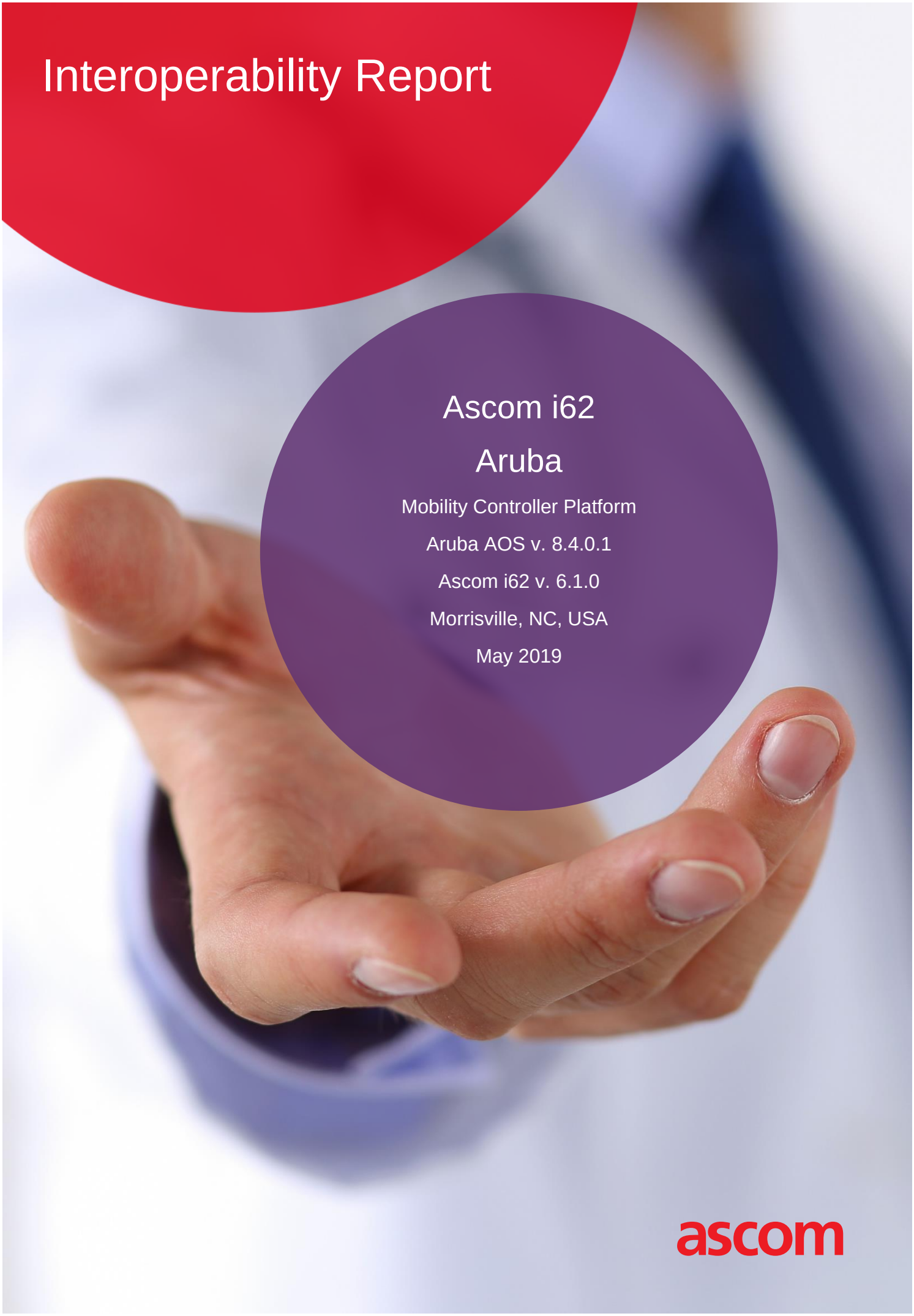
Interoperability Report



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

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

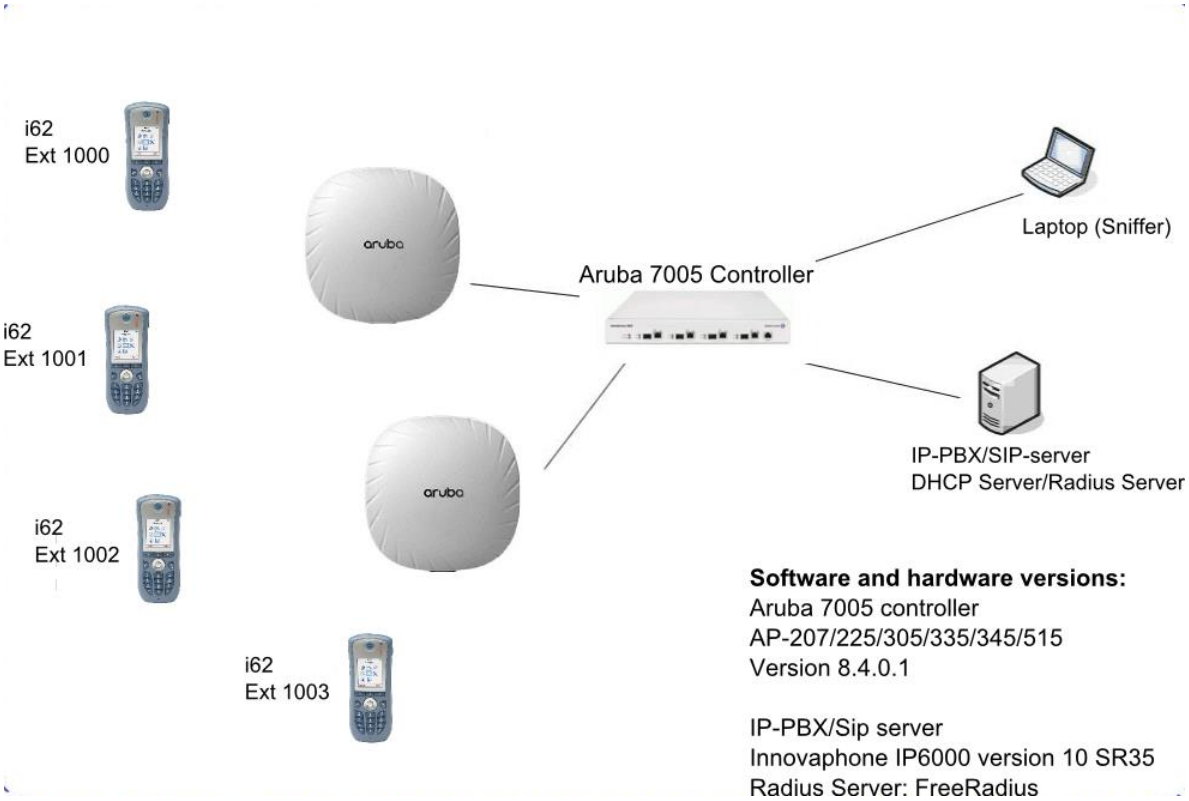
Validation site

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
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. Refer to HPE/Aruba release notes for details.		
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, **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.**	Enable 802.11k but disable "Advertise Quiet IE"	Ascom ticket MRS-290
Due to RF environment it was noted that voice quality and connection stability was generally poor on 2.4GHz radio. This has likely nothing to do with the infrastructure and client interoperability but is rather a result of a congested frequency band. It's suggested to avoid using 2.4GHz RF band for voice if possible. .		

