Interoperability Report

Ascom Myco
Aruba
Mobility Controller Platform
Aruba AOS v. 8.2.1.0
Ascom Myco v. 10.4.0
Morrisville, NC, USA
June 2018
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 8.2.1.0 ............................................................................................ 8
   Ascom Myco Setting Summary .................................................................................................... 17

Appendix B: Detailed Verification 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

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

Participants
Karl-Magnus Olsson, Ascom, Morrisville

Verification topology

Software and hardware versions:
AP-207/225/305/315/325/335
Version 8.2.1.0
IP-PBX/Sip server
Innovaphone IP6000 version 10 SR35
Radius Server: FreeRadius
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 Myco 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.

Unfortunately blocking issues with voice quality and connection stability was found on 2.4GHz radio with AP3xx. It was noticed that access point sends excessive amount of RTS with a very high duration time. It was also noticed that the access point sent data frames at 1Mbps even though the lowest supported rates was set to 12Mbps. At this time no operation of Ascom devices can be recommended on the 2.4GHz radio.

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, 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 8.2.1.0:

AP-207, 214, 215, 224, 225, 275
AP-304, 305, 314, 315, 324, 325, 334, 335

Supported Partner Controller Platforms with AOS version 8.2.1.0:

7000 series Mobility controllers
7200 series Mobility controllers
Verification overview

WLAN Compatibility and Performance

<table>
<thead>
<tr>
<th>High Level Functionality</th>
<th>Result</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association, Open with No Encryption</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association, WPA2-PSK / AES Encryption</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association with EAP-TLS authentication</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Association, Multiple ESSIDs</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Beacon Interval and DTIM Period</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>PMKSA Caching</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>WPA2-opportunistic/proactive Key Caching</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>WMM Prioritization</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>802.11 Power-save mode</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>802.11e U-APSD</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>802.11e U-APSD (load test)</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Roaming, WPA2-PSK, AES Encryption</td>
<td>OK *</td>
<td>Typical roaming time 61 ms</td>
</tr>
<tr>
<td>Roaming, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK **</td>
<td>Typical roaming time 56 ms</td>
</tr>
</tbody>
</table>

*) 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

<table>
<thead>
<tr>
<th>Description and Consequence</th>
<th>Workaround</th>
<th>Ticket(s) raised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem with voice quality and connection stability on 2.4GHz radio with AP3xx.</td>
<td>Avoid using 2.4GHz RF band.</td>
<td>Aruba / HPE case 180675</td>
</tr>
<tr>
<td>It was noticed that access point sent excessive amount of RTS with a very high duration time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>It was also noticed that the access point sent data frames at 1Mbps even though the lowest supported rates was set to 12Mbps.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note that the 5GHz radio not affected. Also note that AP2xx is not affected.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ascom Myco does not handle 802.11K info correctly which affects the roaming negatively.</td>
<td>Do not advertise the 802.11K capabilities for the Ascom Myco SSID.</td>
<td></td>
</tr>
</tbody>
</table>

For additional information regarding the known limitations please contact [interop@ascom.com](mailto:interop@ascom.com) or [support@ascom.com](mailto:support@ascom.com).

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

Aruba 7005 Controller, AOS 8.2.1.0

This section includes screenshots and explanations of basic settings required to use Ascom Myco 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)

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.
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 Myco 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 Myco but the device has no problem operating on a SSIDs where 802.11r is advertised.
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 Myco 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)
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.
Ascom Myco Setting Summary

- Select Network to be active (In this example “ArubaIntopPSK” (created in step below)
- Select frequency band according to system setup (here 5GHz)
- Select only the channels used in the system. In this example default (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".
Pre-Shared key authentication

Network settings for WPA2-PSK
Authentication with dot1X (EAP/PEAP-MSCHAPv2)

802.1X Authentication requires a CA certificate to be uploaded to the device by "right clicking" -> Manage Certificates.

Upload the required CA certificate under Trust list.
Network settings for 802.1X authentication (PEAP-MSCHAPv2)

- Select security mode PEAP-MSCHAPv2.
- Enter User identity and password.
- Select your trusted certificate uploaded to the device in previous step.
Appendix B: Detailed Verification Records

<table>
<thead>
<tr>
<th>Pass</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail</td>
<td>0</td>
</tr>
<tr>
<td>Comments</td>
<td>1</td>
</tr>
<tr>
<td>Not verified</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>21</strong></td>
</tr>
</tbody>
</table>

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):

Document History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>4 June 2018</td>
<td>SEKMO</td>
<td>AOS 8.2.1.0 Draft</td>
</tr>
<tr>
<td>R1</td>
<td>21 June 2018</td>
<td>SEKMO</td>
<td>Corrections after review. Revision R1</td>
</tr>
</tbody>
</table>