

Interoperability Report

Ascom i62

Aruba

Mobility Controller Platform

Aruba AOS v. 8.4.0.1

Ascom i62 v. 6.1.0

Morrisville, NC, USA

May 2019

ascom

Contents

Introduction.....	3
About Ascom.....	3
About Aruba, a Hewlett Packard Enterprise company	3
Site Information	4
Validation site.....	4
Participants	4
Validation topology	4
Summary	5
General conclusions.....	5
Compatibility information	5
Validation overview	6
Known limitations	7
Appendix A: Validation Configurations.....	8
Aruba 7005 Controller, AOS 8.4.0.1.....	8
Appendix B: Detailed Validation Records	21
Document History.....	21

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

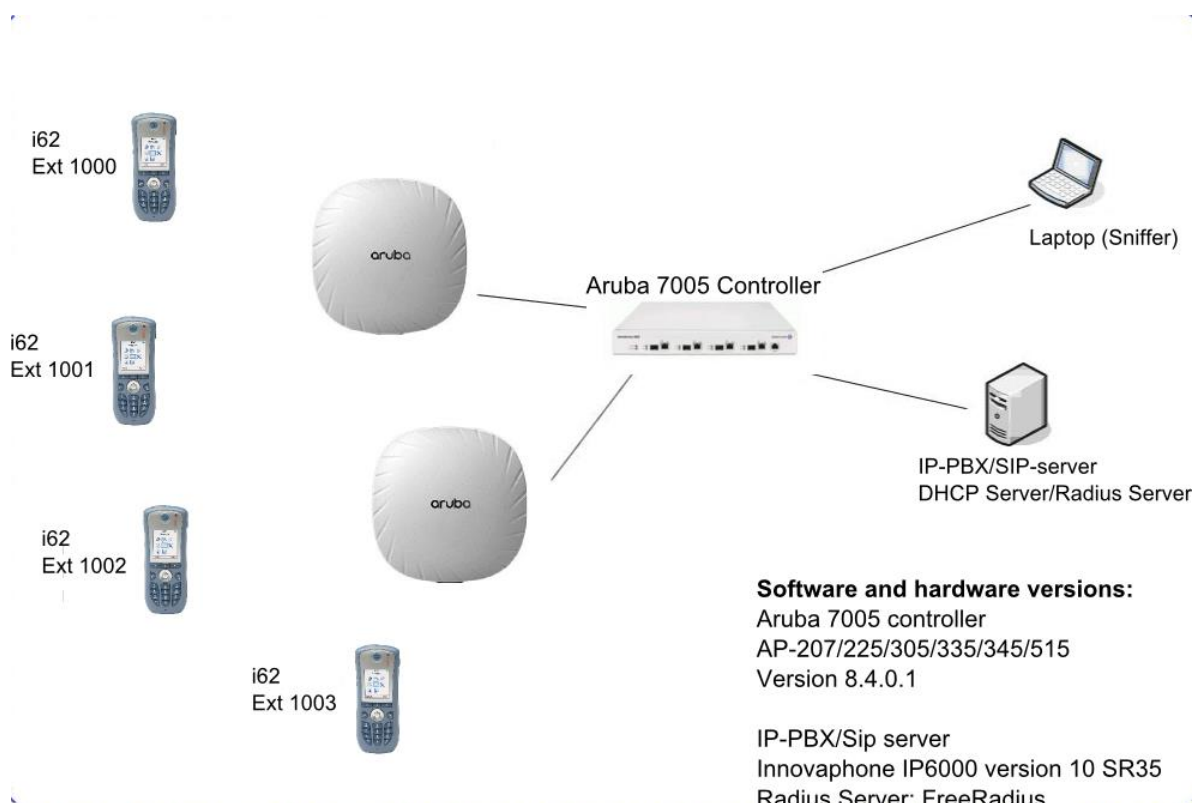
Validation site

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

Participants

Karl-Magnus Olsson, Ascom, Morrisville

Validation 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.

