MEDIT

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. Firmware updates for the device can only be performed through the manufacturer's software. • Users or administrators log in to the manufacturer's secure server and download the firmware using an authenticated account. • The integrity and legitimacy of the firmware are verified using a SHA-256 hash. • Only when the verification is successfully completed does the firmware installation begin. General users do not have access to the firmware update function and only receive automatic update notifications.
	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? In this device, the following RF parameters can be configured in a limited manner through firmware without hardware modification: • Transmit power • Channel number or channel bandwidth • Communication mode However, all these parameters can only be adjusted within predefined configuration ranges, which are designed to prevent exceeding the certified RF characteristics (such as transmit power, spectrum mask, frequency range). Specifically, • The certified parameter values are hardcoded in the firmware as upper limits, so settings exceeding these values cannot be applied. • The values that users can access are restricted in the UI, and even with administrator privileges, RF-related values cannot be directly entered or manipulated. • All RF settings are automatically verified to be within the RF authorization range by integrity verification logic when the device boots or when settings are changed.

	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 firmware installation module verifies the SHA-256 hash value before executing the firmware. If the verification fails, the installation or booting is halted and the device enters an error state. Firmware distribution is only possible via the central server or by authorized installers.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. An encrypted authentication protocol is used. During the wireless authentication process, authentication is performed through an encrypted challenge-response method. For example, the device receives an encrypted random value from the server and returns a response encrypted with a secret key, thereby verifying legitimacy.
	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? N/A
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. Such a method constitutes a violation of FCC regulations, and third parties cannot operate the device in that way. Such a method constitutes a violation of FCC regulations, and third parties cannot operate the device in that way.

	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. Installation of third-party software/firmware is not permitted.
	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. N/A

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?

Professional Installer: Channel selection (within approved frequency range), operation mode, system log, and advanced network settings
General User: SSID and password changes only

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?

Yes. Channel selection, operation mode, etc., are all restricted so as not to exceed FCC-approved parameter ranges. Settings outside permitted ranges are hidden or disabled in the UI, and internal system restrictions are also applied.

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

A limited UI is provided by default, and settings through the UI are blocked by software from exceeding approved firmware-defined ranges.

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 that exceed those authorized?

Only general network settings such as SSID and password are accessible, and all items are restricted not to exceed FCC-certified ranges.

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

Advanced RF-related items are not displayed in the general user UI.

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.?

The country code is factory-set to Korea (KR), and when the device is operated in the U.S., it is forcibly set to "US" by the manufacturer's software.
Users cannot change this manually.

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

Upon restart, the device operates based on previously stored settings that comply with FCC authorization.

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.

Not supported.

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))

The antenna is fixed and cannot be changed.
The device is designed not to produce output that exceeds FCC regulations regardless of its operation mode.