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.

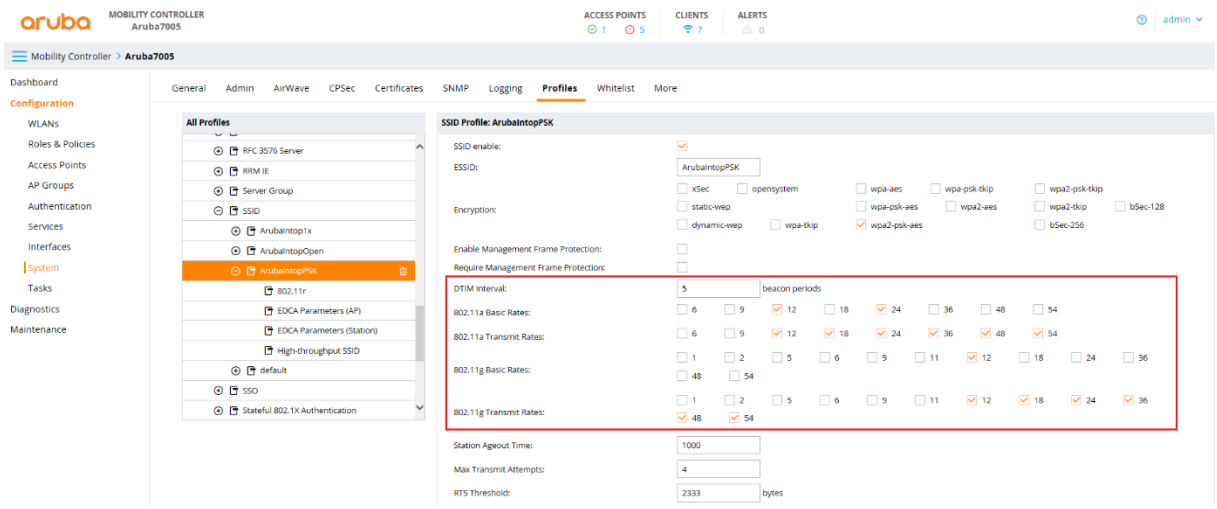
Appendix A: Validation Configurations

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 cas es.

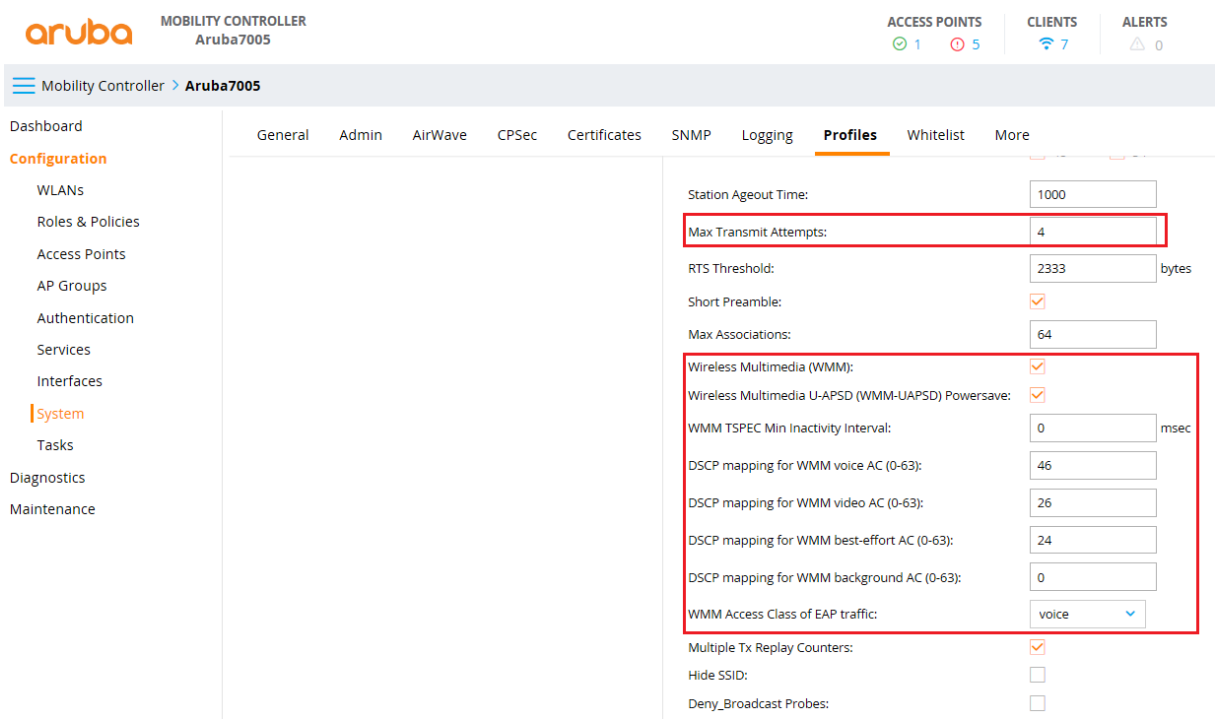
The configuration file is found at the end of this appendix.

