FCC ID: 2AYXT61100004
IC: 29927-61100004

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES REF KDB 594280 D02 U-NII Device Security v01r03	
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 device connects to a manufacturer backend service over https and downloads a software update. Authenticity of the software update is validated with a public-private key signature of the software update.
	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 nay other software/firmware changes will not allow the device to exceed the authorized RF characteristics? Tx power limits are set as driver parameters in software/firmware. These parameters are not exposed in any way externally. They are also not controlled by any other applications, are static, and built directly into the firmware without the ability to update at runtime. These parameters are managed by engineering teams with best practices in place to prevent modification.
	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. Firmware images are signed with a private key. Software/firmware images that are not properly signed will not be accepted to update a device.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. RSA encryption is used for software/firmware update keys
	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? Does not apply
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. No, based on our protocols described above, no third parties have the capability to operate any U.S.-sold devices in violation of the device's authorization.
	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, the device does not permit third-party software or firmware installation.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization. N/A; not a module

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. The user cannot configure any RF functions.
	a) What parameters are viewable and configurable by different parties? No parameters related to RF performance are configurable by any users.
	b) What parameters are accessible or modifiable by the professional installer or system integrators? No parameters related to RF performance are configurable by any users.
	c) What parameters are accessible or modifiable by the end-user? No parameters related to RF performance are configurable by the end-user.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? There are no RF parameters that are accessible by any installers.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? There is no control available to the user to allow them to operate the device outside authorized settings. These settings are not exposed, and the device is secured with ssh keys and passphrases.
	d) Is the country code factory set? Can it be changed in the UI? The country code is not factory set and cannot 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.? N/A
	e) What are the default parameters when the device is restarted? The default parameters when the device is restarted are taken from the same calibration file that is installed on the device at the factory.
	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. N/A
	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? This cannot be set in the UI
	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 cannot be set as an access point and there are no UI controls for this