

Software Security Requirements Cover Letter

Refer to KDB 594280 D02 U-NII Device Security v01r03.

The applicant has response some questions as below, which can clearly demonstrate how the device meets the security requirements

Software Security Description	
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
	Response: RF parameters can only be configured via Barracuda Secure Connector firmware. Barracuda firmware updates are exclusively available via the download portal (https://dlportal.barracudanetworks.com/). WiFi can be configured as access point or client. Please find WiFi settings for WiFi client mode here: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026756/secure-connector-wan-connections/ Please find settings for WiFi access point mode here: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026757/secure-connector-wi-fi-access-point/
	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?
	Response: Authorized RF characteristics are limited by firmware and hardware. WiFi can be configured as access point or client. Please find WiFi settings for WiFi client mode here: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026756/secure-connector-wan-connections/ Please find settings for WiFi access point mode here: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026757/secure-connector-wi-fi-access-point/

	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
	<p>Response:</p> <p>No such authentication protocols. The RF parameters are put in the read-only partition of device's flash and could only be installed by the factory. RF parameters: frequency operation, power settings and country code.</p>
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	<p>Response:</p> <p>Security settings: None, WPA-PSK, WPA2+PSK and Passphrase</p>
	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?
	<p>Response:</p> <p>Device can only be configured as Master XOR Client.</p>
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.
	<p>Response:</p> <p>N/A</p>
	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
	<p>Response:</p> <p>Hardened System. No third-party software or firmware installations allowed or possible.</p>

	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.
	<p>Response:</p> <p>Barracuda is the host manufacturer, thus and firmware and drivers are controlled by Barracuda only. It is not possible to load different drivers.</p>

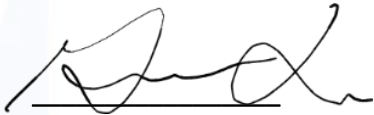
Software Configuration Description	
User Configuration Guide	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.
	<p>Response:</p> <p>No differences for end-users, professional installers, or system integrators. Please find WiFi settings for WiFi client mode here: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026756/secure-connector-wan-connections/</p> <p>Please find settings for WiFi access point mode here: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026757/secure-connector-wi-fi-access-point/</p>
	a) What parameters are viewable and configurable by different parties?
	<p>Response:</p> <p>Please see screen-shots of UI in the Appendix</p>
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	<p>Response:</p> <p>There are no differences for end-user, professional installer or system integrators?</p>
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	<p>Response:</p>

	YES
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	<p>Response:</p> <p>RF parameters restricted by firmware and hardware. User cannot operate the device outside that restriction which is within the authorization in the U.S.</p>
	c) What parameters are accessible or modifiable by the end-user?
	<p>Response:</p> <p>Network Mode, Wi-Fi Channel, SSID, Security Mode, Passphrase Please see screenshots of UI in the appendix.</p>
	1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	<p>Response:</p> <p>YES</p>
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	<p>Response:</p> <p>RF parameters are restricted according to U.S. regulatory by firmware and hardware. User cannot configure settings outside these parameters by software.</p>
	d) Is the country code factory set? Can it be changed in the UI?
	<p>Response:</p> <p>It is on the end-users responsibility to set the correct country.</p>
	1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	<p>Response:</p> <p>User may set different country, but all further setting can only operate within its authorization in the U.S. It is not possible to use settings which are not within its authorization in the U.S.</p>
	e) What are the default parameters when the device is restarted?
	<p>Response:</p> <p>None, there are no default settings. By default WiFi is disabled and needs to be enabled and configured accordingly.</p>
	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.

	Response: N/A
	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?
	Response: Master and Client mode are XOR. You cannot use Master and Client mode at same time.
	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))
	Response: In access point mode only point-to-multipoint is supported. In client mode, only one connection to one access point is possible at same time. Thus, the device using only omnidirectional antennas.

Note: Product (**FCC ID: 2AHVQ-BNET101 & IC: 21331-BNET101**) when it is sale in Canada also satisfy the software security requirement that shown above table. It has individual country code when sale Canada.

Sincerely,



Name: Gary Liu

Position: Hardware NPI Manager

Date: 2022-07-14

APPENDIX:

UI-Location Settings :

Location Specific Settings

Location ☐ Your City

Country ☒ UNITED STATES

State ☐ --not-set--

Located in Timezone ☒ America/Adak

Unit
Optional description for the unit the Secure Connector is used for.

Location
Optional description for the location the Secure Connector is located in.

Country
Optional description for the country the Secure Connector is located in.

State
Optional description for the state the Secure Connector is located in.

UI-WiFi Mode Settings:

Wi-Fi Settings

Wi-Fi Mode ☒ Off

Network Mode ☐ Client-Mode
Access-Point-Manual
Access-Point-Automatic
Access-Point-Mapped

Wi-Fi Channel ☐ Auto

SSID ☐

Name	Active	SSID

Wi-Fi Mode ☒ AP

☒ Wi-Fi enabled

Wi-Fi Mode
The built-in Wi-Fi module can operate in two modes.
In Client mode, it connects to an existing infrastructure and receives the network settings from a DHCP server.
In Access Point mode, the Secure Connector enables clients to connect to a configured SSID and DHCP Server.
The access point can be configured in manual, mapped and automatic mode.
In Manual mode, the IP address and DHCP start/end IPs can be set manually.
In Automatic mode, IP address and DHCP start/end IPs are set by selected data(sub)net.
In Mapped mode, the IP address and DHCP start/end IPs can be set manually and are mapped to selected data(sub)net.
Example: Data network is 172.16.16.0/24 and configured network is 192.168.200.0/24
Configured IP is 192.168.200.200. This IP is set on the LAN port and is mapped to 172.16.16.200
All IPs will be mapped accordingly.

