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.	Wifi driver and firmware are embedded in system firmware and there is not any installation process.
	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 default parameters approved by the FCC are programmed in both driver and firmware which would be embedded in system firmware. End-user cannot access them.
	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.	Wifi driver and firmware are embedded in system firmware and there is no any installation process. All default parameters are programmed in both driver and firmware which would be embedded in system firmware. End-user cannot access them.
	4	Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	The wifi device needs specific driver and firmware to operate; the driver and firmware would recognize some IDs to confirm if the chip is correct. The driver would read the country code regulatory parameter to limit product to operate the device under its authorization in the U.S.
	5	Describe, if any, encryption methods used.	No encryption, but wifi firmware is a binary code.
	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?	The device can be configured as a master and client. Changing between master and client can be done with the selection in the UI. And 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 master or client to meet UNII requirements.
Third-Party Access Control	1	How are unauthorized software/firmware changes prevented?	Wifi driver and firmware are embedded in system firmware and there is no any installation process. System firmware is programmed and protected in flash memory.
	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.	Wifi driver and firmware are embedded in system firmware and there is not any installation process. System firmware is programmed and protected in flash memory. All default parameters are programmed in both driver and firmware which would be embedded in system firmware. End-user cannot access them.
	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. There is a country code regulatory parameter to limit user to operate the device outside its authorization in the U.S. End-use cannot access that parameter.
	4	What prevents third parties from loading non-US versions of the software/firmware on the device?	Wifi driver and firmware are embedded in system firmware and there is not any installation process. System firmware is programmed and protected in flash memory. The third-party cannot access that flash memory.
	5	For modular devices, describe how authentication is achieved when used with different hosts.	Wifi driver and firmware are embedded in system firmware and there is not any installation process. System firmware is programmed and protected in flash memory. The third-party cannot access that flash memory.
SOFTWARE CONFIGURATION DESCRIPTION			
USER CONFIGURATION GUIDE	1	To whom is the UI accessible? (Professional installer, end user, other.)	Wifi driver and firmware are embedded in system firmware and there is not any installation process. System firmware is programmed and protected in flash memory with users are not able to modify the content.
		a) What parameters are viewable to the professional installer/end-user?	All default parameters are programmed in both 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. End user could select which master(AP) to connect in the client mode. And end user could change SSID, password and the use of security in the master mode.
		b) What parameters are accessible or modifiable to the professional installer?	None.
		i) 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 wifi driver and firmware which are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
		ii) 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 configuration options are available to the end-user?	End user could select which master(AP) to connect in the client mode. And end user could change SSID, password and the use of security in the master mode.
		i) 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 wifi driver and firmware which are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
		ii) 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 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't be changed in UI.
		i) If so, what controls exist to ensure that the device can only operate within 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.
		e) What are the default parameters when the device is restarted?	All default parameters are programmed in both 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.	There is no control to change between bridge and 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 device can be configured as a master and client. Changing between master and client can be done with the selection in the UI. And 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 master or client to meet UNII requirements.
	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 can be configured as a master and client. Changing between master and client can be done with the selection in the UI. And 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 master or client to meet UNII requirements.