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. 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.
	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? 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. 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. 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. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. 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? 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. No it is not possible. Device is locked
	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. 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. 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. 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. Professional installer and end user are provided with login information will have access to the WebUI allowing them privileges to change antenna gain (where applicable), authorized channels as well as Frequency Bandwidth.
	a. What parameters are viewable and configurable by different parties?[9] 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 by the professional installer or system integrators?

Forced 20 MHZ bandwidth switch, PSP Xlink mode switch, multimedia/game environment, roaming sensitivity, power saving mode

(1) 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

(2) 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 parameters are accessible or modifiable by 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.

(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

Yes, only the parameters that are authorized can be accessed by the installer

(2) What controls exist so 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

(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization 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 sensitivity of the network physical address: no RF switch : open These default parameters are within the certified parameters
	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, 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? 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: Q9DAPIN0214215, are professionally installed devices. The Maximum Granted Tx Power is hard coded into the RF control logic which is digitally signed preventing any tampering. These Tx Power Levels can not be excided, the proprietary software algorithm will adjust the maximum allowable Tx Power when different antenna gains are utilized to ensure the Maximum Granted Tx Power Level is not exceeded.