General settings (SSID, Radio and QoS)



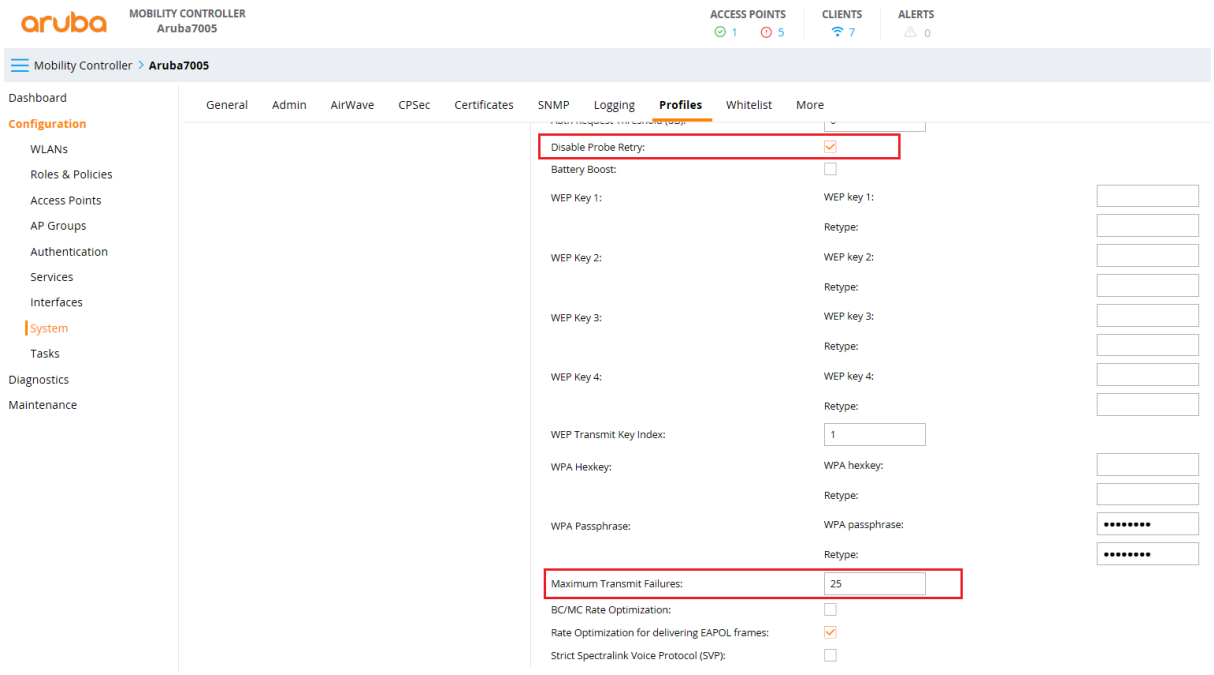
Set DTIM Interval to 5. This value is recommended for maximum battery conservation without impacting call quality. Using a lower value will also decrease the standby time.

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

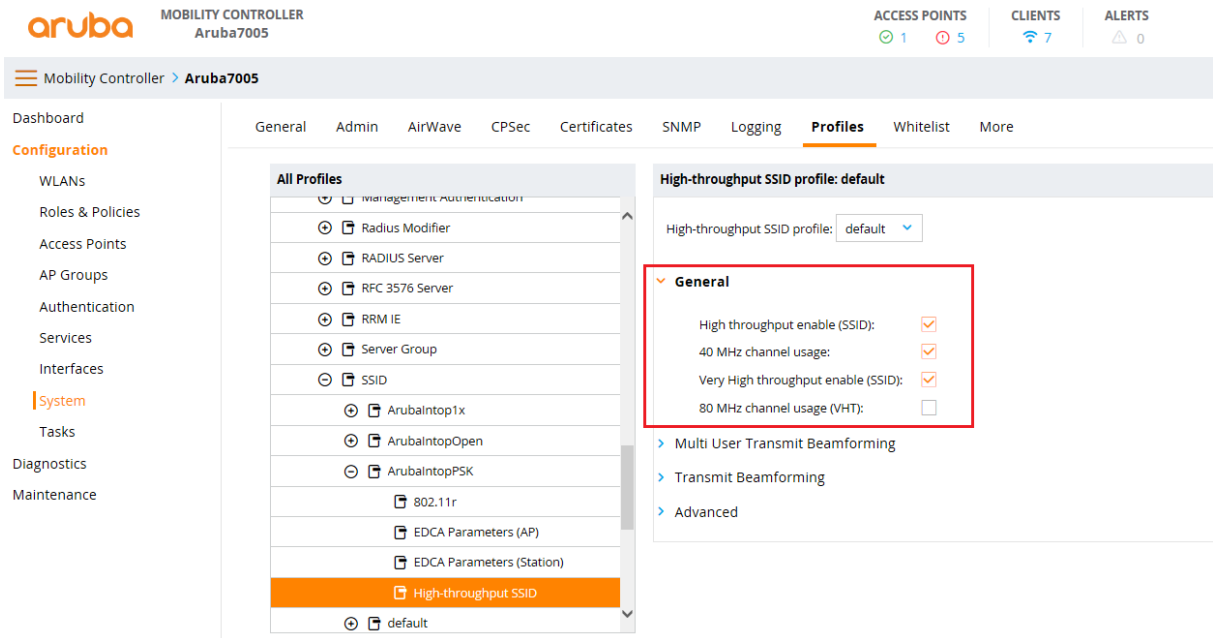


Ascom recommends disabling the lowest rates and recommends that 12Mbps is set as the lowest basic rate.

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.

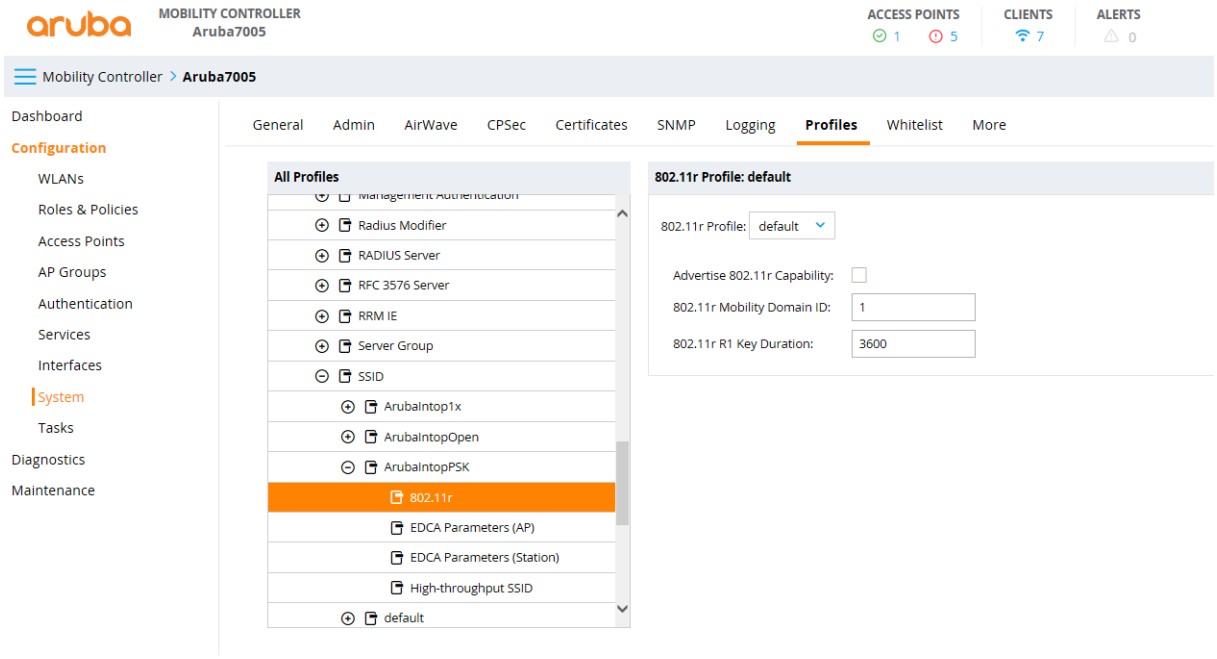


Set “Maximum Transmit Failures” to 25.

