

Interoperability Report

Ascom i62

Aruba

Mobility Controller Platform

Aruba AOS v. 6.5.4.0

Ascom i62 v. 5.5.0

Morrisville, NC, USA

October 2017

ascom

Contents

Introduction	3
About Ascom	3
About Aruba, a Hewlett Packard Enterprise company.....	3
Site Information	4
Verification site	4
Participants	4
Verification topology	4
Summary	5
General conclusions	5
Compatibility information	5
Verification overview.....	6
Known limitations.....	7
Appendix A: Verification Configurations	8
Aruba 7005 Controller, AOS 6.5.4.0	8
Appendix B: Detailed Verification Records	17
Document History	17

Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Aruba's platform, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Aruba's and Ascom's platform 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 Aruba, a Hewlett Packard Enterprise company

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

To learn more, visit Aruba at <http://www.arubanetworks.com> . For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at <http://community.arubanetworks.com> .

Site Information

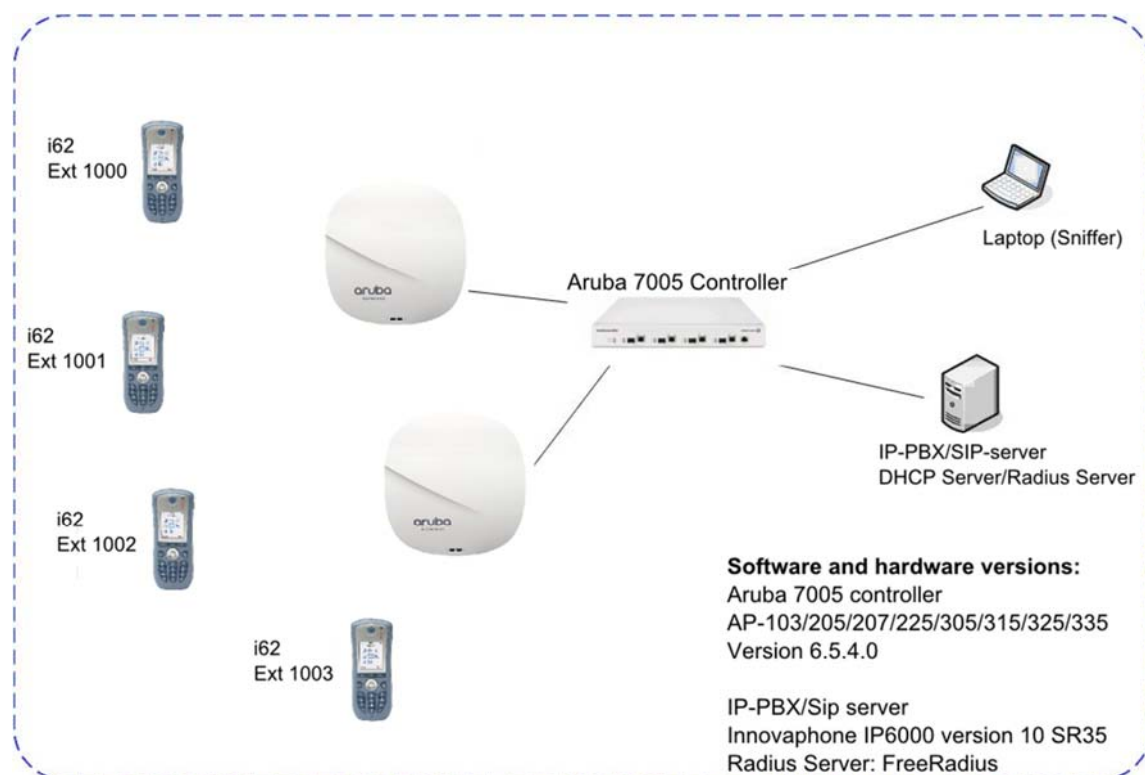
Verification site

Ascom US
300 Perimeter park drive
Morrisville, NC, US-27560
USA

Participants

Karl-Magnus Olsson, Ascom, Morrisville

Verification topology



Summary

General conclusions

The verification, including association, authentication, roaming, and load test produced very good results overall. Roaming times were in general good with roaming times of around 40-60ms both when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

Load testing showed that more than 12 Ascom i62 Handsets could maintain a call via a single Aruba access point when tested both in active and U-APSD modes. Note that 12 was the maximum number of devices tested and not the capacity limit.

