

## WB-1750-KIT AC1750 Wireless Gaming Bridge

# User Manual

Version A1.0, August 2020



## Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at [support@nexuslinkusa.com](mailto:support@nexuslinkusa.com)

For product update, new product release, manual revision, or software upgrades, please visit our website at <http://nexuslinkusa.com>

## Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

### CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.



### WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in [Appendix A - Specifications](#).

## Copyright

Copyright © 2020 NexusLink. All rights reserved. The information contained herein is proprietary to NexusLink. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NexusLink.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>

<b>NOTE:</b> This document is subject to change without notice.
-----------------------------------------------------------------

## Protect Our Environment



This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling center and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

# Table of Contents

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>5</b>
<b>CHAPTER 2 INSTALLATION.....</b>	<b>6</b>
<b>2.1 Hardware Setup .....</b>	<b>6</b>
<b>2.2 LED Indicators .....</b>	<b>8</b>
<b>2.3 Initial Device Setup .....</b>	<b>10</b>
2.3.1 Setup of Wireless Devices via WiFi Protected Setup .....	11
2.3.2 Setup of Wireless Devices via Manual Connection.....	12
<b>CHAPTER 3 WEB USER INTERFACE .....</b>	<b>15</b>
<b>3.1 Default Settings .....</b>	<b>15</b>
<b>3.2 IP Configuration .....</b>	<b>16</b>
<b>3.3 Login Procedure .....</b>	<b>17</b>
<b>CHAPTER 4 LOGIN .....</b>	<b>19</b>
<b>CHAPTER 5 STATUS .....</b>	<b>20</b>
<b>5.1 Status - Device .....</b>	<b>20</b>
<b>5.2 Status – Wireless .....</b>	<b>22</b>
5.2.1 AP Mode.....	22
5.2.2 STA Mode .....	25
<b>5.3 Status – Networking.....</b>	<b>27</b>
<b>5.4 Status – WDS .....</b>	<b>29</b>
<b>5.5 Status – MBSS.....</b>	<b>30</b>
<b>CHAPTER 6 CONFIG.....</b>	<b>32</b>
<b>6.1 Config – Wireless (AP WPA2-AES mode) .....</b>	<b>32</b>
<b>6.2 Config – WPS .....</b>	<b>37</b>
<b>6.3 Config – MAC Filter .....</b>	<b>39</b>
<b>6.4 Config – Networking.....</b>	<b>41</b>
<b>6.5 Config – WDS .....</b>	<b>44</b>
<b>6.6 Config – MBSS.....</b>	<b>46</b>

<b>CHAPTER 7 TOOLS.....</b>	<b>49</b>
7.1 Tools – Log.....	49
7.2 Tools – Admin .....	52
7.3 Tools – Restore.....	53
<b>CHAPTER 8 SYSTEM.....</b>	<b>54</b>
8.1 System – Upgrade .....	54
8.2 System – Reboot .....	56
<b>APPENDIX A - SPECIFICATIONS.....</b>	<b>57</b>

# Chapter 1 Introduction

The WB-1750 is an 802.11ac 4T4R Wireless Gaming Bridge, with two Giga Ethernet ports. WB-1750 performs AP to transmission package TCP/UDP to client, also supporting Station mode, receiving packets and forwarding to the Ethernet port.

The WB-1750 has a high power wireless design which supports 802.11ac 5Ghz band 4T4R and is backward compatible 802.11n, 802.11a.

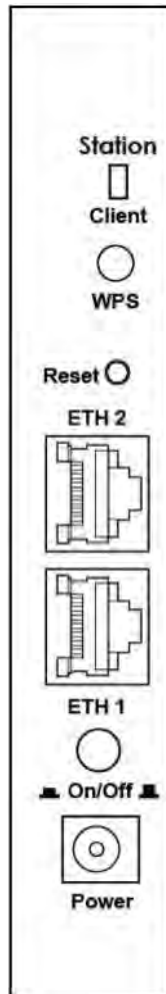
## Chapter 2 Installation

### 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

#### **BACK PANEL**

The figure below shows the back panel of the device.



#### **Power ON**

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section [2.2 LED Indicators](#)).

**Caution 1:** If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.

**Caution 2:** Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

**Ethernet (LAN) Ports**

Use 1000-BASE-T RJ-45 cables to connect two network devices to a Gigabit LAN, or 10/100BASE-T RJ-45 cables for standard network usage. These ports are auto-sensing MDI/X; so either straight-through or crossover cable can be used.

**Reset Button**

To reboot the device press the Reset button for 1-5 seconds. Restore the default parameters of the device by pressing the Reset button for more than 5 seconds. After the device has rebooted successfully, the front panel should display as expected (see section [2.2 LED Indicators](#) for details).

**WPS Button**

Press and release the WPS button to start the WPS connection process with the other device. The connection duration is 2 minutes during which the WPS LED will blink. If there is no client connection the WPS led will turn off. If connection is successful the WPS LED will stay on.

**AP/Station Switch**

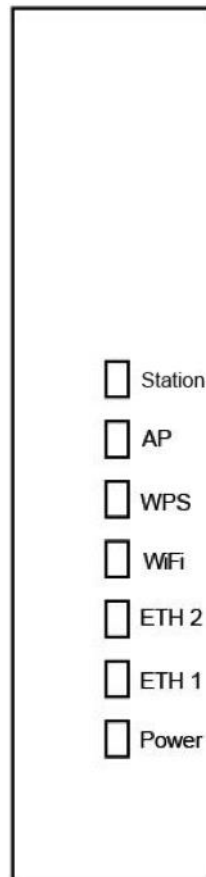
Select the desired option.



## 2.2 LED Indicators

The front panel LED indicators are shown below and explained in the following table.

This information can be used to check the status of the device and its connections.

