Software Security Declaration

FCC ID : 2AB874018

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.	The RF parameters are unchangable by users. Only manufaurer can use special test utility to change the RF parameters. The special test utility will not release to users.
	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?	There is no RF-related SW/Firmware can change RF parameters
	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 RF parameters can only be changed by manufacturer by special test utility which is not public or releasing to users.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	There is no RF-related SW/Firmware can change RF parameters
	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?	The device can be configured as an AP mode or a client mode, the maximum power and channel plan compliance FCC rules, and can`t be changed by end use.

SOFTWARE SECURITY DESCRIPTION		
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.	There are no public software tools can change the regulatory rule.
	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. *Note : See*, for example, www.XXXXX.com/	Only manufacturer can use mass-production utilities provided by Qualcomm Atheros (chip vender) to change regulatory rule and RF parameters.
	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. *Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated*	This is not a modular device.

	into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third-party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing.	

SOFTWARE SECURITY 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.	Users can not change RF parameters through UI
	a. What parameters are viewable and configurable by different parties? *Note: The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output of the device). These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.*	- Wireless Mode : (802.11a, 802.11a/n, 802.11a/n/ac, 802.11b, 802.11b/g, 802.11b/g/n) - Operation Mode : AP
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	- change the Wifi Encryption, Channel, SSID, Data Rate - Status Information: Wifi Encryption, Channel, SSID, Data Rate
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Users can't change RF parameters
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Users can't change RF parameters
	c. What parameters are accessible or modifiable by the end-user?	There is no RF parameters can be modified by users
	(1) What parameters are accessible or modifiable by the end-user?	There is no RF parameters can be modified by users
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	All RF parameters of the shipping devices are unachangable by users.
	d. Is the country code factory set? Can it be changed in the UI?	Default is US channel

	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Default is US channel for shipping to user
	e. What are the default parameters when the device is restarted?	The available frequency of this device is "2.412 ~ 2.462 GHz, 5.180 ~ 5.240GHz, 5.745 ~ 5.825GHz

SOFTWARE SECURITY DESCRIPTION		
USER CONFIGURATION GUIDE	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.	It did not support 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?	The available channel of the device can't be modified by end-user through UI even it is configred as master mode.
	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))	There is no UI for users to change RF parameters.

*Signature*_____

Name/Title: Johnson Wang/ Manager
Company Name: Iconnect
TEL: +8862-796-8477#22
Email: jackie@alfa.com.tw