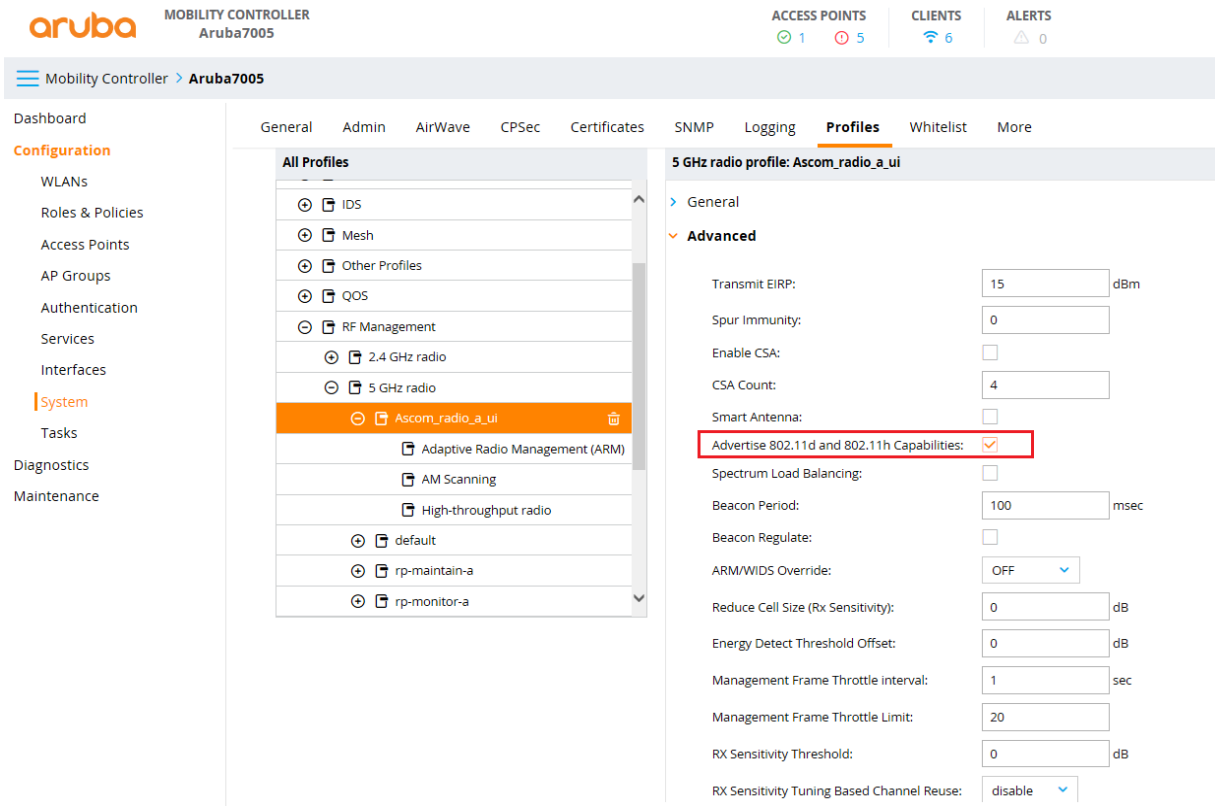


“High throughput enable” enables 802.11n capabilities that are supported in combination with Open encryption and WPA2-AES (PSK or Enterprise).

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



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.



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:

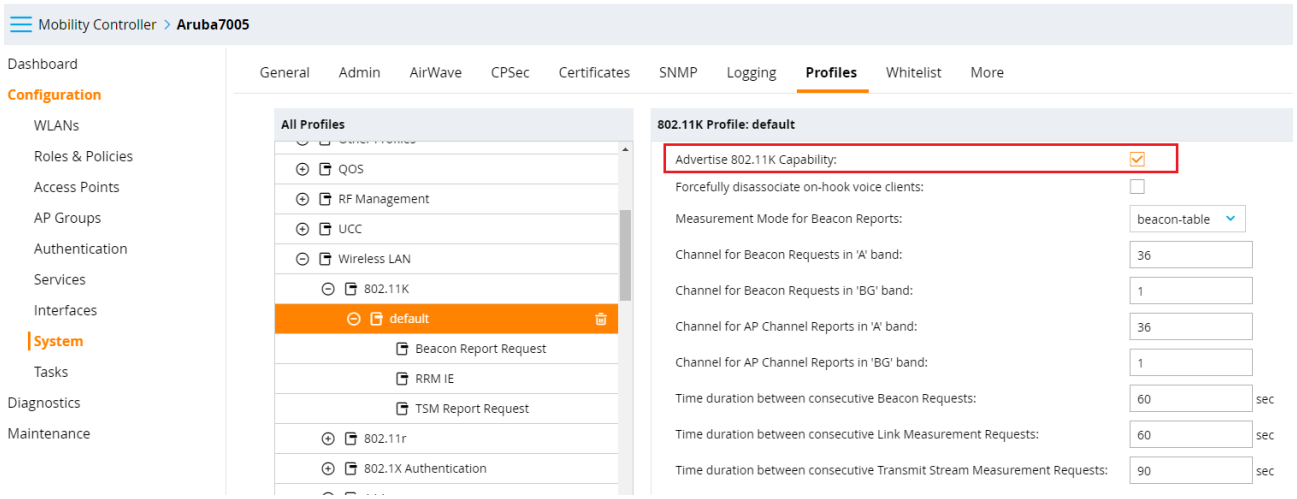
1. ***Enabling more than 8 channels will degrade roaming performance. In situations where UNII1 and UNII3 are used, a maximum of 9 enabled channels can be allowed. Ascom does not recommend exceeding this limit.***