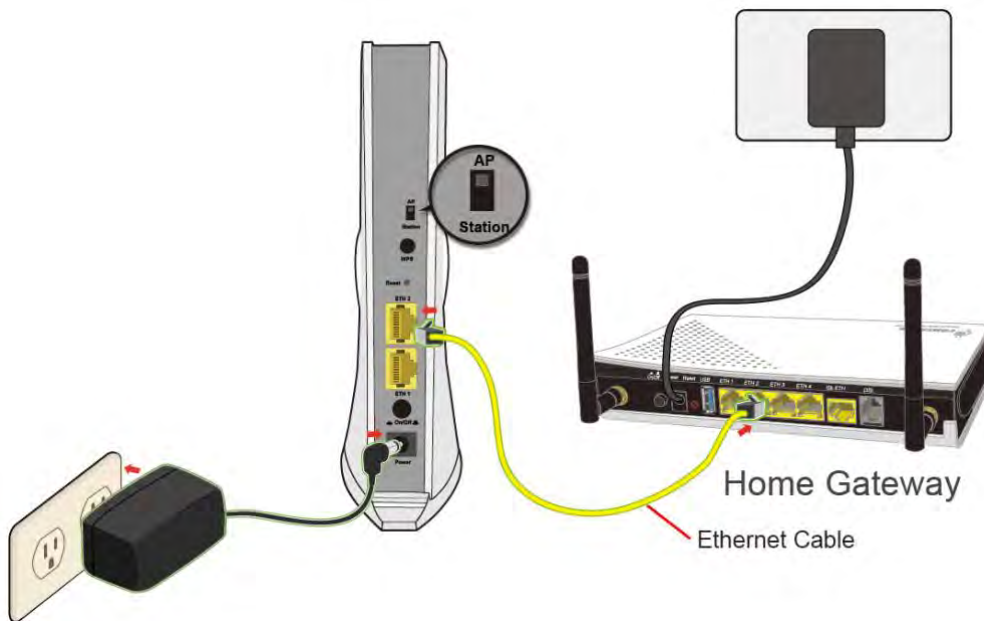


LED	Color	Mode	Description
POWER	GREEN	On	Power on
		Off	Power off
ETH1	GREEN	On	Ethernet connected
		Off	Ethernet not connected
		Blink	Ethernet is transmitting/receiving
ETH2	GREEN	On	Ethernet connected
		Off	Ethernet not connected
		Blink	Ethernet is transmitting/receiving
WiFi	GREEN	On	Wi-Fi enabled
		Off	Wi-Fi disabled
		Blink	[AP] When no client connected [Station] When not connected to the AP
WPS	GREEN	On	WPS connection successful
		Off	No WPS (5G) association process ongoing
		Blink	WPS (5G) connection in progress
AP	GREEN	On	WB-1750 working in AP mode
		Off	WB-1750 working in Station mode
Station	GREEN	On	WB-1750 working in Station mode
		Off	WB-1750 working in AP mode

## 2.3 Initial Device Setup

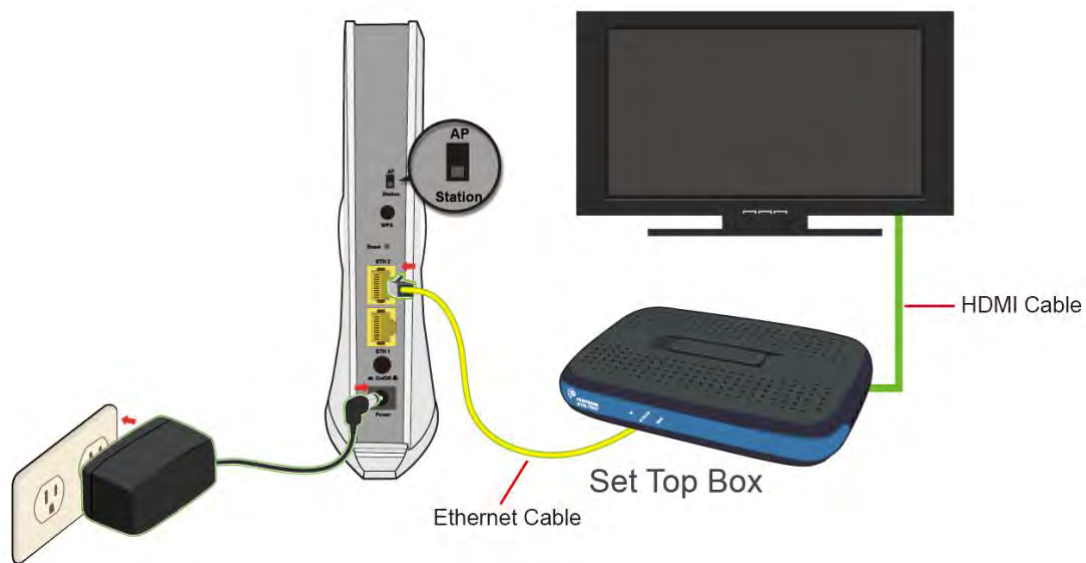
### AP Device Setup

1. Setup the first Wireless Gaming Bridge by plugging in the power adapter and press the **Power Button** to the ON position (IN). Set the Wireless Gaming Bridge to AP Mode by sliding the **AP/Station Switch** to the up position.
2. Connect the Wireless Gaming Bridge to a Network Device (Gateway, Router, etc.) with an Ethernet (RJ-45) cable. You can use either Ethernet ports of the Wireless Gaming Bridge to make this connection.



