Software Security Requirements Cover Letter

FCC ID: Q9DAPIN0754
IC: 4675A-APIN0754

Software Security Description	
General Description	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate
	Response: Software can be accessed from the Aruba networks Central website. Username and Password are required to access the files. The ArubaOS image and Downloadable Regulatory Table (DRT) files are downloaded directly from Central into the controller (or APs, for controllerless installations) 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 (or AP) before installation.
	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?
	Response: The ArubaOS image contains DFS parameters. The DRT defines the allowed channels and maximum EIRP/Tx Power, as detailed in the certification reports.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification
	Response: The ArubaOS files are digitally signed (using x509 certificates). The

	chain of trust leads back to the root certification authority that resides at Aruba Networks. The Aruba controllers (and APs) 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 devices acting as a controller will verify the signature and reject the images files if they cannot be authenticated.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Response: No encryption required. Firmware in Binary form.
	5. 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?
	Response: Not applicable. Master Device ONLY but all provisions are taken to ensure all compliance measures are followed
Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.
	Response: Since the device is locked to US Domain at Manufacturing, a 3rd party does not have the capabilities to make any changes to the regulatory domain. This ensure that any operation will be compliant with the certification.
	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality
	Response: Device does not permit 3rd Party Software or Firmware Installation.

	3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.
	Response: Not Applicable, Device is not a Module
Software Configuration Description	
User Configuration Guide	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.
	Response: Professional installer, ACMP or other Aruba-certified technicians (system integrator) are provided with login information will have access to the Central system allowing them privileges to change antenna gain (where applicable), operating channels as well as Frequency Bandwidth. These qualified technicians are using manufacturer-approved antennas only. The ACMP installer is responsible for ensuring that the Equivalent Isotropically Radiated Power (EIRP) levels for all external antenna devices are compliant with regulatory standards of the host country/domain. Installers are required to record the antenna gain for this device in the system management software. End-Users have no access
	a) What parameters are viewable and configurable by different parties?
	Response: Professional Installers and system integrators, will have access to the operating channel, bandwidth, and maximum EIRP. End-Users have no visibility to the RF parameters. Forced 20 MHz bandwidth switch, 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 by the professional installer or system integrators?
	Response: Professional Installers and system integrators, will have access to the operating channel, bandwidth, and maximum EIRP.
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

	Response: Operation is limited by the DRT, independent of any entry by an installer. If an entry exceeds the constraints in the DRT for channel or power, the system will default to the previous channel and power settings.
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Response: Only US sku devices are sold in the US. They can only operate per the US constraints in the DRT. These devices are locked in manufacturing to prevent any changes to the regulatory domain/country code.
	c) What parameters are accessible or modifiable by the end-user?
	Response: End-Users have no access to the operating parameters.
	1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Response: End-Users have no access to the operating parameters. Operation is limited by the DRT, independent of any entry by an installer. If an entry exceeds the constraints in the DRT for channel or power, the system will default to the previous channel and power settings.
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	Response: End-Users have no access to the operating parameters.
	d) Is the country code factory set? Can it be changed in the UI?
	Response: Only US sku devices are sold in the US. They can only operate per the US constraints in the DRT. These devices are locked in manufacturing to prevent any changes to the regulatory domain/country code.
	1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Response: 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?
	Response: The AP operates per the ap-group profile in the associated controller that defines the operating channels, bandwidths, and Tx power. APs that

	restarted will attempt to communicate to the controller and if successful will resume operate per the assigned ap-group configuration. If a controller is not available, the AP will not resume operation. It will continue to attempt to communicate with the associated controller.
	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.
	Response: The AP can be configured as a Mesh.
	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, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?
	Response: Not applicable, device cannot be configured as a client.
	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))
	Response: Aruba/HPE APs are professionally installed devices. The Maximum Granted Tx Power is coded into the DRT which is digitally signed preventing any tampering. These Tx Power Levels cannot be exceeded.