FCC ID: 2ACCJB157

This device compliance with the latest revision of KDB publication 594280 D02 U-NII Device Security v01r03:

The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within HH500V Security.

The information below describes how we maintain the overall security measures and systems so that only:

1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

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.	The software/firmware update is bundled, as part of "System updates" process, the user or installer cannot modify the contents. The update and installation proceed automatically once the user accepts or launches "System updates" 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?	Radio parameters are fixed at time of production as required by the FCC certification. Any future software/firmware release for "System updates" is verified by the TCL before release. If required, TCL will follow FCC permissive change procedure.
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.	Radio parameters are fixed at time of production as required by the FCC certification. Any future software/firmware release for "System updates" is verified by the TCL before release. If required, TCL will follow FCC permissive change procedure.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Yes, see answer to #1 and #3.
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?	For a device act as a master, the 5G channel bands of operation will be restricted by regional regulations profile. And 2.4G channel bands is randomly chosen from Channel 1/Channel 6/Chanel 11. The device not act as a client

3rd 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.	No third-parties will get rights to modify system property and files.
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.	No
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.	Not applicable, this device is not a module.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
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.	The device only support owner through the UI, it can do the normal configuration, but it is not accessible to change the RF parameters
a) What parameters are viewable and configurable by different parties?	Parameters which are related to RF characteristics and compliance are not accessible to users.
b) What parameters are accessible or	This device is not subject to professional installation.

[1] This section is required for devices which have a "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter. Supporting information is required in the operational description. The operational description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
modifiable by the professional installer or system integrators?	
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Not applicable, end user has no chance to access parameters.
c) What parameters are accessible or modifiable by the end-user?	The parameters related to RF operation and compliance are not accessible to end users
i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	No.
ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	The parameters related to RF operation and compliance are not accessible to end users
d) Is the country code factory set? Can it be changed in the UI?	No, country code is set by software firmware, it can be changed only by software firmware update, it can't be changed by UI.
i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	country code is set by software firmware, it can be changed only by software firmware update through TCL
e) What are the default parameters when the device is restarted?	the parameters used and reported in the equipment 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.	No, Not configured.
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, Not supported.
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 DUT support these modes/features