ARUBA networks
1344 Crossman Avenue | Sunnyvale, California 94089
Tel 408 227 4500 | Fax 408 752 0626
www.arubanetworks.com

Software Defined Radio (SDR)

Date: July 01, 2015

Federal Communications Commission
Authorization and Evaluation Division
7435 Oakland Mills RoadColumbia, MD 21046

Attention: OET Dept.

FCC ID: Q9DAPIN0324325

Regarding Certification as a Software Defined Radio

This letter is to notify the FCC of our intentions regarding submitting for grant approvals as a Software Defined Radio in accordance to KDB 442812 D01 SDR Apps Guide v02r03. All supporting documentation to be approved as an SDR will be included.

Sincerely,

Name: Robert Hastings
Company: Aruba Networks
Title: Regulatory Compliance Manager
Date: 07/01/2015

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software can be accessed from the aruba.com website. Username and Password are required to access the files The image files are downloaded from aruba.com to a local file server via https and then into the controller via ftp, scp or https. The integrity and the authenticity of the image files are secured by using a digital signature that is signed at Aruba and verified on the controller before installation
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters? Software/firmware decided the RF parameters (i.e. allowed channels and Max EIRP Tx Power). Tx Power is limited to the Maximum EIRP certified by the grant.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification. The image files are digitally signed (using x509 certificates). The chain of trust leads back to the root certification authority that resides at Aruba Networks. The controllers have the Aruba root-CA certificate factory-installed. This will be used to verify that the images did indeed originate from Aruba. Before installation of the image files, the controller will verify the signature and reject the images files if they cannot be authenticated.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details. The digital signature mechanism described above will also ensure integrity. Verification of the signature also ensures that the file was not modified.
	5. Describe, if any, encryption methods used. No encryption required. Firmware in Binary form.

	6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation? Not applicable. Master Device ONLY but all provisions are taken to ensure all compliance measures are followed
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented? The RF control logic is fully proprietary and the ArubaOS code is digitally signed using a X.509 certificate, which prevents it from being tampered or modified by third-party in the field.
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded. A 3rd party with administrative permissions can upgrade the controller to a new AoS Image which contain device parameters . The AoS images are digitally signed by Aruba. The controller will verify the signature before proceeding with upgrade. This ensures that ONLY Aruba released images run on our products.
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification. No it is not possible device is locked
	4. What prevents third parties from loading non-US versions of the software/firmware on the device? We don't have Non-US software. We have US specific Hardware, which uses generic software.
	5. For modular devices, describe how authentication is achieved when used with different hosts. Not applicable.. We are not a modular device

SOFTWARE CONFIGURATION DESCRIPTION	
USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other.) Professional installer and end user

a) What parameters are viewable to the professional installer/end-user?[5] Forced 20 MHZ bandwidth switch, 2.4 G / 5 G band switch, PSP Xlink mode switch, multimedia/game environment, navigation, power saving mode, the sensitivity of the network physical address, and RF switch
b) What parameters are accessible or modifiable to the professional installer? Forced 20 MHZ bandwidth switch, PSP Xlink mode switch, multimedia/game environment, roaming sensitivity, power saving mode
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Yes the parameters are limited to only allow access to those certified channels
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? The devices firmware is hard-coded to only operate on authorized U.S. channels and cannot be changed.
c) What configuration options are available to the end-user? End-user if provided with login information will have access to the WebUI allowing them privileges to change authorized channels as well as Frequency Bandwidth.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Yes, only the parameters that are authorized can be accessed by the installer
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? The devices firmware is hard-coded to only operate on authorized U.S. channels and cannot be changed.
d) Is the country code factory set? Can it be changed in the UI? Yes, the country code is factory set, and it cannot be changed in the UI

	i) If so, what controls exist to ensure that the device can only operate within its authorization I in the U.S.? Not applicable since the device is factory locked to only operate within the authorized US parameters.
	e) What are the default parameters when the device is restarted? Forced 20 MHZ bandwidth switch: closed 2.4 G / 5 G band switch: open PSP Xlink mode switch: closed multimedia/game environment: closed navigation: closed power saving mode: closed the sensitivity of the network physical address: no RF switch : open
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02. No, it can't work in the bridge or the mesh mode
	3. For a device that can be configured as a master and client (with active or passive scanning) If this is user configurable, describe what controls exist to ensure compliance. If the device acts as a master in some bands and client in others, how this configured to ensure compliance? Not applicable, device is not configurable. Master ONLY.
	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a)) FCC ID: Q9DAPIN0324325, are professionally installed devices. The maximum Granted Tx Power is hard coded into the RF control logic which is digitally signed which prevents tampering. These Tx Power Levels can not be excided, the proprietary software algorithm will adjust the maximum allowable Tx Power allowed when different antenna gains are utilized to ensure the Maximum Granted Tx Power is not exceeded.