UI-WiFi Client Mode:

Wi-Fi Settings

Wi-Fi Mode ☒ Client-Mode

Network Mode ☒ 802.11g
802.11b
802.11g

Wi-Fi Channel ☐ Auto

SSID ☐

Name	Active	SSID

Wi-Fi Mode ☒ Client

☒ Wi-Fi enabled

Wi-Fi Mode
The built-in Wi-Fi module can operate in two modes.
In Client mode, it connects to an existing infrastructure and receives the network settings from a DHCP server.
In Access Point mode, the Secure Connector enables clients to connect to a configured SSID and DHCP Server.
The access point can be configured in manual, mapped and automatic mode.
In Manual mode, the IP address and DHCP start/end IPs can be set manually.
In Automatic mode, IP address and DHCP start/end IPs are set by selected data(sub)net.
In Mapped mode, the IP address and DHCP start/end IPs can be set manually and are mapped to selected data(sub)net.
Example: Data network is 172.16.16.0/24 and configured network is 192.168.200.0/24
Configured IP is 192.168.200.200. This IP is set on the LAN port and is mapped to 172.16.16.200
All IPs will be mapped accordingly.

Wi-Fi Settings

Wi-Fi Mode

☒ Client-Mode

Network Mode

☒ 802.11g

Wi-Fi Channel

☒ Auto

SSID

☐

1
2
3
4
5
6
7
8
9
10
11

Wi-Fi Mode

☐ Client

☒ Wi-Fi enabled

Wi-Fi Mode

The built-in Wi-Fi module can operate in two modes.

In Client mode, it connects to an existing infrastructure and receives the network settings from a DHCP server.

In Access Point mode, the Secure Connector enables clients to connect to a configured SSID and DHCP Server.

The access point can be configured in manual, mapped and automatic mode.

In Manual mode, the IP address and DHCP start/end IPs can be set manually.

In Automatic mode, IP address and DHCP start/end IPs are set by selected data(sub)net.

In Mapped mode, the IP address and DHCP start/end IPs can be set manually and are mapped to selected data(sub)net.

Example: Data network is 172.16.16.0/24 and configured network is 192.168.200.0/24
Configured IP is 192.168.200.200. This IP is set on the LAN port and is mapped to 172.16.16.200
All IPs will be mapped accordingly.

SSID : SSID01

Active

☒

SSID

☒ TEST123

Security Mode

☒ WPA2-PSK

Passphrase

☒ None
☒ WPA2-PSK
☒ WPA2-PSK

SSID valid for Wi-Fi Mode

☒ Client

Interface Name

☐ WIFI

UI-Access Point Mode Settings:

Wi-Fi Settings

Wi-Fi Mode

☒ Access-Point-Manual

Network Mode

☒ 802.11g
☐ 802.11b
☒ 802.11g
☐ Auto

Wi-Fi Channel

☒ Auto

SSID

☒

Name	Active	SSID
<div> <div><</div> <div></div> <div>></div> </div>		

Wi-Fi Mode

☒ AP

☒ Wi-Fi enabled

Wi-Fi Mode

The built-in Wi-Fi module can operate in two modes.

In Client mode, it connects to an existing infrastructure and receives the network settings from a DHCP server.

In Access Point mode, the Secure Connector enables clients to connect to a configured SSID and DHCP Server.

The access point can be configured in manual, mapped and automatic mode.

In Manual mode, the IP address and DHCP start/end IPs can be set manually.

In Automatic mode, IP address and DHCP start/end IPs are set by selected data(sub)net.

In Mapped mode, the IP address and DHCP start/end IPs can be set manually and are mapped to selected data(sub)net.

Example: Data network is 172.16.16.0/24 and configured network is 192.168.200.0/24
Configured IP is 192.168.200.200. This IP is set on the LAN port and is mapped to 172.16.16.200
All IPs will be mapped accordingly.

Wi-Fi Settings

Wi-Fi Mode	<input checked="" type="checkbox"/>	Access-Point-Manual		
Network Mode	<input checked="" type="checkbox"/>	802.11g		
Wi-Fi Channel	<input checked="" type="checkbox"/>	Auto		
SSID	<input checked="" type="checkbox"/>	<div>Auto</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> <div>6</div> <div>7</div> <div>8</div> <div>9</div> <div>10</div> <div>11</div>		
Wi-Fi Mode	<input checked="" type="checkbox"/>	AP		
<input checked="" type="checkbox"/> Wi-Fi enabled <input checked="" type="checkbox"/>				

Wi-Fi Mode

The built-in Wi-Fi module can operate in two modes.

In Client mode, it connects to an existing infrastructure and receives the network settings from a DHCP server.

In Access Point mode, the Secure Connector enables clients to connect to a configured SSID and DHCP Server.

The access point can be configured in manual, mapped and automatic mode.

In Manual mode, the IP address and DHCP start/end IPs can be set manually.

In Automatic mode, IP address and DHCP start/end IPs are set by selected data(sub)net.

In Mapped mode, the IP address and DHCP start/end IPs can be set manually and are mapped to selected data(sub)net.

Example: Data network is 172.16.16.0/24 and configured network is 192.168.200.0/24
Configured IP is 192.168.200.200. This IP is set on the LAN port and is mapped to 172.16.16.200

All IPs will be mapped accordingly.

SSID : SSID01

— □ ×

Active	<input checked="" type="checkbox"/>	
SSID	Test1234	
Security Mode	WPA2-PSK	
Passphrase	<div>None</div> <div>WPA-PSK</div> <div>WPA2-PSK</div>	
SSID valid for Wi-Fi Mode	Access-Point	
Interface Name	WIFI	