ArubaOS 8.x replaces Call Admission Control with Intelligent Call Handling (ICH). ICH monitors the channel utilization of all radios of the APs on the managed device. If the channel utilization exceeds beyond a configurable threshold on a radio, new UCC calls are not prioritized. This is to ensure that existing calls on the radio are not penalized due to a new call when channel utilization is very high. ICH is enabled by default and applies to all ALGs supported by UCM. These features have not been included in the test

Compatibility information

One Access point model from every product generation has been selected as a representation (AP-207, 225, 305, 335, 345 and 515). 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 8.4.0.1:

AP-207, 214, 215, 224, 225, 275

AP-304, 305, 314, 315, 324, 325, 334, 335, 344, 345, 514, 515

Supported Partner Controller Platforms with AOS version 8.4.0.1:

7000 series Mobility controllers

7200 series Mobility controllers

Validation 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 44 ms
Roaming, PEAP-MSCHAPv2 Auth, AES Encryption	OK **	Typical roaming time 55 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
<p>AP-510 series is currently unable to modify the data rate sets from default. It's therefor not possible to disable the lowest data rates such as 1, 2 and 5.5 Mbps on 2.4GHz.</p> <p>Refer to HPE/Aruba release notes for details.</p>		
<p>For the 802.11d "Country Information" element to be broadcasted on non DFS channels its necessary to have 802.11k enabled. This is important for regions utilizing "world mode" regulatory domain,</p> <p>The default 11k profile enables "Quiet IE" to be broadcasted. This causes the Ascom device to function poorly with frequently disconnects. It is therefore critical to modify the 802.11k profile and disable "Quiet IE". Refer to configuration settings in this document.</p>	<p>Enable 802.11k but disable "Advertise Quiet IE"</p>	<p>Ascom ticket MRS-290</p>
<p>Due to RF environment it was noted that voice quality and connection stability was generally poor on 2.4GHz radio.</p> <p>This has likely nothing to do with the infrastructure and client interoperability but is rather a result of a congested frequency band.</p> <p>It's suggested to avoid using 2.4GHz RF band for voice if possible. .</p>		

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

For detailed validation results, refer to Appendix B: Detailed Validation Records.

Appendix A: Validation Configurations

Aruba 7005 Controller, AOS 8.4.0.1

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 Mobility Controller web interface for the 'ArubaintopPSK' SSID profile. The 'DTIM Interval' is set to 5. The '802.11a Basic Rates' and '802.11g Basic Rates' are configured with specific checkboxes. The '802.11a Transmit Rates' and '802.11g Transmit Rates' are also configured with specific checkboxes. The 'Station Ageout Time' is set to 1000, 'Max Transmit Attempts' is set to 4, and 'RTS Threshold' is set to 2333 bytes.

DTIM Interval:	5	beacon periods
802.11a Basic Rates:	<input type="checkbox"/> 6	<input type="checkbox"/> 9
802.11a Transmit Rates:	<input type="checkbox"/> 6	<input type="checkbox"/> 9
802.11g Basic Rates:	<input type="checkbox"/> 1	<input type="checkbox"/> 2
802.11g Transmit Rates:	<input type="checkbox"/> 1	<input type="checkbox"/> 2

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.

Note. Not all HPE Aruba AP models support DTIM 5.

MOBILITY CONTROLLER
Aruba7005

ACCESS POINTS
1 5

CLIENTS
7

ALERTS
0

Mobility Controller > Aruba7005

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
System
Tasks
Diagnostics
Maintenance

GeneralAdminAirWaveCPSecCertificatesSNMPLoggingProfilesWhitelistMore

Station Ageout Time:1000

Max Transmit Attempts:4

RTS Threshold:2333bytes

Short Preamble:☒

Max Associations:64

Wireless Multimedia (WMM):☒

Wireless Multimedia U-APSD (WMM-UAPSD) Powersave:☒

WMM TSPEC Min Inactivity Interval:0msec

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):0

WMM Access Class of EAP traffic:voice

Multiple Tx Replay Counters:☒

Hide SSID:☐

Deny_Broadcast Probes:☐

Ascom recommends disabling the lowest rates and recommends that 12Mbps 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 MOBILITY CONTROLLER Aruba7005

