SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

In accordance with FCC KDB 594280 D02 v01r02, 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 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	WiFi driver and firmware are embedded in system software and there is no installation and download process.
	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?	All default parameters approved by the FCC are programmed in driver and firmware which would be embedded in system. So end-user can not access those 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.	WiFi driver and firmware are embedded in system software and there is no installation process. End-user can not access them.
	4 Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	No encryption, but WiFi firmware is an binary code.
	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 is configured as a client only. There is a country code regulatory parameter to limit product to operate the device under its authorization in the U.S. This regulatory parameter would define which channel would be available to operate in passive scan to meet U-NII requirements.
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.	The device has a country code regulatory parameter to operate it under its authorization in the U.S. Also, end-user can not access that value.
	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.	WiFi driver and firmware are embedded in system and there is no installation process. This system software is programmed and protected in flash memory. The third-parties can not access that flash memory.
	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. 7	The device has a country code regulatory parameter to operate it under its authorization in the U.S. This regulatory parameter would define which channel would be available to operate in passive scan to meet U-NII requirements. Also, this parameter can not be modified by outside because it is contained in WiFi driver and firmware.

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.	WiFi driver and firmware that can affect the device's RF parameters are embedded in system and there is not any installation process. System firmware is programmed and protected in flash memory.
	a) What parameters are viewable and configurable by different parties?9	All default parameters are programmed in both driver and firmware which would be embedded in system firmware. End-user only could select which master(AP) to connect.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	None.

	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes. Some parameters are programmed in driver and firmware are embedded in system, and the installer cannot access them. Also, the system firmware protected in flash memory. The professional installer/end-user cannot access the flash memory.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	There is a country code regulatory parameter to limit user to operate the device outside its authorization in the U.S.
	c) What parameters are accessible or modifiable by the end-user?	None. End user only could select which master(AP) to connect and input password.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes. Some parameters are programmed in driver and firmware are embedded in system, and the installer cannot access them. Also, the system firmware protected in flash memory. The professional installer/end-user cannot access the flash memory.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	There is a country code regulatory parameter to limit product to operate the device outside its authorization in the U.S.
	d) Is the country code factory set? Can it be changed in the UI?	Yes, country code is factory set, and can not 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.?	It can not be changed. There is a country code regulatory parameter to limit product to operate the device outside its authorization in the U.S.
	e) What are the default parameters when the device is restarted?	All default parameters are programmed in driver and firmware which would be embedded in system firmware. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
	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. The device can not be configured in both 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?	No, end-user can not configure the WiFi device to be as a master or 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))	The device is not a access point.