Compatibility information

One Access point model from every product generation has been selected as a representation (AP-103, 205, 207, 225, 305, 315, 325 and 335). By testing these access points we are considered cover all major Aruba access points based on chipset compatibility.

Supported Partner Access Points with AOS version 6.5.4.0:

AP-103, 204, 205, 207, 214, 215, 224, 225, 275,

AP-304, 305, 314, 315, 324, 325, 334, 335

Supported Partner Controller Platforms with AOS version 6.5.4.0:

7000 series Mobility controllers

7200 series Mobility controllers

Verification overview

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	OK	
PMKSA Caching	OK	
WPA2-opportunistic/proactive Key Caching	OK	
WMM Prioritization	OK	
802.11 Power-save mode	OK	
802.11e U-APSD	OK	
802.11e U-APSD (load test)	OK	
Roaming, WPA2-PSK, AES Encryption	OK *	Typical roaming time 47 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK **	Typical roaming time 58 ms

*) Average roaming times are measured using 802.11a/n. Refer to Appendix B for detailed test results

* *) Measured times is with opportunistic/proactive Key Caching enabled (default enabled)

Known limitations

Description and Consequence	Workaround	Ticket(s) raised
Ascom i62 does not handle 802.11K info correctly which affects the roaming negatively.	Do not advertise the 802.11K capabilities for the Ascom i62 SSID.	
If call admission control is desired Ascom recommend using Aruba's proprietary Call Admission Control instead of WMM TSPEC. With this method the controller will interact by dropping the SIP invite when the maximum number of calls / maximum bandwidth is reached.		

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

For detailed verification results, refer to Appendix B: Detailed Verification Records.

Appendix A: Verification Configurations

Aruba 7005 Controller, AOS 6.5.4.0

This section includes screenshots and explanations of basic settings required to use Ascom i62 Handsets with an Aruba 7005 Mobility Controller. 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 this appendix.

General settings (SSID, Radio and QoS)

The screenshot shows the Aruba Cloud Services Controller configuration interface. The left sidebar contains a navigation menu with categories like WIZARDS, NETWORK, SECURITY, WIRELESS, and MANAGEMENT. The main content area is titled 'Configuration > AP Group > Edit "Interop"'. It displays the 'Profiles' section on the left and the 'Profile Details' section on the right. The 'Profile Details' section is for the 'SSID Profile > ArubaIntopPSK-ssid_prof'. It shows the 'Basic' tab with settings for 'SSID enable' (checked), 'ESSID' (ArubaIntopPSK), and 'Encryption' (wpa2-psk-aes). The 'Advanced' tab is also visible, showing 'DTIM Interval' set to 5 and '802.11a Basic Rates' and '802.11a Transmit Rates' with various checkboxes selected. A red box highlights the 'DTIM Interval' and the '802.11a' rate settings.

Profile	ArubaIntopPSK-aaa_prof	ArubaIntopPSK-ssid_prof	ArubaIntopPSK-ssid_prof
Wireless LAN			
Virtual AP			
ArubaIntopPSK-vap_prof			
ArubaIntopPSK-vap_prof			
AAA	ArubaIntopPSK-aaa_prof		
802.11X	default		
Hotspot 2.0			
SSID	ArubaIntopPSK-ssid_prof		
EDCA Parameters Station			
EDCA Parameters AP			
High-throughput SSID		ArubaIntopPSK-hthead_prof	
802.11r			
WMM Traffic Management			
Anyport			
ArubaIntop-vap_prof			
RF Management			
AP			
QoS			
IOS			
Mesh			