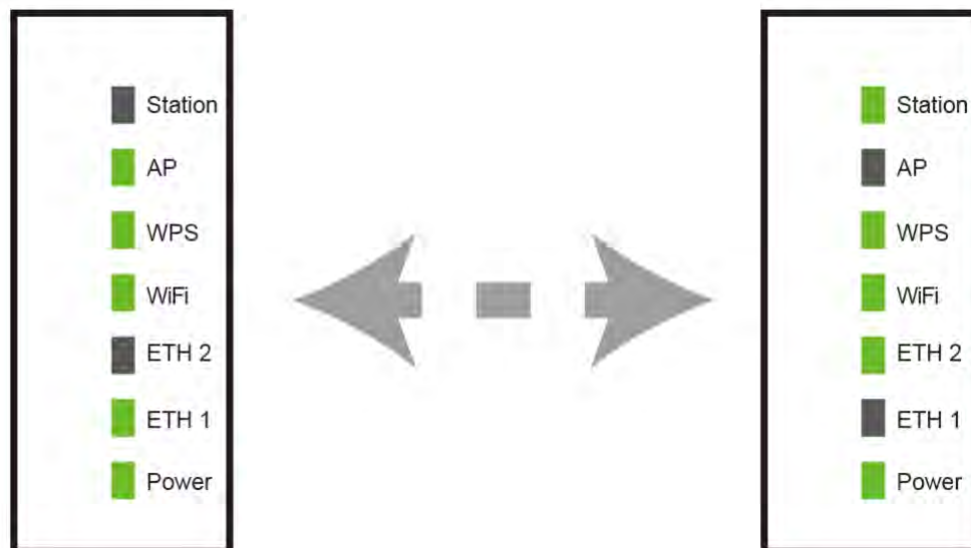
### Client Device Setup

3. Setup the additional Wireless Gaming Bridge closest to the location you want to directly connect the Internet Enabled Device (STB, DVR, etc.). Plug in the power adapter and press the **Power Button** to the ON position (IN). Set the Wireless Gaming Bridge to Station mode by sliding the **AP/Station** to the down position.
4. Connect the Wireless Gaming Bridge to an Internet Enabled Device (STB, DVR, etc.) with an Ethernet (RJ-45) cable. You can use either Ethernet ports of the Wireless Gaming Bridge to make this connection.



### 2.3.1 Setup of Wireless Devices via WiFi Protected Setup

5. Press and release the WPS button on the device setup in AP Mode and the **WPS LED** will start to blink **GREEN**.
6. Within two minutes press and release the WPS button on the device setup in Station mode the **WPS LED** will start to blink **GREEN**.



7. Upon successful connection, the **WPS LED** and **WiFi LED** will light up solid **GREEN** on both of the Wireless Gaming Bridges.
8. Repeat steps 3-6 to add additional client devices.

### 2.3.2 Setup of Wireless Devices via Manual Connection

**NOTE:** If you do not wish to setup your Wireless Gaming Bridges via WPS you can set it up manually.

1. Plug one end of the Ethernet cable into the LAN port of a Notebook/PC (setup with a fixed IP 10.0.0.11 and subnet mask 255.255.255.0) and the other end into the Ethernet port of the Wireless Gaming Bridge that is in Station mode.



2. Open your Internet browser to access 10.0.0.10 and input the Username: root and Password: 12345

A screenshot of the login page for the Wireless Gaming Bridge Web UI. The page has a light gray background. At the top, there is a 'Username\*' label followed by a text input field containing the text 'root'. Below this is a 'Password\*' label followed by a text input field containing five black dots. At the bottom of the form is a large gray button with the word 'LOGIN' in white capital letters.

3. Once you have accessed the Web UI, click Config> Wireless (as shown below). Next, click "Scan AP."

4. Select an SSID (AP unit) and input the passphrase. The SSID and passphrase (**WiFi Key**) can be found a label on the bottom on the Wireless Gaming Bridge. Next, click "connect."

**SSID : NexusLinkE221**

**WiFi Key : 265940E221**

	SSID	Mac Address	Channel	RSSI	Security
1	NexusLinkE221	00:26:59:40:e2:22	149	48	Yes
2	don5G	d8:b6:b7:07:e1:4d	149	46	Yes
3	Dr-Chiang-5G	64:09:80:4f:2d:0e	149	33	Yes
4	iccfliht-master5G	c4:a8:1d:8f:16:f6	149	15	Yes
5	D430ACS5G	80:1f:02:07:e3:4e	44	11	Yes

Current SSID: ComtrendE221

Passphrase: 265940E221 x

Connect

Rescan

5. To confirm that the connection is successful, check that the current SSID is the same as the one that you tried to connect to in the previous step.

## ACCESS POINT LIST

Current SSID: NexusLinkE221

	SSID	Mac Address	Channel	RSSI	Security
1	NexusLinkE221	00:26:59:40:e2:22	149	50	Yes
2	don5G	d8:b6:b7:07:e1:4d	149	46	Yes
3	Dr-Chiang-5G	64:09:80:4f:2d:0e	149	31	Yes
4	icflight-master5G	c4:a8:1d:8f:16:f6	149	14	Yes
5	D430ACS5G	80:1f:02:07:e3:4e	44	10	Yes
6	CTMIS-INT-5G	74:da:38:40:e0:f3	153	54	No
7	CTMIS-INT-5G	d8:b6:b7:07:dd:d1	36	21	No
8	CTMIS-INT-5G	74:da:38:40:e0:ed	149	13	No
9	CTMIS-INT-5G	d8:b6:b7:07:dd:d3	161	10	No
10	CTMIS-INT	80:1f:02:57:22:aa	161	10	No

Rescan

## Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 6.0 and later).

### 3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address AP: 10.0.0.2
- LAN IP address STA: 10.0.0.10
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root**, password: **12345**)

**Caution:** The LAN setting default is DHCP mode, if a device connects to the DHCP network, the LAN IP will be changed by the DHCP server assigned.

#### **Technical Note**

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than ten seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.