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.***

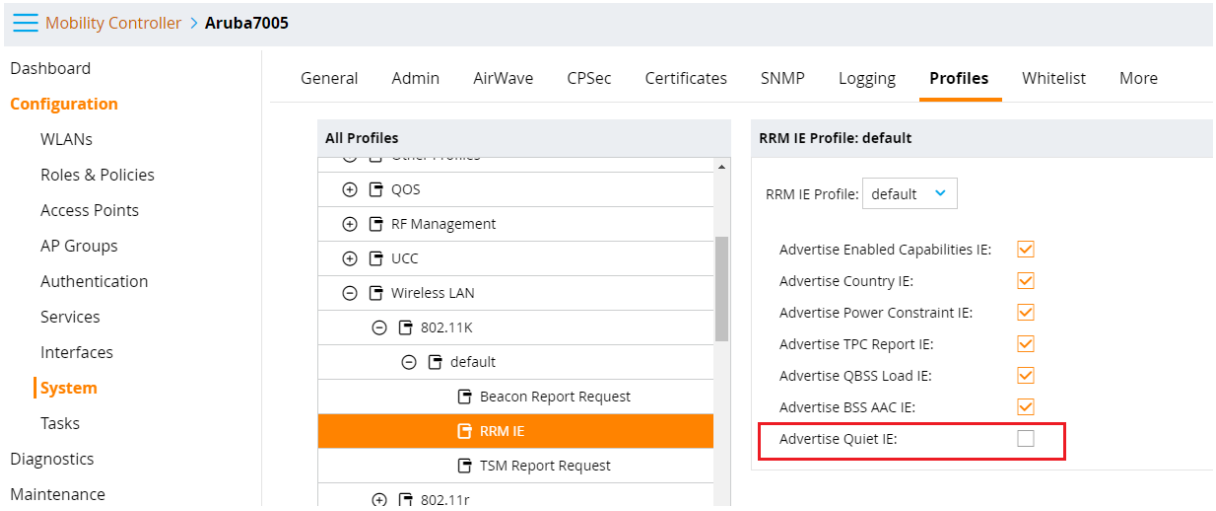
3. ***Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80MHz channel bonding as it severely reduces the number of available non overlapping channels.***

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)**

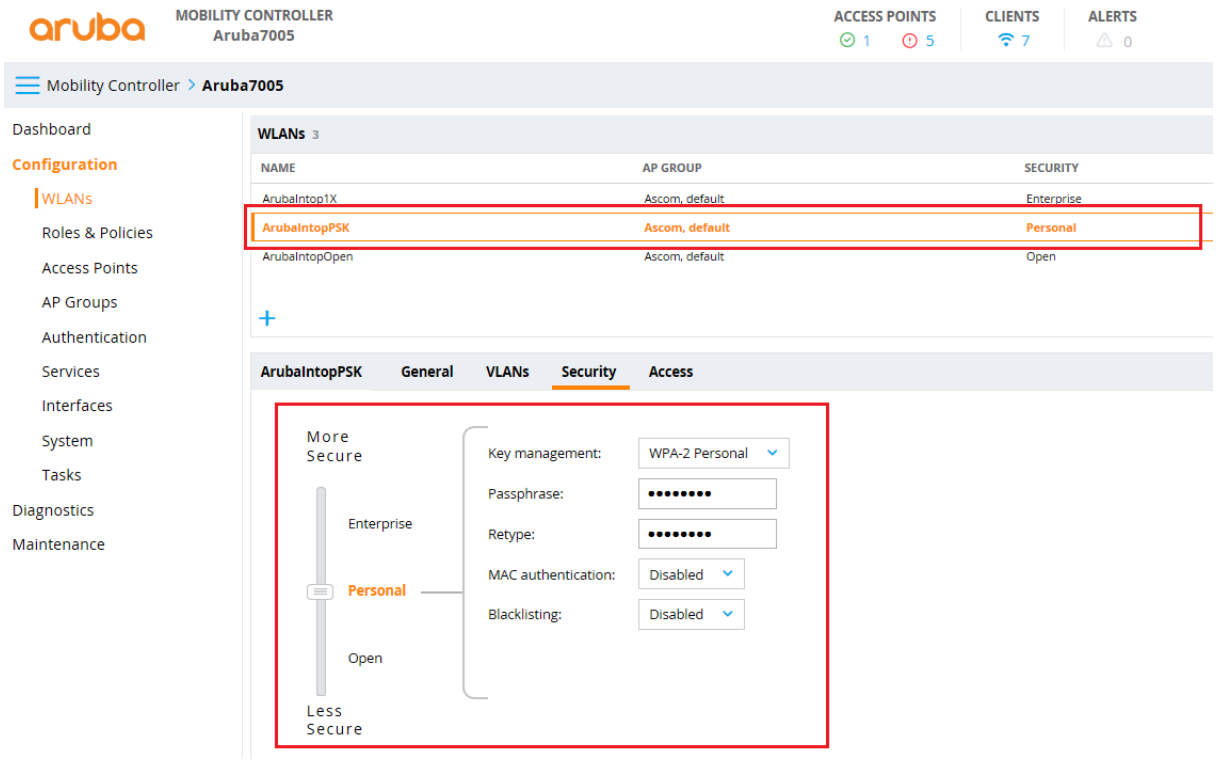


Enable 802.11k but remember to disable Quiet IE in next step.

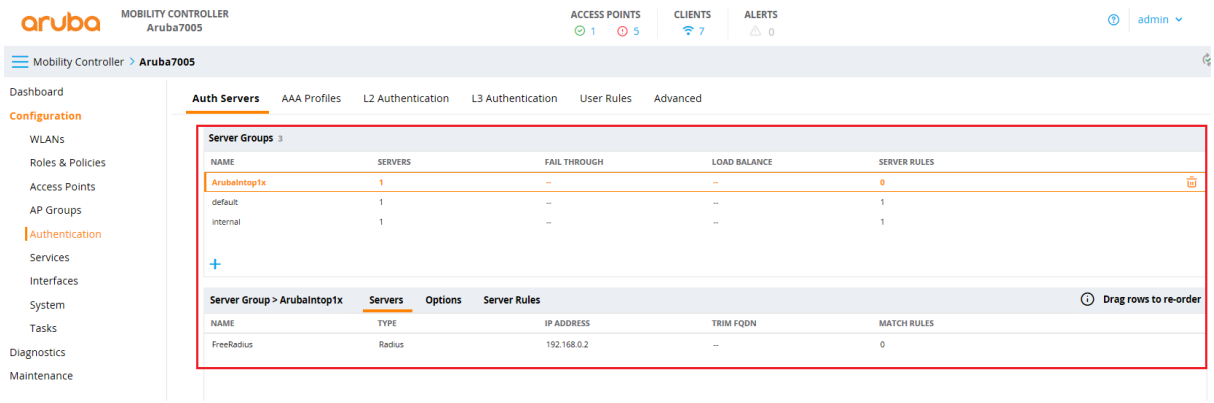


Disable “Advertise Quiet IE”