Profile Details	ArubaIntopPSK-ssid_prof
SSID enable	☒
ESSID	ArubaIntopPSK
Encryption	☐ opensystem ☐ static-wep ☐ dynamic-wep ☐ wpa-tkip ☐ wpa-aes ☐ wpa-psk-tkip ☐ wpa-psk-aes ☐ wpa2-aes ☒ wpa2-psk-aes ☐ wpa2-psk-tkip ☐ wpa2-tkip
Enable Management Frame Protection	☐
Require Management Frame Protection	☐
DTIM Interval	5 beacon periods
802.11a Basic Rates	☐ 6 ☐ 9 ☒ 12 ☐ 18 ☒ 24 ☐ 36 ☐ 48 ☐ 54
802.11a Transmit Rates	☐ 6 ☐ 9 ☒ 12 ☒ 18 ☒ 24 ☒ 36 ☒ 48 ☒ 54

Set DTIM Interval to 5. This value is recommended for maximum battery conservation without impacting call quality. Using a lower value will also decrease the standby time slightly.

CLOUD SERVICES CONTROLLER

Aruba7005

[Log out](#)

Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP

Configuration > AP Group > Edit "Interop"

Wireless LAN

Virtual AP

ArubaIntop1X-vap_prof

ArubaIntopPSK-vap_prof

AAA

ArubaIntopPSK-aaa_prof

802.11K

default

Hotspot 2.0

SSID

ArubaIntopPSK-ssid_prof

EDCA Parameters Station

default

EDCA Parameters AP

default

High-throughput SSID

ArubaIntopPSK-hssid_prof

802.11r

WMM Traffic Management

Anyspot

ArubaIntop-vap_prof

default

AlcatelPSK

RF Management

AP

QOS

IDS

Mesh

Profile Details

802.11g Basic Rates

☐ 1
☐ 2
☐ 5
☐ 6
☐ 9
☐ 11
☒ 12
☐ 36
☐ 18
☒ 24
☐ 48
☐ 54

802.11g Transmit Rates

☐ 1
☐ 2
☐ 5
☐ 6
☐ 9
☐ 11
☒ 12
☒ 18
☒ 24
☒ 36
☒ 48
☒ 54

Station Ageout Time

1000 sec

Max Transmit Attempts

4

RTS Threshold

2333 bytes

Short Preamble

☒

Max Associations

64

Wireless Multimedia (WMM)

☒

Wireless Multimedia U-APSD (WMM-UAPSD) Powersave

☒

WMM TSPEC Min Inactivity Interval

0 msec

Override DSCP mappings for WMM clients

☒

DSCP mapping for WMM voice AC (0-63)

46

DSCP mapping for WMM video AC (0-63)

26

DSCP mapping for WMM best-effort AC (0-63)

24

DSCP mapping for WMM background AC (0-63)

8

Ascom recommends disabling the lowest rates and recommends that 12mbits is set as the lowest basic rate.

Ensure that WMM and U-APSD are enabled. To match the default values in the i62 ensure to use DSCP 46 for Voice, 26 for video. The rest are left as default. It is also recommended that "Max Transmit Attempts" be set to 4.

aruba NETWORKS CLOUD SERVICES CONTROLLER | Aruba7005

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP
Bandwidth Calculator
Threshold
ADVANCED SERVICES

Configuration > AP Group > Edit "Interop"

Profiles	Profile Details
Wireless LAN	Hide SSID ☐
Virtual AP	Deny_Broadcast Probes ☐
ArubaIntop1X-vap_prof	Local Probe Request Threshold (dB) 0
ArubaIntopPSK-vap_prof	Auth Request Threshold (dB) 0
AAA	Disable Probe Retry ☒
802.11K	Battery Boost ☐
Hotspot 2.0	WEP Key 1 Retype:
SSID	WEP Key 2 Retype:
EDCA Parameters Station	WEP Key 3 Retype:
EDCA Parameters AP	WEP Key 4 Retype:
High-throughput SSID	WEP Transmit Key Index 1
802.11r	WPA Hexkey Retype:
WMM Traffic Management	WPA Passphrase Retype:
Anyspot	Maximum Transmit Failures 25
ArubaIntopPSK-aaa_prof	BC/MC Rate Optimization ☐
ArubaIntopPSK-ssid_prof	
ArubaIntopPSK-htssid_prof	
ArubaIntopPSK-htssid_prof	
RF Management	
AP	
QOS	
IDS	
Mesh	