## 3.2 IP Configuration

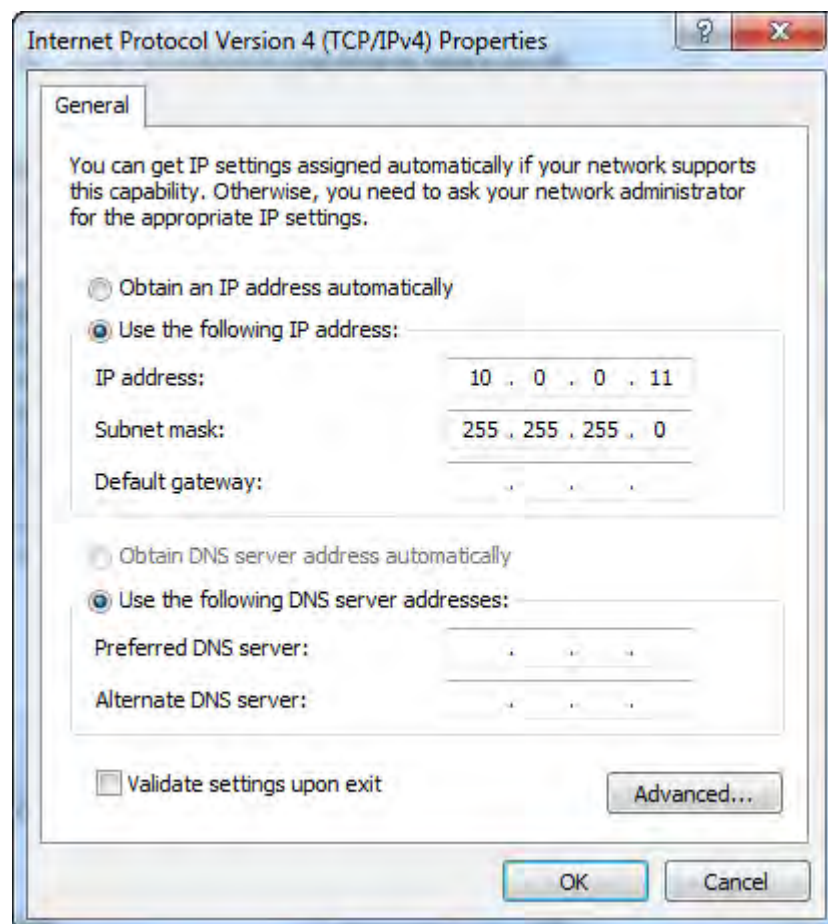
### STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

Follow these steps to configure your PC IP address to use subnet 10.0.0.x.

**NOTE:** The following procedure assumes you are running Windows. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

- STEP 1:** From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the **Properties** button.
- STEP 2:** Select Internet Protocol (TCP/IP) **and click the** Properties button.
- STEP 3:** Change the IP address to the 10.0.0.x (10<x<254) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



- STEP 4:** Click **OK** to submit these settings.

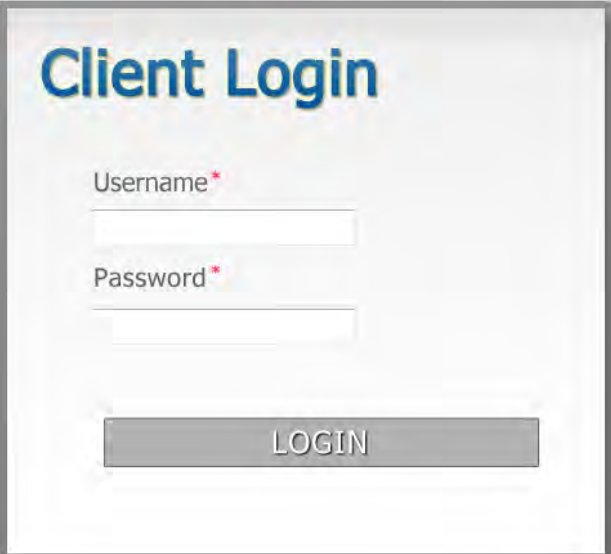
## 3.3 Login Procedure

Perform the following steps to login to the web user interface.

**NOTE:** The default settings can be found in section [3.1 Default Settings](#).

**STEP 1:** Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 10.0.0.2, type <http://10.0.0.2>

**STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in section [3.1 Default Settings](#).

A screenshot of a web-based login dialog box titled "Client Login" in a large blue font. Below the title, there are two input fields: "Username\*" and "Password\*", each with a red asterisk indicating a required field. Below these fields is a grey button with the word "LOGIN" in white capital letters. The entire dialog box is centered on a light grey background.

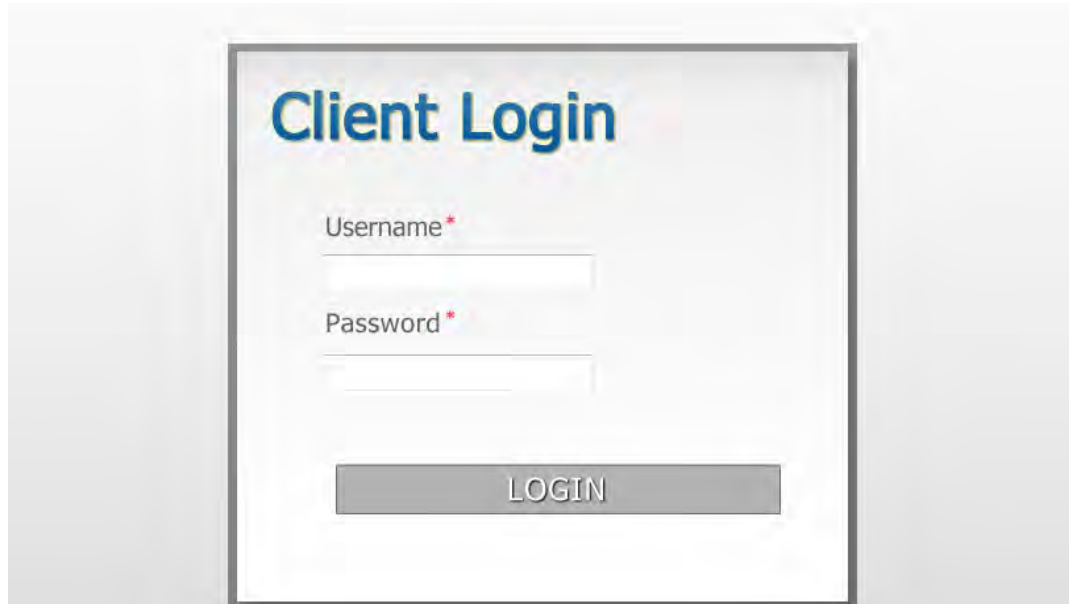
Click **LOGIN** to continue.

