

SOFTWARE SECURITY DESCRIPTION (KDB 594280 D02 V01r02)

| <u>General Description</u> | |
|----------------------------|---|
| Q1 | Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security. |
| Ans | Only properly authenticated software is loaded and operating the device. The software 6.0 can be accessed through manufacturer's website, but the user can not modify any RF parameters outside of the authorization. |
| Q2 | Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters? |
| Ans | The radio frequency 5180~5240MHz and 5745~5825MHz for this device can not be modified by user except by manufacturer. |
| Q3 | Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification. |
| Ans | The software is protected against modification from key encryption technology. |
| Q4 | Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. |
| Ans | The software 6.0 is encrypted by manufacturer. |
| Q5 | Describe in detail any encryption methods used to support the use of legitimate software/firmware. |
| Ans | Use the key encryption technology. |
| Q6 | 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 can only be configured as client mode, it can not be modified by end user or an installer. |
| | |

Third-Party Access Control

| | |
|-----|---|
| Q1 | Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification. |
| Ans | The Software can not be modified by end user or an installer. |
| Q2 | What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT. |
| Ans | The software and hardware is limited to end user or an installer, it can not be modified otherwise the device can not work properly. |
| Q3 | For Certified Transmitter modular devices, describe how the module grantee ensures that hosts 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 parameters are not modified outside the grant of authorization. |
| Ans | The software and hardware is limited to end user or an installer, it can not be modified otherwise the device can not work properly. |

SOFTWARE CONFIGURATION DESCRIPTION

| | | |
|-----|--|---|
| Q1 | To whom is the UI accessible? (Professional installer, end user, other.) | |
| Ans | Professional installer | |
| | a) | What parameters are viewable to the professional installer/end-user? |
| | Ans | 2.4G/5G WIFI link status, connection operate interface. |
| | b) | What parameters are accessible or modifiable by the professional installer? |
| | Ans | The professional installer can not modify any RF parameters. |
| | (1) | Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? |
| | Ans | The professional installer can not modify any RF parameters. |
| | (2) | What controls exist that the user cannot operate the device outside its authorization in the U.S.? |
| | Ans | The software and hardware is limited to end user or an installer, it can not be modified otherwise the device can not be work properly. |
| | c) | What parameters are accessible or modifiable to by the end-user? |
| | Ans | The end-user can not modify any RF parameters. |
| | (1) | Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? |
| | Ans | The installer can not modify any RF parameters. |
| | (2) | What controls exist that the user cannot operate the device outside its authorization in the U.S.? |
| | Ans | The software and hardware is limited to end user or an installer, it can not be modified otherwise the device can not be work properly. |
| | d) | Is the country code factory set? Can it be changed in the UI? |
| | Ans | No. It can not be changed in the UI. |
| | (1) | If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? |
| | Ans | Manufacturer set up what channel should disable and what channel should used on our initial file. Manufacturer would modify it base on different country. |
| | e) | What are the default parameters when the device is restarted? |
| | Ans | The radio frequency 5180~5240MHz and 5745~5825MHz for this device |
| Q2 | 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 can not be configured in bridge or mesh mode. | |
| Q3 | 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? | |
| | Manufacturer does not provide API to Application. It can not be modified by end user or an installer. | |
| Q4 | 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)) | |
| | Manufacturer does not provide API to Application. It can not be modified by end user or an installer. | |