Set "Maximum Transmit Failures" to 25.

aruba NETWORKS CLOUD SERVICES CONTROLLER | Aruba7005

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP
Bandwidth Calculator
Threshold
ADVANCED SERVICES

Configuration > AP Group > Edit "Interop"

Profiles	Profile Details
Wireless LAN	High-throughput SSID Profile > ArubaIntopPSK-htssid_prof
Virtual AP	Basic Advanced
ArubaIntop1X-vap_prof	General
ArubaIntopPSK-vap_prof	High throughput enable (SSID) ☒
AAA	40 MHz channel usage ☒
802.11K	Very High throughput enable (SSID) ☒
Hotspot 2.0	80 MHz channel usage (VHT) ☐
SSID	Transmit Beamforming
EDCA Parameters Station	VHT - Explicit Transmit Beamforming ☒
EDCA Parameters AP	Multi User Transmit Beamforming
High-throughput SSID	VHT - Multi User Transmit Beamforming ☐
802.11r	
WMM Traffic Management	

"High throughput enable" enables 802.11n capabilities that are supported in combination with Open encryption and WPA2-AES (PSK or Enterprise).

See page 14 for further additional recommendations on 11a/n/ac channel configuration.

aruba NETWORKS CLOUD SERVICES CONTROLLER | Aruba7005 [Log out](#)

Dashboard Monitoring **Configuration** Diagnostics Maintenance [Save Configuration](#)

WIZARDS
 AP
 Controller
 Campus WLAN
 Remote AP
 AirWave
 NETWORK
 Controller
 VLANs
 Ports
 IP
 SECURITY
 Authentication
 Access Control
 WIRELESS
 > **AP Configuration**
 AP Installation
 MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator
 Threshold
 ADVANCED SERVICES
 Redundancy

Configuration > AP Group > Edit "Interop"

Profiles	Profile Details
- Wireless LAN - RF Management 802.11a radio ch 36 - Adaptive Radio Management (ARM) default-a - High-throughput Radio default-a - AM Scanning default 802.11g radio default - RF Optimization default - RF Event Thresholds default - AP - QoS - IDS - Mesh	802.11a radio profile > ch 36 Show Reference Save As Reset Basic Advanced Radio enable ☒ Mode ap-mode High throughput enable (radio) ☒ Very high throughput enable (radio) ☒ Channel 36 Channel Width: ☒ 20MHz ☐ 40MHz ☐ 80MHz ☐ 80+80MHz ☐ 160MHz Transmit EIRP 13.0 Non-Wi-Fi Interference Immunity 2 Spur Immunity 0 Enable CSA ☐ CSA Count 4 Smart Antenna ☐ Advertise 802.11d and 802.11h Capabilities ☒ Spectrum Load Balancing ☐ Beacon Period 100 msec Beacon Regulate ☐ Advertized regulatory max EIRP 0 ARM/WIDS Override OFF Reduce Cell Size (Rx Sensitivity) 0 dB Energy Detect Threshold Offset 0 dB Management Frame Throttle Interval 1 sec

Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities. 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.

General guidelines when deploying Ascom i62 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)

Encryption and Authentication Settings

Configuration > AP Group > Edit "Interop"

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General

Profiles

Wireless LAN	
Virtual AP	
ArubaIntop1X-vap_prof	
ArubaIntopPSK-vap_prof	
AAA	ArubaIntopPSK-aaa_prof
802.11K	default
Hotspot 2.0	
802	ArubaIntopPSK-802_prof
EDCA Parameters Station	default
EDCA Parameters AP	
High-throughput SSID	ArubaIntopPSK-h2aid_prof
802.11r	
WMM Traffic Management	

Profile Details

SSID Profile > ArubaIntopPSK-ssid_prof

Show Reference Save As Reset

Basic Advanced

Network Name (SSID) ArubaIntopPSK

802.11 Security

Network Authentication ☐ None ☐ 802.1X/WEP ☐ WPA2 ☒ WPA2-PSK

Encryption ☒ AES

Keys

PSK AES Key/Passphrase *****

Confirm Key/Passphrase *****

Format PSK Passphrase

The PSK AES Hex Key should be a 64 character hexadecimal string
The PSK AES Passphrase should be an ASCII string 8-63 characters in length

WPA2-PSK. Set the security profile to WPA2-PSK, AES encryption.