**STEP 3:** After successfully logging in for the first time, you will reach the Status - Device screen **AP** (Access Point) shown here.

<b>Status</b>	<b>STATUS - DEVICE</b>
Device	Device Name: WB-1750-KIT
Wireless	Software Version: EM51-3671361CTU-C01_R02
Networking	Uptime: 1min
WDS	Device Mode: <input checked="" type="checkbox"/> Access Point (AP) <input type="checkbox"/> Station (STA)
MBSS	
<b>Config</b>	
Wireless	
WPS	
MAC Filter	
Networking	
WDS	
MBSS	
<b>Tools</b>	
Log	
Admin	
Restore	
<b>System</b>	
Upgrade	
Reboot	

## Chapter 4 Login

- (username: **root**, password: **12345**)

A screenshot of a web form titled "Client Login". The form is enclosed in a light gray border. It features two input fields: "Username" and "Password", both with red asterisks indicating they are required. Below the input fields is a gray button labeled "LOGIN".

**Client Login**

Username \*

Password \*

LOGIN

<http://<address>/login.php>

Please enter the user name and the password to login to the web page system of the device.

## Chapter 5 Status

### 5.1 Status - Device

This screen shows the status of the device.

<b>Status</b>	<b>STATUS - DEVICE</b>
Device	Device Name: WB-1750-KIT
Wireless	Software Version: EM51-3671361CTU-C01_R02
Networking	Uptime: 1min
WDS	Device Mode: <input checked="" type="checkbox"/> Access Point (AP) <input type="checkbox"/> Station (STA)
MBSS	
<b>Config</b>	
Wireless	
WPS	
MAC Filter	
Networking	
WDS	
MBSS	
<b>Tools</b>	
Log	
Admin	
Restore	
<b>System</b>	
Upgrade	
Reboot	

[http://<address>/status\\_device.php](http://<address>/status_device.php)

Menu Item	Description	Options	Detail
<b>Device Name</b>	Name of the NexusLink device		
<b>Software Version</b>	Gets the software version of the current system		The version number of the current firmware
<b>Uptime</b>	Displays the uptime of the device		There are two types of display, one kind is minutes and days, another kind is XX:XX(hours:minutes)
<b>Device Mode</b>	AP or STA mode	Access Point(AP) Station(STA)	Device Acts as Access Point or Station. The [X] indicates the current device mode.

## 5.2 Status – Wireless

This screen shows the wireless status of the device in AP mode.

### 5.2.1 AP Mode

Status

Device  
Wireless  
Networking  
WDS  
MBSS

Config

Wireless  
WPS  
MAC Filter  
Networking  
WDS  
MBSS

Tools

Log  
Admin  
Restore

System

Upgrade  
Reboot

## STATUS - WIRELESS

Wifi Interface: wifi0(00:26:86:F0:3 ▾)

---

Device Mode:

Access Point (AP)

Wireless Band:

802.11ac

Bandwidth:

80 MHz

AP Mac Address (BSSID):

00:26:86:F0:30:81

Channel:

36

Associated Devices Count:

0

Association Table

Packets Received Successfully:

0

Bytes Received:

0

Packets Transmitted Successfully:

4

Bytes Transmitted:

676

Refresh

[http://<address>/status\\_wireless.php](http://<address>/status_wireless.php)

Menu Item	Description	Options	Detail
<b>WiFi Interface</b>	Real wireless device name and MAC Address in CPE		
<b>Device Mode</b>	AP or STA mode	Access Point(AP) Station (STA)	Device Acts as Access Point or Station

<b>Wireless Band</b>	Current system Band	802.11a or 802.11an or 802.11ac	
<b>Bandwidth</b>	Per the 802.11a or 802.11an or 802.11ac standard	20 MHz	20 MHz operation
	Per 802.11an or 802.11ac standard	40 MHz	40 MHz operation
		80MHz(11ac only)	80 MHz operation(11ac only)
<b>AP Mac Address (BSSID)</b>	The current associated BSSID of the Wi-Fi system		In AP mode, it will be the same as the Wireless MAC address
<b>Channel</b>	Available 5Ghz channels based on region setting	36-64, 100-136, 149-161	5.125-5.825, 4.920-4.980 GHz are the supported frequency ranges
<b>Associated Devices Count</b>	The connected devices number		The number of the stations connecting to the AP. Clicking the "Association Table" will link to the Association Table page and display information of all the connected stations.
<b>Packets Received</b>	Wireless packets which are		



<b>Successfully</b>	received successfully		
<b>Bytes Received</b>	The total bytes received successfully		
<b>Packets Transmitted Successfully</b>	Wireless packets transmitted		
<b>Bytes Transmitted</b>	Total bytes transmitted successfully		

This screen shows the information of all station devices which are connecting with the wifi0 of the AP.

ASSOCIATION TABLE							
	Station	VAP	RSSI	Rx Bytes	Tx Bytes	Bw	Time Associated
1	00:26:86:F0:30:83	wifi0	-13 dbm	0	1029512	80	10
2	00:26:86:01:14:43	wifi0	-13 dbm	774	1105666	80	297
<input type="button" value="Refresh"/>							

In above example, STA with MAC address 00:26:86:F0:30:83 and 00:26:86:01:14:43 are currently associated to the primary interface (wifi0), If more MACs are listed, more STA are connected with the wifi0.

[http://<address>/assoc\\_table.php](http://<address>/assoc_table.php)

## 5.2.2 STA Mode

This screen shows the wireless status of the device that acts as a STA.

Status

Device  
Wireless  
Networking

Config

Wireless  
WPS  
Networking

Tools

Log  
Admin  
Restore

System

Upgrade  
Reboot

### STATUS - WIRELESS

Device Mode:

Station (STA)

Wireless Band:

802.