WLAN, Encryption and Authentication Settings

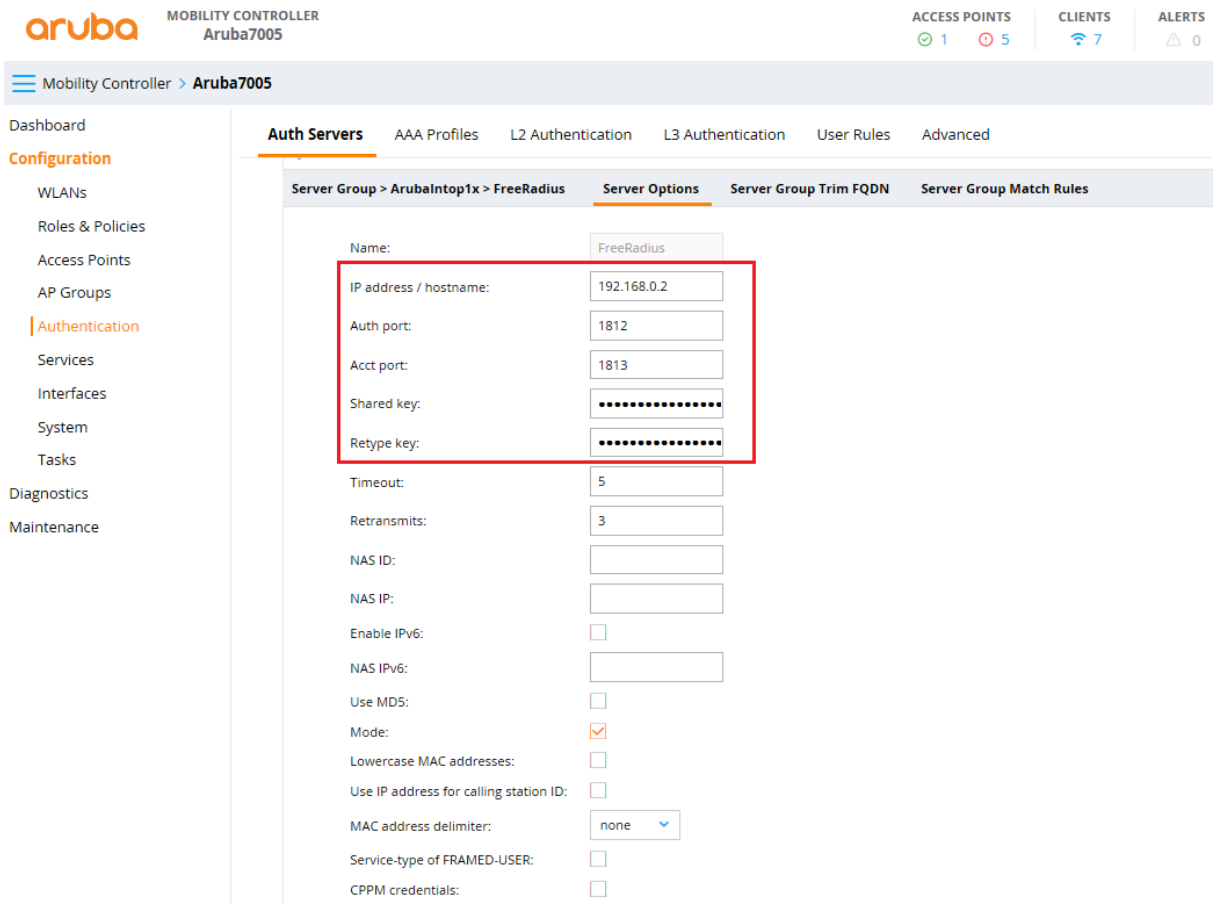


WPA2-PSK. Set the security profile to WPA2-PSK, AES encryption.

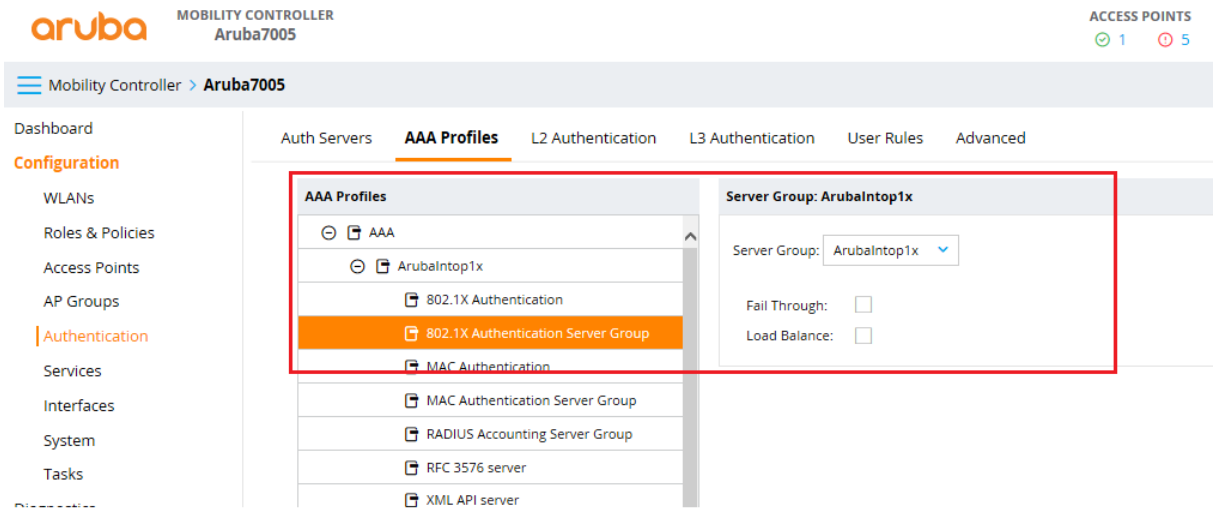


Enterprise/.1X authentication.