Security > Authentication > Servers

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning

Servers

AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group

RADIUS Server

freeRADIUS

LDAP Server

Internal DB

Tacacs Accounting Server

TACACS Server

XML API Server

RFC 3576 Server

Windows Server

RADIUS Server > freeRADIUS

Show Reference Save As Reset

Host 192.168.0.2

Key *****

Retype: *****

CPPM credentials

cpm_username

cpm_password Retype:

Auth Port 1812

Acct Port 1813

Radius Port 2083

Retransmits 3

Timeout 5 sec

NAS ID

NAS IP

Enable IPv6

NAS IPv6

Source Interface vlanid

ipvsaddr

Enterprise/.1X authentication.

Step 1: When configuring the authentication mode using a Radius server, the IP address and the Key must correspond to the IP address and the credential used by the Radius server. The RADIUS server should be added to a Server Group.

Security > Authentication > Profiles

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration

Profiles

AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA

ArubaIntop-aaa_prof

ArubaIntop1X-aaa_prof

MAC Authentication

MAC Authentication Server Group default

802.1X Authentication dot1x_prof-0k043

802.1X Authentication Server ArubaIntop1X-802p-Group ng88

RADIUS Accounting Server Group

XML API server

RFC 3576 server

ArubaIntopPSK-aaa_prof

802.1X Authentication Profile > dot1x_prof-0k043

Show Reference Save As Reset

Basic Advanced

Max authentication failures 0

Enforce Machine Authentication ☒

Machine Authentication: Default Machine Role voice

Machine Authentication: Default User Role voice

Reauthentication ☐

Termination ☐

Termination EAP-Type ☐ eap-tls ☐ eap-peap

Termination Inner EAP-Type ☐ eap-mschapv2 ☐ eap-gtc

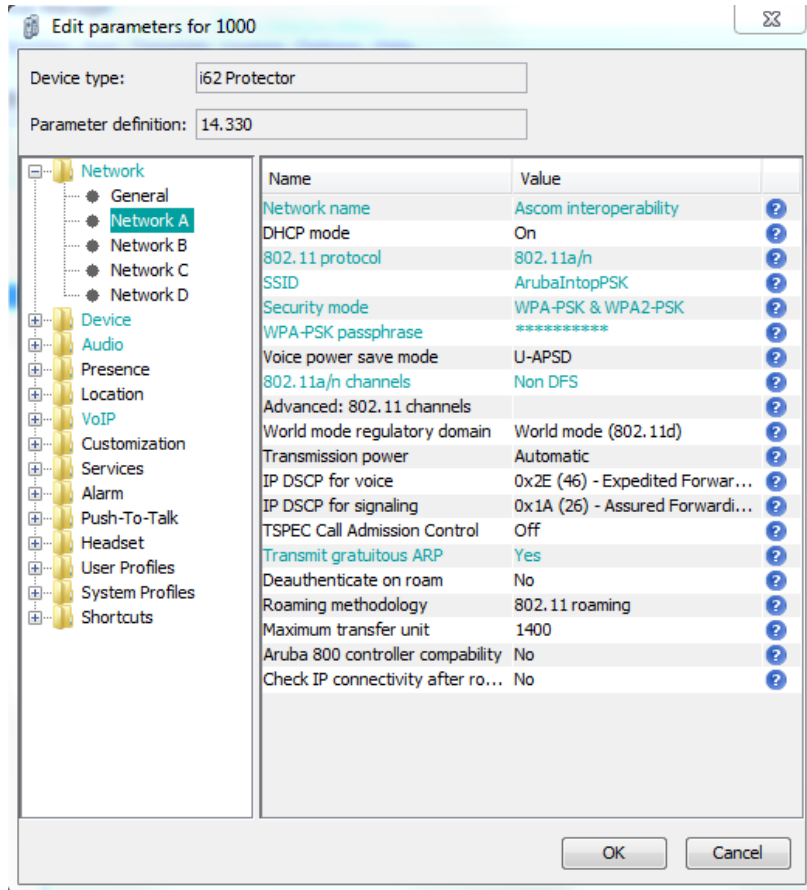
Step 2: Create an 802.1X Authentication Profile.



