

## SOFTWARE SECURITY INFORMATION

**FCC ID:** EF400189

Pursuant to:

FCC Part 15E 15.407(l) and KDB 594280 D02 UNII Device Security v01r03.

The information within this section is to show compliance against the SW Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03. The information below describes how to 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.**

SOFTWARE SECURITY DESCRIPTION		
	Requirement	Answer
<b>General Description</b>	1. Describe how any software/firmware updates for elements that 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 factory firmware is produced by Grantee and it is delivered to the factory via a secured channel. The factory loads the firmware to the device on the production line with specialized tools not available to consumers. After setting up the device by the user for the first use all firmware upgrades are automatically delivered from Grantee's secure SW repository via a secure upgrade channel(encrypted and digitally signed) that prevents any tampering. The user cannot install any firmware not authorized by Grantee.
	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 is verified by the Grantee before release. If required, Grantee 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.	Yes, software/firmware is digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Yes, see answers 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?	This device only supports Client mode, please refer to test report for compliance ensured in each band of operation.

	Requirement	Answer
<b>Third Party Access Control</b>	1. Explain if any third parties have the capability to operate a U.S./Canada -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./Canada.	Only Grantee can release or make changes to the software/firmware using proprietary secure protocols
	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./Canada. 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, refer to the answers #1, 2, and 3 under General Description
	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 modular.

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

SOFTWARE CONFIGURATION DESCRIPTION		
	Requirement	Answer
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.	Only the End user configuration is permitted. 1. The radio parameters are not accessible through a UI to any operating party. 2. End users are only able to enter a UI that allows connection to an established AP network and WPS configuration.
	a) What parameters are viewable and configurable by different parties?	None that affects compliance
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	None that affects compliance
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Not applicable as these types of settings are not accessible to any operating party.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	The device does not allow third-party access to software / firmware parameters or configurations including operation outside the scope of FCC authorization.
	c) What parameters are accessible or modifiable by the end-user?	None that affects compliance
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Not applicable
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	The device does not allow third-party access to software / firmware parameters or configurations including operation outside the scope of FCC authorization.
	d) Is the country code factory set? Can it be changed in the UI?	The country code is hardcoded into the device firmware 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./Canada?	Not applicable
	e) What are the default parameters when the device is restarted?	1. Network/Wi-Fi Configured device would be acting in Wi-Fi-station (client) mode after device is restarted 2. All Wi-Fi parameters are subjected to connected Wi-Fi Access Point (Home router) 3. Network un-configured device (at factory reset condition) would be acting as Wi-Fi Access Point in 2.4 GHz band.
	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
	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	1. The device enforces compliance via the signed software 2. The maximum output power is restricted by setting limits based on our FCC test results

	<p>some bands and client in others, how is this configured to ensure compliance?</p>	<p>3. The device supports either (Wi-Fi Access Point) master or (Wi-Fi station) client mode. It can't act as both master and client at same time.          4. Device supports only 2.4GHz band in master mode.          5. No Wi-Fi parameters can be configured by end-user / installer.          6. The maximum output power is the same regardless of whether it functions as a master or a client.          7. Device doesn't support ad-hoc, Wi-Fi direct modes</p>
	<p>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)).</p>	<p>1. The device can't be configured as different types of access points.          2. No support for external antenna is provided in the device</p>

**Company Information: Nortek Security & Control LLC**  
**Name and surname of applicant (or authorized representative): Horsen Ma**

**Date: 2020.6.30      Signature: *Horsen Ma***