ACCESS POINTS 1 5 CLIENTS 7 ALERTS 0

Mobility Controller > Aruba7005

Dashboard Configuration

General Admin AirWave CPsec Certificates SNMP Logging Profiles Whitelist More

Profiles

Disable Probe Retry: ☒

Battery Boost: ☐

WEP Key 1: WEP key 1:

Retype:

WEP Key 2: WEP key 2:

Retype:

WEP Key 3: WEP key 3:

Retype:

WEP Key 4: WEP key 4:

Retype:

WEP Transmit Key Index:

WPA Hexkey: WPA hexkey:

Retype:

WPA Passphrase: WPA passphrase:

Retype:

Maximum Transmit Failures:

BC/MC Rate Optimization: ☐

Rate Optimization for delivering EAPOL frames: ☒

Strict Spectralink Voice Protocol (SVP): ☐

Set “Maximum Transmit Failures” to 25.

Aruba MOBILITY CONTROLLER Aruba7005

ACCESS POINTS 1 5 CLIENTS 7 ALERTS 0

Mobility Controller > Aruba7005

Dashboard Configuration

General Admin AirWave CPsec Certificates SNMP Logging Profiles Whitelist More

Profiles

All Profiles

High-throughput SSID profile: default

High-throughput SSID profile: default

General

High throughput enable (SSID): ☒

40 MHz channel usage: ☒

Very High throughput enable (SSID): ☒

80 MHz channel usage (VHT): ☐

Multi User Transmit Beamforming

Transmit Beamforming

Advanced

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

See page 12 for further additional recommendations on 11a/n/ac channel configuration.

The screenshot shows the Aruba Mobility Controller interface for Aruba7005. The left sidebar contains navigation options: Dashboard, Configuration (highlighted), WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, System, Tasks, Diagnostics, and Maintenance. The main panel is titled 'Profiles' and shows a list of 'All Profiles' on the left, including 802.11r, EDCA Parameters (AP), EDCA Parameters (Station), High-throughput SSID, and default. The right panel shows the configuration for the '802.11r Profile: default'. The settings are: 802.11r Profile: default, Advertise 802.11r Capability: ☐, 802.11r Mobility Domain ID: 1, and 802.11r R1 Key Duration: 3600.

802.11r is not supported by Ascom i62 but the device have no problem operating on a SSIDs were 802.11r (FT) is advertised in conjunction with a legacy method.

The screenshot shows the Aruba Mobility Controller interface for Aruba7005. The left sidebar is the same as the previous screenshot. The main panel is titled 'Profiles' and shows a list of 'All Profiles' on the left, including 5 GHz radio, Ascom_radio_a_ui, Adaptive Radio Management (ARM), AM Scanning, High-throughput radio, default, rp-maintain-a, and rp-monitor-a. The right panel shows the configuration for the '5 GHz radio profile: Ascom_radio_a_ui'. The settings are: Transmit EIRP: 15 dBm, Spur Immunity: 0, Enable CSA: ☐, CSA Count: 4, Smart Antenna: ☐, Advertise 802.11d and 802.11h Capabilities: ☒ (highlighted with a red box), Spectrum Load Balancing: ☐, Beacon Period: 100 msec, Beacon Regulate: ☐, ARM/WIDS Override: OFF, Reduce Cell Size (Rx Sensitivity): 0 dB, Energy Detect Threshold Offset: 0 dB, Management Frame Throttle interval: 1 sec, Management Frame Throttle Limit: 20, RX Sensitivity Threshold: 0 dB, and RX Sensitivity Tuning Based Channel Reuse: disable.

