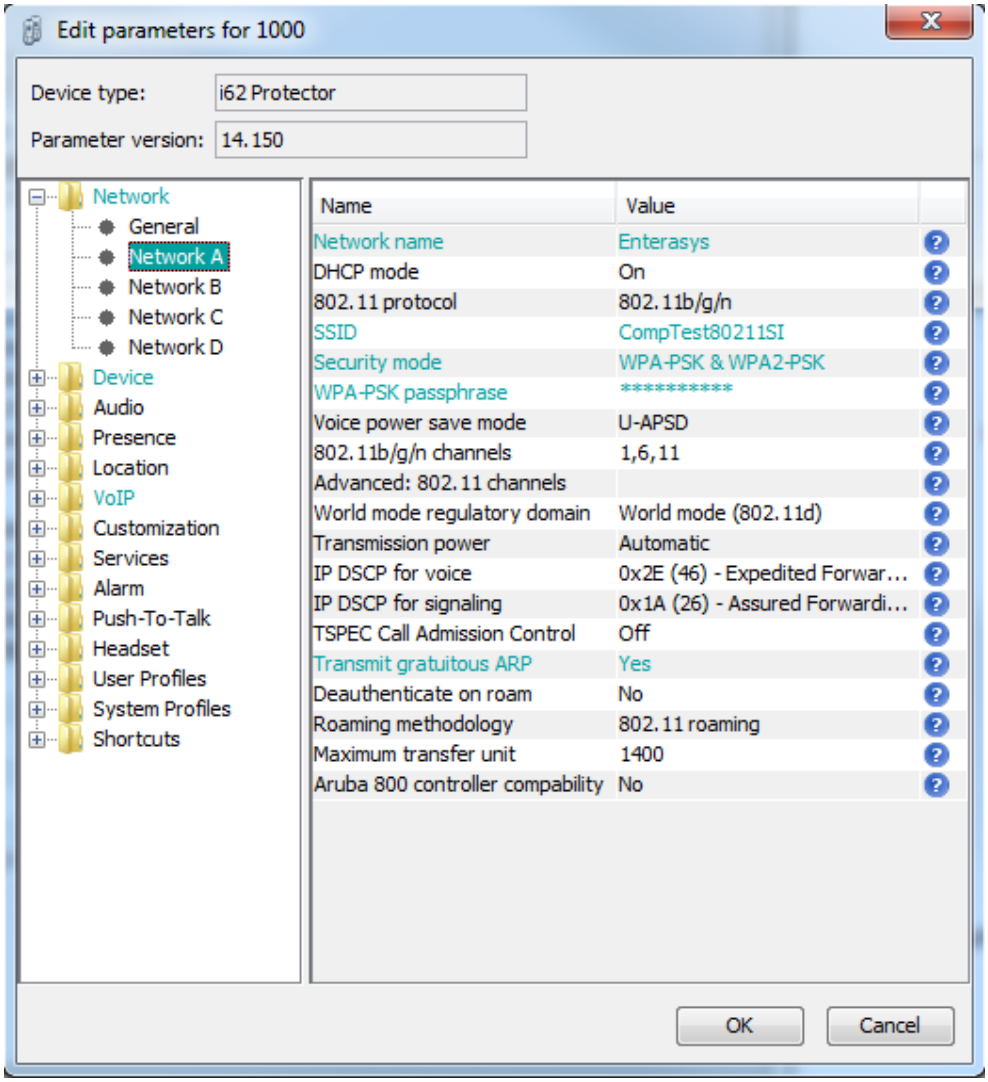
3. Make sure that all non-DFS channel are taken before resorting to DFS channels. The handset can cope in mixed non-DFS and DFS environments; however, due to "unpredictability" introduced by radar detection protocols, voice quality may become distorted and roaming delayed. Hence Ascom recommends avoiding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

