Software Security Description – KDB 594280 D02v01r03 Section II	
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. ANS: The software is developed and designed by the manufacturer, pre-recorded in the system, and can be updated via USB/OTA. The update does not involve modification of RF parameters.
	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? ANS: After the device is certified according to relevant standards, software updates do not involve RF parameter modifications1.
	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. ANS: The pre-recorded software is independently developed by our company
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. ANS: The device uses compiled binary code, making it difficult to crack
	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? ANS: The device uses a standardized WiFi RF IC, which cannot be modified
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. ANS: The software is updated via USB/OTA, and it is compiled into binary code, making it difficult for third parties to crack. Additionally, the update does not involve any modifications to RF parameters
	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.

	ANS: After the device is pre-recorded, it cannot be modified and does not support third-party software modifications to RF parameter settings
	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. ANS: The device does not support modifying RF parameters through software

Software Configuration Description – KDB 594280 D02v01r03 Section III
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.

a. What parameters are viewable and configurable by different parties?

ANS:

The device can only view WiFi SSID/PW and encryption methods, but cannot view RF parameters

b. What parameters are accessible or modifiable by the professional installer or system integrators?

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

ANS:

The device does not open control permissions

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

ANS:

The device does not open control permissions

c. What parameters are accessible or modifiable by the end-user?

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

ANS:

The device can only view WiFi SSID/PW

(2) What controls exist that the user cannot operate the device outside its authorization in t U.S.?

ANS:

The device does not open control permissions

d. Is the country code factory set? Can it 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.?

ANS:

No country code and device does not support modifying parameters through ui

---

e. What are the default parameters when the device is restarted?

ANS:

The parameters are stored inside the IC and are re-read every time the device is started

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.

ANS:

It cannot be set

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?

ANS:

During production, the RF section of the device complies with standards, and users cannot modify RF parameters

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))

ANS:

The antenna is inside the machine and uses a special type of antenna that cannot be replaced