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. *Description:* Firmware updates are obtained via Lantronix. New firmware can be downloaded via HTTP(S) or FTP; it is automatically installed as it is downloaded into an alternate bank of flash memory. If the download, installation, and verification are all successful, the configuration is updated to boot from the alternate bank, and the device is rebooted automatically.
	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? *Description:* The channel used by the STA interface is determined by the access point to which it is connected. The SOFT AP interface (operating on group owner mode) is limited to the channels listed in the channel table at the end of this document. The Soft AP interface uses the same channel as the STA interface (in the absence of a STA connection the SoftAP may use any of the available non-DFS channels.) The Cypress firmware (running in the radio module) restricts the selection of channels to those listed in the channel table at the end of this document.
	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. *Description:* Firmware upgrade images contain a header that describes the image. The header contains a product code and image type identifiers that are validated for the device, and contains checksums that are validated before the active flash memory bank is switched (see above). The firmware is not directly accessible by the user; the root

	user is disabled and all interactions with the application firmware, kernel, drivers, etc. is through the application firmware user interface(s).
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. *Description:* Encryption is not used in firmware upgrade except for transport when using HTTPS.
	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? *Description:* Compliance with channel restrictions is enforced by the Cypress firmware running in the radio module.
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. *Description:* A regulatory domain setting is accessible to OEM customers which allow them to select the operational country. This setting is only available to OEM customers and is inaccessible to end users.
	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. *Description:* Full disclosure: nothing in the firmware prevents this. There is validation, as mentioned, of information in the ROM header. But the utility used to create that header is in the public domain, as it is released as part of the Lantronix SDK. It should be noted that creating operational firmware and spoofing a valid Lantronix validation header is by no means a trivial effort.
	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. *Description:* The regulatory domain setting, which determines all of the transmitter parameters, is enforced by the firmware running in the radio module. This setting is not accessible by end users.

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?

Description:

Soft AP mode, authentication suite.

The Soft AP interface uses the same channel as the STA interface (in the absence of a STA connection the SoftAP may use any of the available non-DFS channels.) The Cypress firmware (running in the radio module) restricts the selection of channels to those listed in the channel table at the end of this document.

b. What parameters are accessible or modifiable by the professional installer or system integrators?
Description:

Soft AP mode, authentication suite.

The Soft AP interface uses the same channel as the STA interface (in the absence of a STA connection the SoftAP may use any of the available non-DFS channels.) The Cypress firmware (running in the radio module) restricts the selection of channels to those listed in the channel table at the end of this document.

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
Description:

Most parameters, apart from things like configurable passwords, are selectable from pre-defined lists. All transmission parameters are controlled by the regulatory domain, which is only configurable in the factory.

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

Country code settings are factory configurable only and not available to the end

user.

c. What parameters are accessible or modifiable by the end-user?
Description:

The mode is selectable between Soft AP. The authentication suite is configurable. All transmission parameters are controlled by the regulatory domain, which is only configurable in the factory.

(1) Are the parameters in some way limited, so that the installers will not enter parameters t exceed those authorized?

Description: Yes

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

Description:

Country code settings are factory configurable only and not available to the end user.

d. Is the country code factory set? Can it be changed in the UI?
Description:

Yes, it is factory set. It 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.?

Description:
The regulatory domain (country code) can only be set in the factory.

e. What are the default parameters when the device is restarted?
Description:
The device maintains its programmed configuration trough a reboot.

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.
Description:
It can be configured for Wi-Fi to Ethernet bridging. No mesh support.

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?
Description:
These controls are not user configurable.

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))

Description:

The unit data sheet lists the antennas that are qualified for use with the product and provides instructions for their usage. The antennas stated in the data sheet were validated as part of this certification package. The data sheet was submitted as part of the certification package to fulfill the user manual requirement.

20Mhz Channels

		Region:		
	Frequency	**Channel**	**Scan Type**	**Client/Soft AP**
2.4 GHz Band	2412	**1**	Active	Yes
	2417	**2**	Active	Yes
	2422	**3**	Active	Yes
	2427	**4**	Active	Yes
	2432	**5**	Active	Yes
	2437	**6**	Active	Yes
	2442	**7**	Active	Yes
	2447	**8**	Active	Yes
	2452	**9**	Active	Yes
	2457	**10**	Active	Yes
	2462	**11**	Active	Yes
	2467	**12**	N/A	N/A
	2472	**13**	N/A	N/A
	2484	**14**	N/A	N/A
5 GHz Band	5180	**36**	Active	Yes
	5200	**40**	Active	Yes
	5220	**44**	Active	Yes
	5240	**48**	Active	Yes
	5260	**52**	Passive	Yes
	5280	**56**	Passive	Yes
	5300	**60**	Passive	Yes
	5320	**64**	Passive	Yes
	5500	**100**	Passive	Yes
	5520	**104**	Passive	Yes
	5540	**108**	Passive	Yes
	5560	**112**	Passive	Yes
	5580	**116**	Passive	Yes
	5600	**120**	Passive	Yes
	5620	**124**	Passive	Yes
	5640	**128**	Passive	Yes
	5660	**132**	Passive	Yes
	5680	**136**	Passive	Yes
	5700	**140**	Passive	Yes
	5745	**149**	Active	Yes
	5765	**153**	Active	Yes
	5785	**157**	Active	Yes
	5805	**161**	Active	Yes
	5825	**165**	Active	Yes

40Mhz Channels

		Region:		
	Frequency	**Channel**	**Scan Type**	**Client/Soft AP**
5 GHz Band	5190	**38**	Active	Yes
	5230	**46**	Active	Yes
	5270	**54**	Passive	Yes
	5310	**62**	Passive	Yes
	5510	**102**	Passive	Yes
	5550	**110**	Passive	Yes

	5590	**118**	Passive	Yes
	5630	**126**	Passive	Yes
	5670	**134**	Passive	Yes
	5755	**151**	Active	Yes
	5795	**159**	Active	Yes

80Mhz Channels

		Region:		
	Frequency	**Channel**	**Scan Type**	**Client/Soft AP**
5 GHz Band	5210	**42**	Active	Yes
	5290	**58**	Passive	Yes
	5530	**106**	Passive	Yes
	5610	**122**	Passive	Yes
	5690	**138**	Passive	Yes
	5775	**155**	Active	Yes

Notes:

1. *Frequencies from 5150 Mhz to 5250 Mhz for indoor use only.*
2. *The unit supports 20 MHz bandwidth channels for 2.4 Ghz channels.*
3. *The unit supports 20, 40 MHz bandwidth channels for 5 Ghz channels.*
4. *xPico 270 supports 80Mhz bandwidth channels for 5Ghz channels.*
5. *Country code modifications are not available to the end user.*
6. *If the unit is connected as a client to an external AP, the soft AP channel follows the external AP. Otherwise, the Soft AP defaults to automatically choosing a channel based on RSSI and channel usage. A unit that is not connected to an external AP may also be configured for a specific channel.*
7. *In Soft AP mode, the product will not initiate any connection or active scan in 5G DFS bands and will only follow external AP or master device to use a channel.*