Step 3: Choose the 802.1X Authentication profile created in previous step and configure the Authentication Server group.

Choose configured AAA Profile and set WPA2/AES as the security mode.

See Appendix B for the controller configuration used for the certification process.



Network settings for WPA2-PSK

- Select frequency band according to system setup (here 802.11a/n)
- Select only the channels used in the system. In this example Non DFS (UNII1 and 3)

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to "USA". Consider the known issues chapter.

Edit parameters for 1000

Device type: i62 Protector

Parameter definition: 14.330

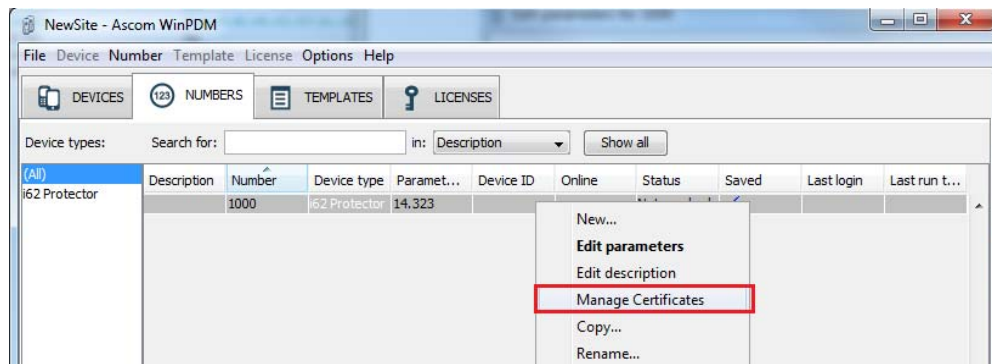
Name	Value	
Network name	Ascom interoperability	?
DHCP mode	On	?
802.11 protocol	802.11a/n	?
SSID	ArubaIntop1X	?
Security mode	PEAP-MSCHAPv2	?
EAP authentication identity	testuser	?
EAP authentication password	*****	?
EAP anonymous identity		?
EAP client certificate	None	?
Validate server certificate	Yes	?
Voice power save mode	U-APSD	?
802.11a/n channels	Non DFS	?
Advanced: 802.11 channels		?
World mode regulatory domain	World mode (802.11d)	?
Transmission power	Automatic	?
IP DSCP for voice	0x2E (46) - Expedited Forward...	?
IP DSCP for signaling	0x1A (26) - Assured Forwardi...	?
TSPEC Call Admission Control	Off	?
Transmit gratuitous ARP	Yes	?
Deauthenticate on roam	No	?
Roaming methodology	802.11 roaming	?
Maximum transfer unit	1400	?
Aruba 800 controller compability	No	?
Check IP connectivity after ro...	No	?

OK Cancel

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

- Select frequency band according to system setup (here 802.11a/n)
- Select only the channels used in the system. In this example Non DFS (UNII1 and 3)

Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to "USA". Consider the known issues chapter.



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

Note that both a root and a client certificate are needed for TLS. Otherwise only a CA certificate is needed. Server certificate validation can be overridden in version 4.1.12 and above per handset setting (Validate server certificate under Network settings).

Appendix B: Detailed Verification Records

Pass	18
Fail	0
Comments	2
Not verified	1
Total	21

Refer to the attached file for detailed verification results.

Refer to the verification specification for explicit information regarding each verification case.

The specification can be found here (requires login):

<https://www.ascom-ws.com/AscomPartnerWeb/en/startpage/Sales-tools/Interoperability/Templates/>

Document History

Rev	Date	Author	Description
R1	7 November 2017	SEKMO	Revision R1. AOS 6.5.4.0