

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

(594280 D02 U-NII Device Security 1.3, 11/12/15)

Company Name: Ruckus Wireless, Inc.
FCC ID: S9G-MPE5N33A
Product Name: MPE5N33A Radio Module

<u>General Description</u>	
Q1	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.
Ans	Ruckus releases software updates through Ruckus servers and maintains sole control of distribution of software images to customers. Installation is performed via Ruckus controllers which verify the integrity of the software image downloaded from Ruckus servers.
Q2	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?
Ans	The following R.F parameters can be modified without hardware changes: Channel Frequencies are limited to country code limits. The country code for FCC products is locked during manufacturing and cannot be modified by operators. Channel Bandwidth The AP allows 20/40 or 80MHz channelization to be specified. Restrictions are enforced as per regulatory limits, specified by country code. Transmit Power For host devices with only internal antennas, output power can only be decreased below the FCC allowed powers. The Installer cannot increase output power above authorized RF power levels. For host devices which provide an option for external antennas; when activating the external antenna, the professional installer is given the option of inputting the antenna gain and cable loss. The output power for device is then calculated based on allowed output power limits, EIRP limits, and antenna gain to insure compliance with power limits.

Q3	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.
Ans	Each firmware image contains a header that defines whether the image is valid and matches the capabilities of the board. This header is proprietary and opaque. There is an authentication protocol for the AP to register with an entity that can send firmware updates. The protocol is based on SSL v2. Certificates are embedded into the AP that allows both the firmware and the entity that can send software to mutually authenticate. These servers are maintained by Ruckus Wireless. Ruckus distributes firmware updates only to registered customers.
Q4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
Ans	No encryption used at present. Each firmware image has a signature computed with a signed certificate.
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	Device is only a Master device.

Third-Party Access Control

Q1	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.
Ans	All devices sold in US are locked to US country code. There is no option for Installers or Users to change country code for all devices sold in the US.
Q2	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.
Ans	Each firmware image contains a header that defines whether the image is valid and matches the capabilities of the board. This header is proprietary and opaque. Ruckus APs are factory locked to only function in the US. This lock is performed at the board level, not within the device firmware. So Loading non-US firmware will result in one of two scenarios – 1) the AP will not function or 2) the AP will work with only within the US regulatory limits that are identified by the board level “US” lock. Ruckus uses a bootloader which is only capable of booting Ruckus software images. These images have to be signed by Ruckus build servers using a public cryptographic key. The Trusted computing module on the C500 stores a private key and the signature of the firmware image is sent to the TPM for validation. If validation of these images fails, the image will not be saved into flash memory.
Q3	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.
Ans	This module is installed only in Ruckus branded and manufactured devices. Ruckus Wireless, Inc. has control over the manufacture and installation of all host devices that use the S9GMPE5N33A module.

SOFTWARE CONFIGURATION DESCRIPTION

Q1	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.		
Ans	Professional Installer only.		
	a)	What parameters are viewable and configurable by different parties?	
	Ans	Parameters are only viewable by the professional installer. Configurations are password protected. Please see Exhibit 1: Radio Parameters for screen shots of the GUI Parameters as they are viewed by the professional installer.	
	b)	What parameters are accessible or modifiable by the professional installer or system integrators?	
	Ans	The following R.F parameters can be modified without hardware changes: Channel Channel Bandwidth Transmit Power	
	(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
	Ans	Parameters are limited to country code limits. The country code for FCC products is locked during manufacturing and cannot be modified by operators. Parameters do not allow changes outside of the authorized parameters. For host devices with only internal antennas, output power can only be decreased below the FCC allowed powers. The Installer cannot increase output power above authorized RF power levels. For host devices which provide an option for external antennas; when activating the external antenna, the professional installer is given the option of inputting the antenna gain and cable loss. The output power for device is then calculated based on allowed output power limits, EIRP limits, and antenna gain to insure compliance with power limits.	
	(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?	
	Ans	No Parameters that can affect the compliance of the device can be set or changed by the user or installer when internal antennas are configured. In the case of external antennas, the output power for device is calculated based on the regulatory limits to insure compliance with power limits.	
	c)	What parameters are accessible or modifiable to by the end-user?	
	Ans	The end user has no configuration options. Only professional installers have access to the configuration.	
	(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
	Ans	The end user has no configuration options. Only professional installers have access to the configuration. Configuration does not allow changes outside of the authorized parameters. Only output power calculations when using external antennas rely on information input by the professional installer.	
	(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?	

	Ans	Country code is locked at the factory. There is no option to change the device from the US country code.
d)		Is the country code factory set? Can it be changed in the UI?
	Ans	Country code is locked at the factory. There is no option to change the device from the US country code.
	(1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Ans	There is no option to change the device from the US country code.
e)		What are the default parameters when the device is restarted?
	Ans	Device restarts with last saved parameters.
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		The unit cannot be configured into 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?
Ans		Device is Master device only.
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.
Ans		The unit cannot be configured in bridged or mesh mode. The device requires professional installation. In case of use in a host with external antenna options, the installer is responsible for ensuring that systems employing external antennas are used in compliance with the maximum output power and antenna types approved under the FCC grant.

Exhibit 1: Radio Parameters

Configuration :: Radio 5G :: Common

Common Wireless9 Wireless10 Wireless11 Wireless12 Wire

Radio Network:

Radio 5G

Wireless Mode:

5GHz (802.11ac/a/n) ▾

Channel:

SmartSelect ▾

Channel Width:

40 MHz ▾

Country Code:

United States ▾

Advanced Settings:

Edit Common Settings

Update Settings

[Restore previous settings](#)

Please note: Country Code selection is locked and changes are not available for all product sold in the US. The device cannot be modified to operate outside of US Country Code parameters.

Configuration :: Radio 5G :: Advanced :: Common

Transmit Power:

Full ▾

Protection Mode:

☒ Disabled ☐ CTS-only ☐ RTS-CTS

Update Settings

[Restore previous settings](#)

[« Go back to Wireless Configuration](#)

Output power can only be reduced below “Full” (i.e. powers approved during regulatory approval).

Status :: Radio 5G

Enable Auto-update

CommonWireless9Wireless10Wireless11Wireless12Wireless13

SSID: Wireless9
BSSID: 00:00:00:00:00:00
Wireless Status:  Down
Broadcast SSID?  Enabled
Encryption Mode: Disabled

Connected Devices

No stations are currently associated with this WLAN