For the 802.11d “Country Information” element to be broadcasted on non DFS channels its necessary to have 802.11k enabled. This is important for regions utilizing “world mode” regulatory domain,

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)**

Mobility Controller > Aruba7005

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- System
- Tasks
- Diagnostics
- Maintenance

General Admin AirWave CPSec Certificates SNMP Logging **Profiles** Whitelist More

All Profiles

- QoS
- RF Management
- UCC
- Wireless LAN
- 802.11K
- default**
- Beacon Report Request
- RRM IE
- TSM Report Request
- 802.11r
- 802.1X Authentication

802.11K Profile: default

Advertise 802.11K Capability: ☒

Forcefully disassociate on-hook voice clients: ☐

Measurement Mode for Beacon Reports: beacon-table

Channel for Beacon Requests in 'A' band: 36

Channel for Beacon Requests in 'BG' band: 1

Channel for AP Channel Reports in 'A' band: 36

Channel for AP Channel Reports in 'BG' band: 1

Time duration between consecutive Beacon Requests: 60 sec

Time duration between consecutive Link Measurement Requests: 60 sec

Time duration between consecutive Transmit Stream Measurement Requests: 90 sec

Enable 802.11k but remember to disable Quiet IE in next step.

Mobility Controller > Aruba7005

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- System
- Tasks
- Diagnostics
- Maintenance

General Admin AirWave CPSec Certificates SNMP Logging **Profiles** Whitelist More

All Profiles

- QoS
- RF Management
- UCC
- Wireless LAN
- 802.11K
- default
- Beacon Report Request
- RRM IE**
- TSM Report Request
- 802.11r

RRM IE Profile: default

RRM IE Profile: default

Advertise Enabled Capabilities IE: ☒

Advertise Country IE: ☒

Advertise Power Constraint IE: ☒

Advertise TPC Report IE: ☒

Advertise QBSS Load IE: ☒

Advertise BSS AAC IE: ☒

Advertise Quiet IE: ☐

Disable "Advertise Quiet IE"

WLAN, Encryption and Authentication Settings

aruba MOBILITY CONTROLLER
Aruba7005

ACCESS POINTS: 1 (green), 5 (red)
CLIENTS: 7
ALERTS: 0

Mobility Controller > **Aruba7005**

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
System
Tasks
Diagnostics
Maintenance

NAME	AP GROUP	SECURITY
ArubaIntop1X	Ascom, default	Enterprise
ArubaIntopPSK	Ascom, default	Personal
ArubaIntopOpen	Ascom, default	Open

ArubaIntopPSK General VLANs **Security** Access

More Secure
Enterprise
Personal
Open
Less Secure

Key management: WPA-2 Personal
Passphrase:
Retype:
MAC authentication: Disabled
Blacklisting: Disabled

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

aruba MOBILITY CONTROLLER Aruba7005

ACCESS POINTS 1 5 CLIENTS 7 ALERTS 0

Mobility Controller > Aruba7005

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Diagnostics

Maintenance

Auth Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

Server Groups 3

NAME	SERVICES	FAIL THROUGH	LOAD BALANCE	SERVER RULES
ArubaIntop1x	1	--	--	0
default	1	--	--	1
internal	1	--	--	1

+

Server Group > ArubaIntop1x

Servers

Options

Server Rules

NAME TYPE IP ADDRESS TRIM FQDN MATCH RULES

FreeRadius Radius 192.168.0.2 -- 0

Drag rows to re-order

Enterprise/.1X authentication.

Create a server group and a server.

aruba MOBILITY CONTROLLER Aruba7005

ACCESS POINTS 1 5 CLIENTS 7 ALERTS 0

Mobility Controller > Aruba7005

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Diagnostics

Maintenance

Auth Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

Server Group > ArubaIntop1x > FreeRadius

Server Options

Server Group Trim FQDN

Server Group Match Rules

Name: FreeRadius

IP address / hostname: 192.168.0.2

Auth port: 1812

Acct port: 1813

Shared key:

Retype key:

Timeout: 5

Retransmits: 3

NAS ID:

NAS IP:

Enable IPv6: ☐

NAS IPv6:

Use MDS: ☐

Mode: ☒

Lowercase MAC addresses: ☐

Use IP address for calling station ID: ☐

MAC address delimiter: none

Service-type of FRAMED-USER: ☐

CPPM credentials: ☐

When configuring the authentication 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.

aruba MOBILITY CONTROLLER Aruba7005 ACCESS POINTS 1 5

Mobility Controller > Aruba7005

Dashboard Configuration

WLANs Roles & Policies Access Points AP Groups Authentication Services Interfaces System Tasks