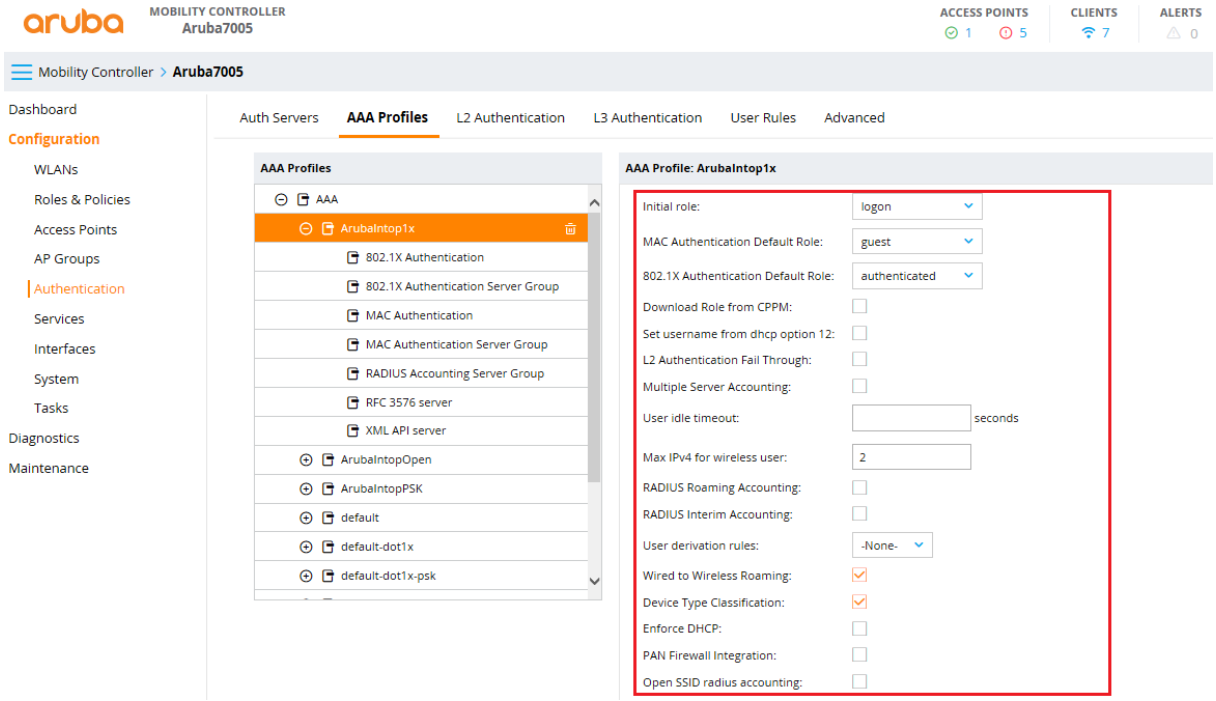
Create a server group and a server.



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.

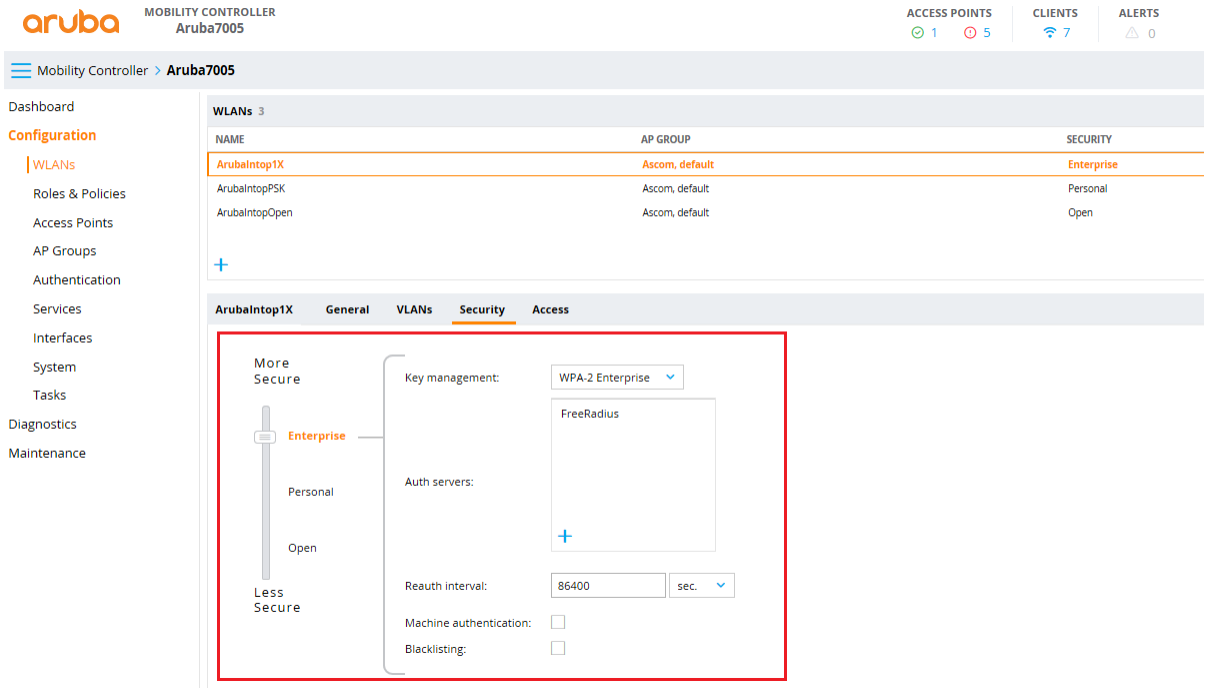


Select the Server Group just created.



Create an 802.1X Authentication Profile.