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

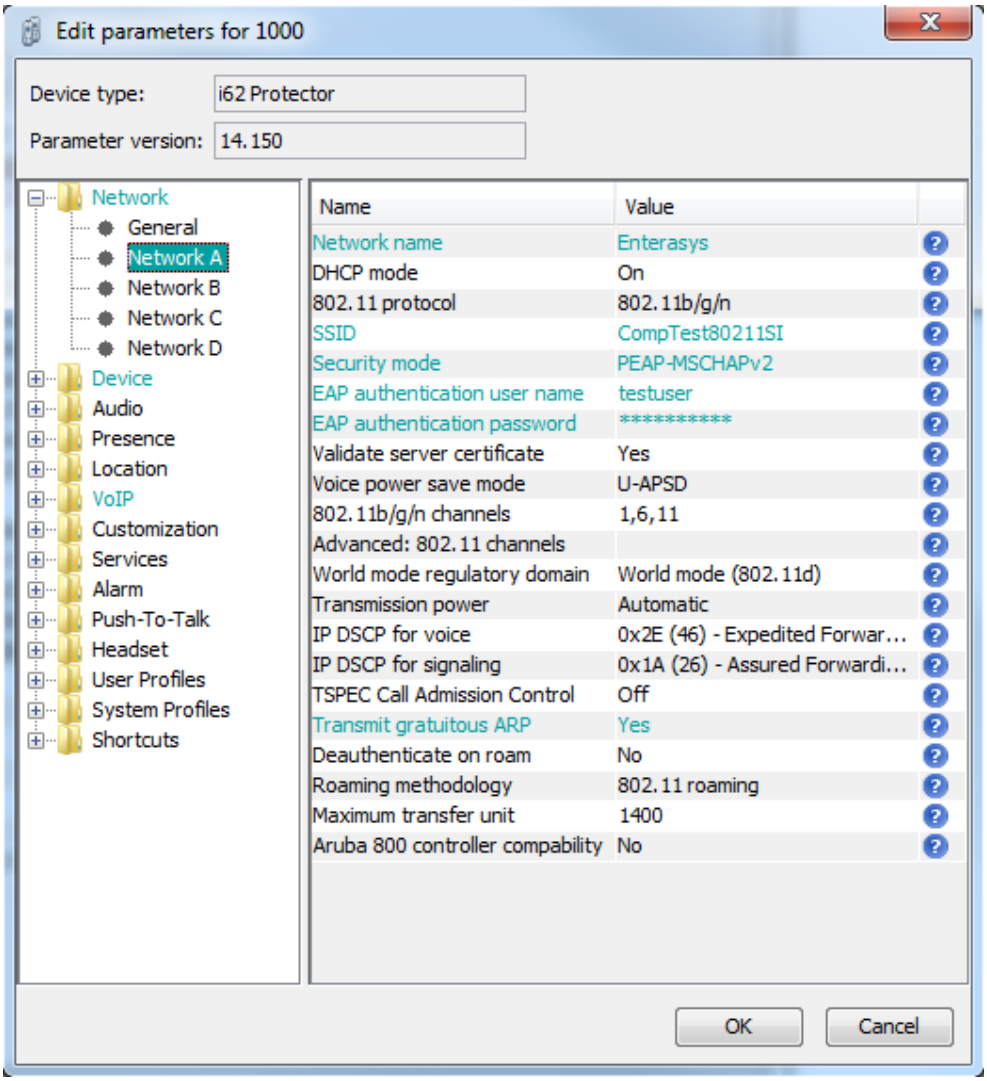
Controller configuration

See attached file (controller_config.cli) for controller configuration.

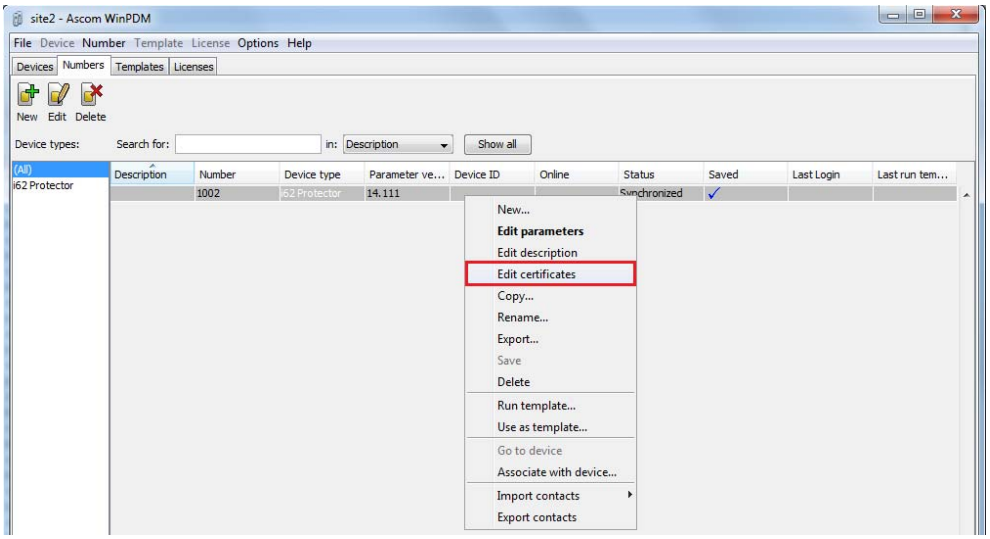
Ascom i62



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.

APPENDIX B: DETAILED TEST RECORDS

VoWIFI

Pass	26
Fail	0
Comments	2
Untested	5
Total	33

See attached file (WLANinteroperabilityTestReport_Enterasys.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
PA	2013-10-29	SEKMO	Draft 1
PB	2013-10-31	SEKMO	Minor changes after review. Draft2
R1	2013-11-11	SEKMO	Revision 1
R1a	2014-12-02	SEKMO	Added outdoor AP 3765/3767