Auth Servers **AAA Profiles** L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- AAA
- ArubaIntop1x
- 802.1X Authentication
- 802.1X Authentication Server Group**
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server

Server Group: ArubaIntop1x

Server Group: ArubaIntop1x

Fail Through: ☐

Load Balance: ☐

Select the Server Group just created.

aruba MOBILITY CONTROLLER Aruba7005 ACCESS POINTS 1 5 CLIENTS 7 ALERTS 0

Mobility Controller > Aruba7005

Dashboard Configuration

WLANs Roles & Policies Access Points AP Groups Authentication Services Interfaces System Tasks Diagnostics Maintenance

Auth Servers **AAA Profiles** L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- AAA
- ArubaIntop1x**
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server
- ArubaIntopOpen
- ArubaIntopPSK
- default
- default-dot1x
- default-dot1x-psk

AAA Profile: ArubaIntop1x

Initial role: logon

MAC Authentication Default Role: guest

802.1X Authentication Default Role: authenticated

Download Role from CPPM: ☐

Set username from dhcp option 12: ☐

L2 Authentication Fail Through: ☐

Multiple Server Accounting: ☐

User idle timeout: seconds

Max IPv4 for wireless user: 2

RADIUS Roaming Accounting: ☐

RADIUS Interim Accounting: ☐

User derivation rules: -None-

Wired to Wireless Roaming: ☒

Device Type Classification: ☒

Enforce DHCP: ☐

PAN Firewall Integration: ☐

Open SSID radius accounting: ☐

Create an 802.1X Authentication Profile.

Except for default roles that are set to “Authenticated” all settings are left as default.

MOBILITY CONTROLLER
Aruba7005

ACCESS POINTS

1
5

CLIENTS

7

ALERTS

0

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

Diagnostics

Maintenance

Mobility Controller > Aruba7005

WLANs 3

NAME	AP GROUP	SECURITY
ArubaIntop1X	Ascom, default	Enterprise
ArubaIntopPSK	Ascom, default	Personal
ArubaIntopOpen	Ascom, default	Open

+

ArubaIntop1X

General

VLANs

Security

Access

More Secure

Enterprise

Personal

Open

Less Secure

Key management:

WPA-2 Enterprise

FreeRadius

Auth servers:

+

Reauth interval:

86400

sec.

Machine authentication:

☐

Blacklisting:

☐

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.