Bandwidth:

80 MHz

AP Mac Address (BSSID):

Not Associated

Channel:

165

Association Status:

Not Associated

Association Table

RSSI:

Not Associated

Packets Received Successfully:

0

Bytes Received:

0

Packets Transmitted Successfully:

0

Bytes Transmitted:

0

Refresh

[http://<address>/status\\_wireless.php](http://<address>/status_wireless.php)

Menu Item	Description	Options	Detail
Device Mode	AP or STA mode	Access Point(AP) Station (STA)	Device Acts as Access Point or Station
Wireless Band	Current system Band	802.11n or 802.11ac	
Bandwidth	Per the 802.11n or 802.11ac standard	20 MHz	20 MHz operation
		40 MHz	40 MHz operation

		80MHz(11ac only)	80 MHz operation(11ac only)
<b>AP Mac Address (BSSID)</b>	The current associated BSSID of the Wi-Fi system		In STA mode and associated to an AP: this will be the value of the AP's MAC address. If the STA is not associated, this will state: "Not Associated".
<b>Channel</b>	Available 5Ghz channels based on region setting	36-48, 149-165	5.180-5.240, 5.745-5.825 GHz are the supported frequency ranges
<b>Association Status</b>	The association status of the device		If the STA has connected with an AP, it will display "Associated". If the STA has not connected with an AP, it will display "Not Associated".
<b>RSSI</b>	Received Signal Strength Indication		A measurement of the power present in a received radio signal. The value is the current RSSI in dBm for the association.
<b>Packets Received Successfully</b>	Wireless packets which are received successfully		

<b>Bytes Received</b>	The total bytes received successfully		
<b>Packets Transmitted Successfully</b>	Wireless packets transmitted		
<b>Bytes Transmitted</b>	Total bytes transmitted successfully		

## 5.3 Status – Networking

This screen shows the status of the networking.

Status

Device

Wireless

Networking

WDS

MBSS

Config

Wireless

WPS

MAC Filter

Networking

WDS

MBSS

Tools

Log

Admin

Restore

System

Upgrade

Reboot

### STATUS - NETWORKING

IP Address:

10.0.0.2

Netmask:

255.0.0.0

Ethernet0 MAC Address:

00:26:86:F0:2F:B9

Ethernet1 MAC Address:

02:26:86:F0:2F:B9

Wireless MAC Address:

00:26:86:F0:30:81

BSSID:

00:26:86:F0:30:81

Refresh

[http://<address>/status\\_networking.php](http://<address>/status_networking.php)

Menu Item	Description	Options	Detail
<b>IP Address</b>	The IP Address of the system		Logged into the web GUI with this IP address. It can be changed in the Config Networking page.
<b>Netmask</b>	The netmask of the IP address		
<b>Ethernet MAC Address</b>	This is the IEEE compliant MAC address of the Ethernet interface		The internal network bridge uses this MAC address
<b>Wireless MAC Address</b>	This is the IEEE compliant MAC address of the Wi-Fi interface		The WLAN MAC address
<b>BSSID</b>	The current associated BSSID of the Wi-Fi system		In AP mode: this will be the SAME as the Wireless MAC address. In STA mode and associated to an AP: this will be the value of the AP's MAC address. If the STA is not associated, this will state: "Not-Associated".

## 5.4 Status – WDS

This screen shows the status of the WDS links.

The screenshot shows a web interface for monitoring WDS links. On the left is a navigation menu with four categories: Status, Config, Tools, and System. The main area is titled 'STATUS - WDS' and features a table with three columns: WDS, MAC Address, and RSSI(dBm). A 'Refresh' button is located below the table.

[http://<address>/status\\_wds.php](http://<address>/status_wds.php)

This option is not available on STA mode, the typical WDS link status includes:

- The interface name of the WDS link, the name is managed by the system automatically, usually it is: WDS0/WDS1/WDS2...so on.
- The WDS peer MAC address of the opposite side, this MAC address is same as the address which you are using when creating WDS links.
- The WDS link quality.

## 5.5 Status – MBSS

This option is not available on STA mode.

[http://<address>/status\\_mbssid.php](http://<address>/status_mbssid.php)

Menu Item	Description	Options	Detail
<b>SSID</b>	SSID of the MBSS		This will be the SSID of the wireless network. The other STA must be configured to the same SSID and security to connect to the Virtual AP.
<b>Broadcast</b>	Enabled or disabled SSID	TRUE	SSID will be broadcasted

	broadcast		
		FALSE	Wi-Fi devices can't scan out this SSID
<b>Association</b>	Associated STA number	$\geq 0$	The number of STAs which are connected to the Virtual AP



## Chapter 6 Config

### 6.1 Config - Wireless (AP WPA2-AES mode)

This screen has two tab pages, "Basic" and "Advanced".

[http://<address>/config\\_wireless.php](http://<address>/config_wireless.php)

#### Basic

The screenshot shows the 'CONFIG - WIRELESS' interface with the 'Basic' tab selected. The left sidebar contains three main sections: 'Status' (Device, Wireless, Networking, WDS, MBSS), 'Config' (Wireless, WPS, MAC Filter, Networking, WDS, MBSS), and 'Tools' (Log, Admin, Restore). The 'System' section (Upgrade, Reboot) is also visible. The main configuration area includes the following fields:

- Device Mode:** A dropdown menu set to 'Access point'.
- ESSID:** A text input field containing 'NexusLink2FB9'.
- Broadcast SSID:** A checkbox that is checked.
- Channel:** A dropdown menu set to 'Auto', with a secondary field showing 'Current Channel:36'.
- PMF:** A dropdown menu set to 'Disabled'.
- Encryption:** A dropdown menu set to 'WPA2-AES'.
- Passphrase:** A text input field containing '2686F02FB9'.
- Group Key interval(in sec):** A text input field containing '3600'.