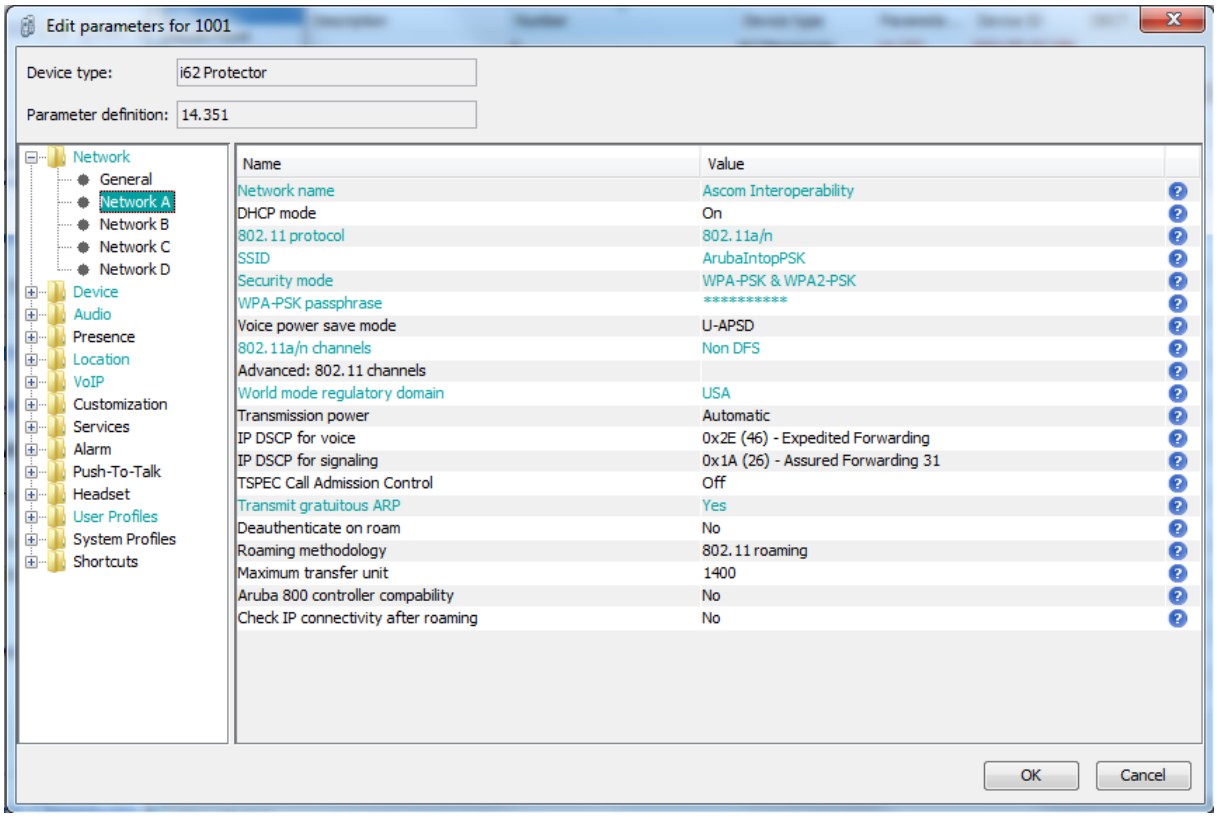
Except for default roles that are set to “Authenticated” all settings are left as default.



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.

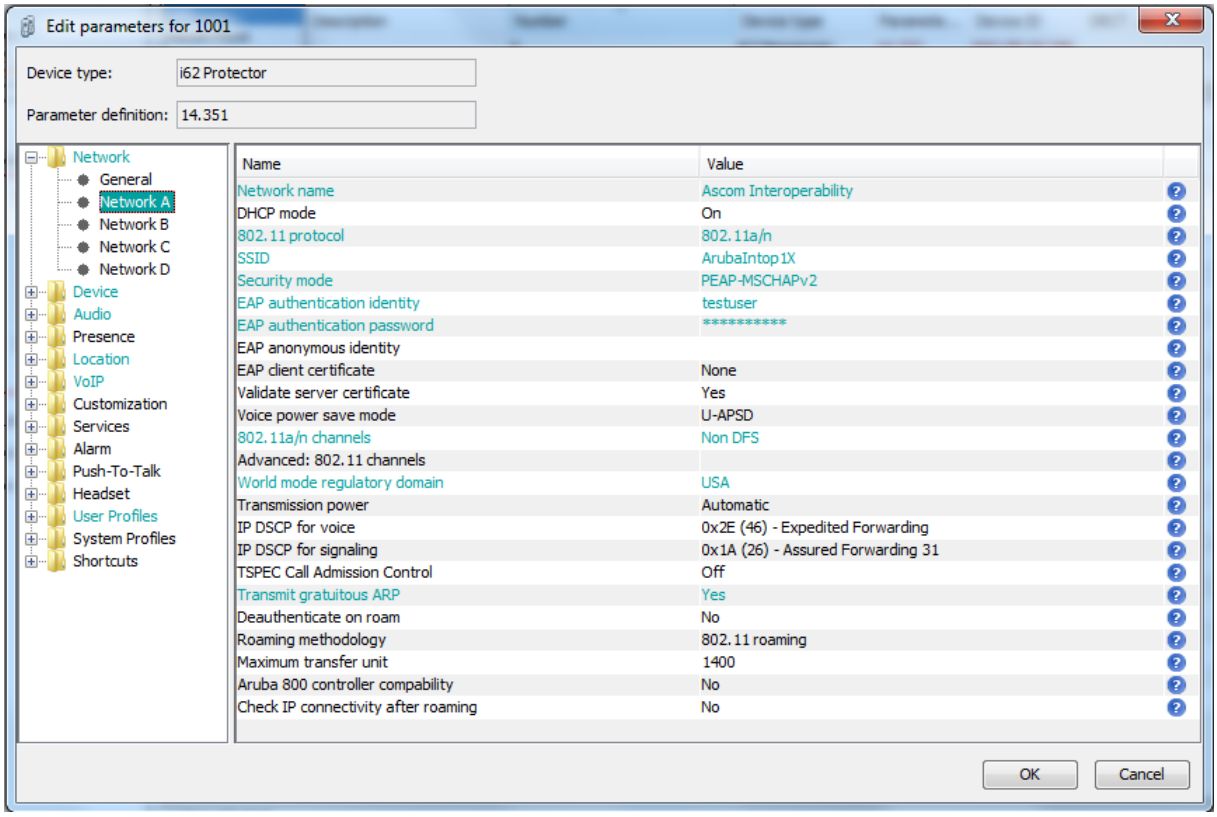
See Appendix B for the controller configuration used for the certification process.



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)

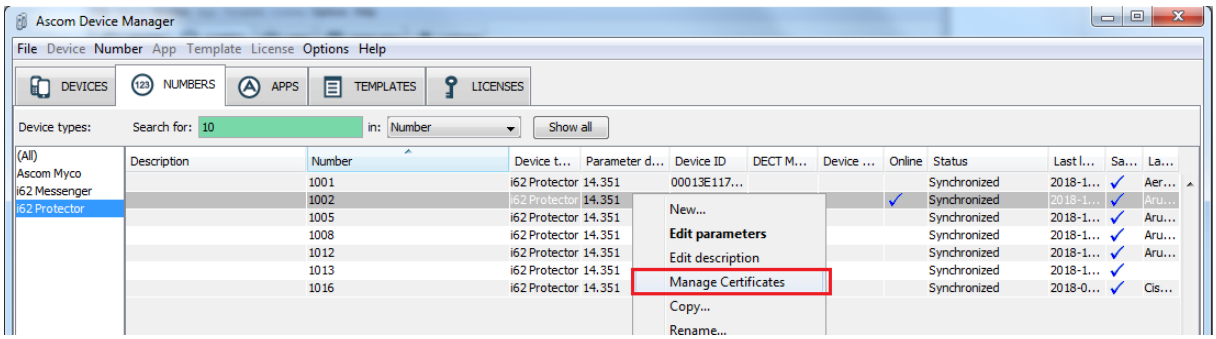
Note. FCC is no longer allowing 802.11d to determine regulatory domain. Devices deployed in USA must set Regulatory domain to "USA". Consider the known issues chapter.



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