Interoperability Report
Ascom i62 – Aruba

Date
2019-05-03

Page
17 / 21

Edit parameters for 1001

Device type: i62 Protector

Parameter definition: 14.351

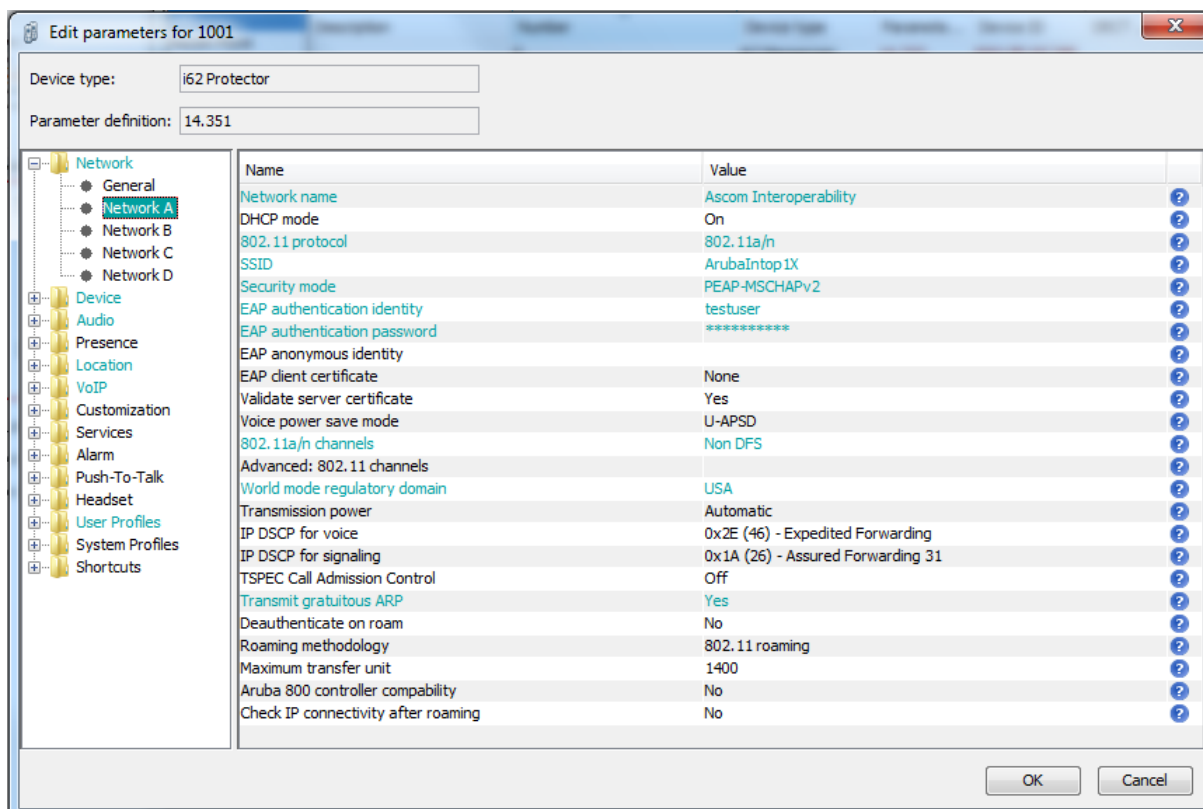
Name	Value
Network name	Ascom Interoperability
DHCP mode	On
802.11 protocol	802.11a/n
SSID	ArubaIntopPSK
Security mode	WPA-PSK & WPA2-PSK
WPA-PSK passphrase	*****
Voice power save mode	U-APSD
802.11a/n channels	Non DFS
Advanced: 802.11 channels	
World mode regulatory domain	USA
Transmission power	Automatic
IP DSCP for voice	0x2E (46) - Expedited Forwarding
IP DSCP for signaling	0x1A (26) - Assured Forwarding 31
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 roaming	No

OK Cancel

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)

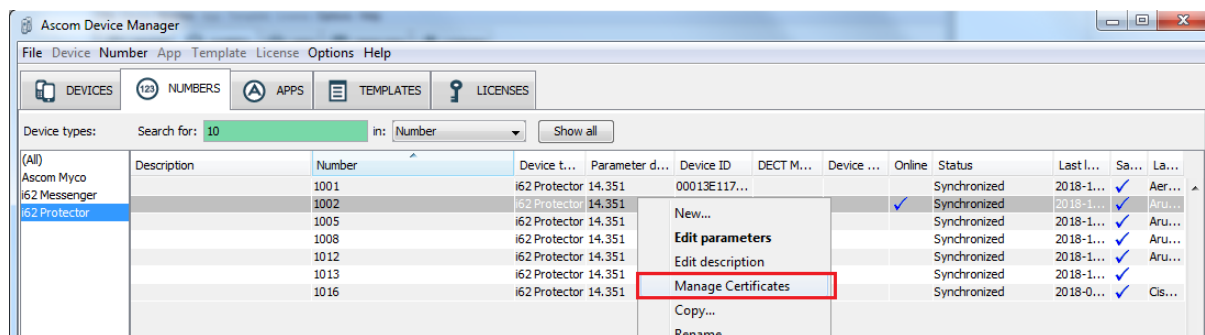
Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to “USA”. Consider the known issues chapter.



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 Validation Records

Pass	17
Fail	0
Comments	2
Not verified	2
Total	21

Contact your Ascom representative for additional information about interoperability and test results.

Document History

Rev	Date	Author	Description
P1	3 May 2019	SEKMO	Draft. AOS 8.4.0.1
R1	20 May 2019	SEKMO	Official revision R1