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Menu Item	Description	Options	Detail
<b>Device Mode</b>	AP or STA mode	Access Point	Device Acts as Access Point
		Station	Device Acts as Station
<b>ESSID</b>	SSID of the AP	Can be set to desired SSID	This will be the SSID of the

		name	wireless network. The STA must be configured to the same SSID and security (see below) to connect to the AP.
<b>Channel</b>	Available 5Ghz channels based on region setting	36-48, 149-165	5.180-5.240, 5.745-5.825 GHz are the supported frequency ranges
<b>PMF</b>	Protected Management Frames		Sets the 802.11w / PMF capability. Applies to AP
<b>Encryption</b>	802.11 compliant authentication and encryption	WPA2/AES	The STA must use WPA2 encryption. This mode is recommended.
		NONE-OPEN	Disables encryption (OPEN mode)
		WPA2 + WPA (Mixed mode)	The STA can use WPA or WPA2 encryption
		WPA2/AES Enterprise	The STA must use WPA2 encryption, and authentication via RADIUS server
		WPA2 + WPA Enterprise	The STA can use WPA or WPA2 encryption, and authentication via RADIUS server
<b>Passphrase</b>	The current		

	passphrase. Applies to AP only.		
<b>Group Key interval(in sec)</b>	Group key renewal interval for enterprise security	Group key interval needs to be between 0 and 43200	This is the interval at which the group key is renewed for clients associated to this SSID

## Advanced

Status

Device

Wireless

Networking

WDS

MBSS

Config

Wireless

WPS

MAC Filter

Networking

WDS

MBSS

Tools

Log

Admin

Restore

System

Upgrade

Reboot

### CONFIG - WIRELESS

Basic Advanced

Wireless Band: 802.11ac  
Bandwidth: 80MHz  


---

NSS: Auto  
TX Rate: Auto  
Priority: 0  
Beacon Interval (in ms): 100  
DTIM Period: 2  
Short GI: ☒  
VLAN:   


---

Save Cancel

Menu Item	Description	Options	Detail
<b>Wireless Band</b>	Frequency Band to be used	802.11a	802.11a 5 GHz operation
		802.11an	802.11an 5 GHz operation
<b>Bandwidth</b>	Per the 802.11a or 802.11an or	20 MHz	20 MHz operation

	802.11ac standard		
	Per the 802.11an or 802.11ac standard	40 MHz	40 MHz operation. Will fall back automatically to 20Mhz if STA does not support 40Mhz. If STA is a NexusLink station device, it will also fall back to 20Mhz.
		80MHz(11ac only)	80 MHz operation(11ac only)
<b>NSS</b>	The maximum number of spatial streams	Auto 1 2 3 4	
<b>Tx Rate</b>	Transmitted data rate	Not support for 802.11a standard	Auto Rate Control, MCS 0-76
		Auto or MCS0 ~MCS76 for 802.11an standard	
		Only Auto for 802.11ac standard	
<b>Priority</b>	The priority is used to differentiate traffic between different SSIDs	0~3	

<b>Beacon Interval</b>	Set the interval of the beacon		How often the device sends a Beacon. The interval should be between 25 and 5000. The default value is 100.
<b>DTIM Period</b>	Delivery Traffic Indication Message		The DTIM period indicates how often clients serviced by the access point should check for buffered data awaiting pickup on the access point. The value should be between 1 and 15.
<b>Short GI</b>	Guard Intervals	Checked	The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). The GI is 400ns.
<b>VLAN</b>	Virtual Lan for different interface	1-4096	

## 6.2 Config – WPS

Connect to AP or STA without selecting an SSID and inputting a Passphrase.

[http://<address>/config\\_wps.php](http://<address>/config_wps.php)

Status	CONFIG - WPS	
Device Wireless Networking WDS MBSS	Wifi Interface: <input type="text" value="wifi0(00:26:86:F0:3 )"/>	
<b>Config</b>	WPS State: <input type="text" value="Configured"/>	
Wireless WPS MAC Filter Networking WDS MBSS	WPS PBC:	<input type="button" value="WPS PBC"/>
	WPS PIN:	<input type="text" value=""/> <input type="button" value="WPS PIN"/>
	WPS AP PIN:	<input type="text" value="12345670"/> <input type="button" value="Regenerate"/>
<b>Tools</b>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
Log Admin Restore		
<b>System</b>		
Upgrade Reboot		

Menu Item	Description	Options	Detail
<b>WPS State</b>	Set WPS states	Disabled	WPS disabled
		Not configured	WPS enabled Client can remotely change AP's wireless settings...SSID, Encryption and Passphrase for example.
		Configured	User needs to fill certain parameters to start WPS connection
<b>WPS PBC</b>	WPS push button		Push button to start WPS connection
<b>WPS PIN</b>	For Web UI pin WPS pin mode	Character string	This will be the PIN used for Web UI WPS pin mode. STA must have same pin.
<b>WPS AP PIN</b>			STA must have same PIN and press same Web UI button within 2 minutes. Recommend to use external WPS push button on the enclosure.

## 6.3 Config – MAC Filter

This screen shows the MAC addresses filtering configurations that are used for the AP.

**MAC ADDRESS LIST**

Wifi Interface:

MAC Address Filtering:

MAC Address:

No results

[http://<address>/config\\_macfilter.php](http://<address>/config_macfilter.php)

Menu Item	Description	Options	Detail
<b>Wifi Interface</b>	Real wireless device name and MAC Address in CPE		
<b>MAC Address Filtering</b>	The device filter MAC address	NONE	The AP can block a selected station from associating based on its MAC (hardware interface) address.



