SOFTWARE SECURITY DESCRIPTION	
General Description	any software/firmware is updated by OTA,we will sign the OTA package with OTA private key.if signature of OTA package is not the same with the OTA public key stored in platform,the OTA package will be prevented.
	Device manufacture may change RF parameters by calibration tools provided by chipset manufacture,so that improving the RF performance. But this need database file that must correpond to the current software of the device,so RF parameters are well protected, and other software/firmware will not affect RF parameters.
	this device has e-fuse mechanism to prevent the third image from flashing the device. And it has private release key to prevent invalid OTA package from being updated. The two mechanisms ensure that RF-related software/firmware is valid and protected.
	this device uses RSA encryption methods to generate private key and public key,and e-fuse mechanism ensures public key is not changed, and use password to protect OTA public key.while flashing or upgrading the software ,the device will check the signature of image or OTA package, if they are not the same, then flashing or upgrading will fail
	This device is configured as client mode by default, it only supports client mode, and doesn't support master mode.

Third-Party Access Control	Because there is no software interfact to be open for third parties, they can't modify the RF parameters,so that the device will not violate the authorization of the device
	This device only permit third-party software installation but does not permit third-party firmware, because there is no software interface to be open for third-party,so these software can't modify the RF parameters,and ensure that the RF parameters of the device is authorized
	you may flash third-party ROM to this device and check whether you can flash it,e-fuse mechanism will prevent third-party ROM from being flashed, so RF parameters will be protected. Or you may use calibration tools provided by chipset manufacture to try to modify the RF parameters, you can't get database file,so you can't modify the RF parameters.

SOFTWARE CONFIGURATION DESCRIPTION	
	1. The engineers of manufacture can configure some parameters to debug and locate WIFI issues by using META tools.Using META tools needs database file corresponding to current device software,end-users and third-parties will not get database file, so they can't modify the WIFI parameters.
	a. The engineers of manufacture can configure following parameters,TX/RX power,bandwidth, frequency band etc by META tools,other parties can't configure these parameters.
	b. The engineers of manufacture can only configure WIFI parameters,anyone else can't configure these parameters.

USER CONFIGURATION GUIDE	(1) Yes,only the engineers of manufacture can configure parameters to debug and locate WIFI issues,other installers can't enter parameters.
	(2) There is no interface to modify parameters for the user,so that they only operate the device by default settings and can't operate the device outside its authorization.
	c. There is no any parameters are accessible or modifiable by end-user.
	(1) Yes, No any parameters can't be modified by end-user
	(2) There is no interface to modify parameters for the end-user,so that they only operate the device by default settings and can't operate the device outside its authorization.
	d. Yes, the factory will set the default value of the country code. It cann't be changed in the UI, it will be changed according to the registered network. According to registered network, the device will abtain corresponding country code, then will configure Wi-Fi parameters by the country code,these parameters include TX/RX power,bandwidth, frequency band etc.
	(1) These parameters are stored in NVRAM,and each country code will correspond to different NVRAM record,so this can ensure the device will operate within its authorization.
	e. The default parameters are stored in NVRAM, including following these parameters, TX/RX power,bandwidth, frequency band etc
	2. No
	3. This device is configured as client mode by default, it doesn't support master mode,there is no software interface to be open for user, so user can't modify this.
	4. The different types of access points will use the same antennas, the parameters corresponding to each types will be read from different NVRAM record , so that this can ensure the compliance