SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

In accordance with FCC KDB 594280 D02 v01r01, the new Software Security requirements for U-NII Devices, the following information is provided to describe the security features of the software in this device.

SOFTWARE SECURITY DESCRIPTION		
General Description	1 Describe how any software/firmware update will be obtained, downloaded, and installed.	The upgrade control message is communicated via DTLS and the software binary image is downloaded by using sFTP.
	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?	- all the radio frequency parameters that are modified by any software  - These parameters is limited in UI. (See file 1)
	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.	Baisically, AP and APC is authenticated each other. All control messages between AP and APC is encrypted via DTLS. Regarding to the binary image file for upgrade, AP checks the CRC value for integrity test and the header information of software binary image after downloading software binary image received from APC or the upgrade server. If the software may be modified, CRC checksum error happends or AP will
	4 Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	
	5 Describe, if any, encryption methods used.	
	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?	- Our device is operated as master - UI(WEB) is limited to ensure compliance and device also has limitation to ensure compliance
Third-Party Access Control	1 How are unauthorized software/firmware changes prevented?	Refer to the 3 ~ 5 of General Description
	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.	- No. it is not possible for third parties to load device drivers that could modify the RF parameters
	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 for devices are authorization in U.S
	4 What prevents third parties from loading non-US versions of the software/firmware on the device?	HW is limited to US. The non-US versions software/firmware can't change
	5 For modular devices, describe how authentication is achieved when used with different hosts.	Not modular devices

SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE	1 To whom is the UI accessible? (Professional installer, end user, other.)	Professional installer, or IT Manager
	a) What parameters are viewable to the professional installer/end-user?	 -. See file 1
	b) What parameters are accessible or modifiable to the professional installer?	 -. See file 1
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes

	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	User can't control device's country information for devices are authorization in the U.S.
	c) What configuration options are available to the end-user?	 -. See file 1
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	User can't control device's country information for devices are authorization in the U.S.
	d) Is the country code factory set? Can it be changed in the UI?	No for devices are authorization in U.S
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	No for devices are authorization in U.S
	e) What are the default parameters when the device is restarted?	U.S
	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.	N/A
	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?	N/A
	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))	N/A (can't use different types of antenna)

File 1

Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes.

Radio > 802.11a/n/ac > General

Apply

SERVICE	Enable / Disable

Apply

General

BANDWIDTH (MHZ)	80
BEACON PERIOD (TUS)	100
RTS THRESHOLD (BYTES)	2346
SHORT RETRY	4
LONG RETRY	10
FRAGMENTATION THRESHOLD (BYTES) [1]	1000
TX MSDU LIFE TIME (TUS)	512
RX MSDU LIFE TIME (TUS)	512
MAX. ALLOWED STATIONS ON AN AP [2]	127
CONTROLLED VOICE OPTIMIZATION [3]	Enable / Disable
MULTI-ANTENNA MODE [4]	Dynamic / Static

Apply

Data Rates [5]

6 MBPS	Disable
9 MBPS	Disable
12 MBPS	Disable
18 MBPS	Disable
24 MBPS	Basic
36 MBPS	Supported
48 MBPS	Supported
54 MBPS	Supported