			<p>"NONE"= Disable MAC address filtering.</p> <p>Click the "Config MAC Filter" button link to the MAC ADDRESS LIST page.</p>
		Authorize if not denied	Accept a STA association request unless the MAC address for that STA has been blocked
		Deny if not authorized	Block a STA association request unless the MAC address for that STA has been authorized
<b>MAC Address</b>	Verify the MAC address		Checks whether the MAC address can be connected
<b>MAC Address List</b>	List the authorized or denied MAC addresses		<p>According to the MAC address filter.</p> <p>"Authorize if not denied" filter lists the denied MAC addresses.</p> <p>"Deny if not authorized" filter lists the authorized MAC addresses.</p>

## 6.4 Config – Networking

These screens show the networking configuration.

[http://<address>/config\\_networking.php](http://<address>/config_networking.php)

### DHCP

Status	CONFIG - NETWORKING	
Device	DHCP: <input checked="" type="radio"/> Static IP: <input type="radio"/>	
Wireless	IP Address:	<input type="text" value="10.0.0.2"/>
Networking	Netmask:	<input type="text" value="255.0.0.0"/>
WDS	Ethernet0 MAC Address:	<input type="text" value="00:26:86:F0:2F:B9"/>
MBSS	Ethernet1 MAC Address:	<input type="text" value="02:26:86:F0:2F:B9"/>
	Wireless MAC Address:	<input type="text" value="00:26:86:F0:30:81"/>
	BSSID:	<input type="text" value="00:26:86:F0:30:81"/>
	<div>Save Cancel</div>	

### Static IP

Status

Device

Wireless

Networking

WDS

MBSS

Config

Wireless

WPS

MAC Filter

Networking

WDS

MBSS

Tools

Log

Admin

Restore

System

Upgrade

Reboot

## CONFIG - NETWORKING

DHCP: ☐

Static IP: ☒

IP Address:

10.0.0.2

Netmask:

255.0.0.0

Ethernet0 MAC Address:

00:26:86:F0:2F:B9

Ethernet1 MAC Address:

02:26:86:F0:2F:B9

Wireless MAC Address:

00:26:86:F0:30:81

BSSID:

00:26:86:F0:30:81

Save

Cancel

Menu Item	Description	Options	Detail
<b>DHCP or Static IP</b>	Set the network configuration to DHCP or Static IP	DHCP	The device will try to get its IP address with DHCP from a device like a router
		Static IP	The device will use the static IP address
<b>IP Address</b>	The IP Address of the system		This can be changed from this interface, by editing this field. If the device is using DHCP, the IP address is not allowed to change.

			<b>CAUTION:</b> After selecting "Save", the IP Address will change IMMEDIATELY. The Web UI must be pointed at the new address in order to continue your Web UI Session.
<b>Netmask</b>	Netmask of the IP address		
<b>Ethernet MAC Address</b>	This is the IEEE compliant MAC address of the Ethernet interface		The internal network bridge uses this MAC address. This cannot be changed.
<b>Wireless MAC Address</b>	This is the IEEE compliant MAC address of the Wi-Fi interface.		The WLAN MAC address. This cannot be changed.
<b>BSSID</b>	The current associated BSSID of the Wi-Fi system.		<p>In AP mode: this will be the SAME as the Wireless MAC address.</p> <p>In STA mode and associated to an AP: this will be the value of the AP's MAC address.</p> <p>If the STA is not associated, this will state: "Not-Associated".</p>

## 6.5 Config – WDS

This screen shows the configuration of the WDS links.

WDS	MAC Address	Passphrase	VLAN
<input type="checkbox"/> WDS0:			
<input type="checkbox"/> WDS1:			
<input type="checkbox"/> WDS2:			
<input type="checkbox"/> WDS3:			
<input type="checkbox"/> WDS4:			
<input type="checkbox"/> WDS5:			
<input type="checkbox"/> WDS6:			
<input type="checkbox"/> WDS7:			

Save Cancel

[http://<address>/config\\_wds.php](http://<address>/config_wds.php)

This option is not available if the device is configured as a STA.

Menu Item	Description	Options	Detail
<b>WDS checkbox</b>	To determine if the WDS link is enabled	Checked	The WDS link will be stored to a file after clicking the Save Button

		Not Checked	The WDS link will be discarded after clicking the Save Button
<b>MAC Address</b>		48bit MAC address	The WDS peer MAC address on the opposite side
<b>Passphrase</b>		64 ASCII PSK	Wi-Fi devices can see the SSID in scan. Now the passphrase string is displayed as "*****" instead.
		Empty	The WDS link does not have security
<b>VLAN</b>	Virtual Lan for different interface	1-4096	

## 6.6 Config – MBSS

This option is not available if the device is configured as a STA.

Status

Device  
Wireless  
Networking  
WDS  
MBSS

Config

Wireless  
WPS  
MAC Filter  
Networking  
WDS  
MBSS

Tools

Log  
Admin  
Restore

System

Upgrade  
Reboot

### CONFIG - MBSS

1: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

2: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

3: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

4: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

5: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

6: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

7: ☐

SSID:

VLAN:

Broadcast: ☐ Priority:  
0

PMF:  
Disabled

Encryption:  
NONE-OPEN

Passphrase:

Save

Cancel

[http://<address>/config\\_mbss.php](http://<address>/config_mbss.php)

Menu Item	Description	Options	Detail
<b>SSID</b>	SSID of the MBSS		This will be the SSID of the wireless network. The other STAs must be configured to the same SSID and security to connect to the Virtual AP.
<b>VLAN</b>	Virtual Lan for different interface	1-4096	
<b>Broadcast</b>	Enabled or disabled SSID broadcast	TRUE	SSID will be broadcast
		FALSE	Wi-Fi devices can see the SSID in scan
<b>Priority</b>	The priority is used to differentiate traffic between different SSIDs	0 is highest priority. 3 is lowest priority.	
<b>PMF</b>	Protected Management Frames		Sets the 802.11w / PMF capability. Applies to AP
<b>Encryption</b>	802.11 compliant encryption	NONE-OPEN	Disables encryption (OPEN mode)
		WPA2/AES	The STA must use WPA2 encryption. This mode is recommended.
		WPA2+WPA (mixed mode)	The STA can use WPA or WPA2

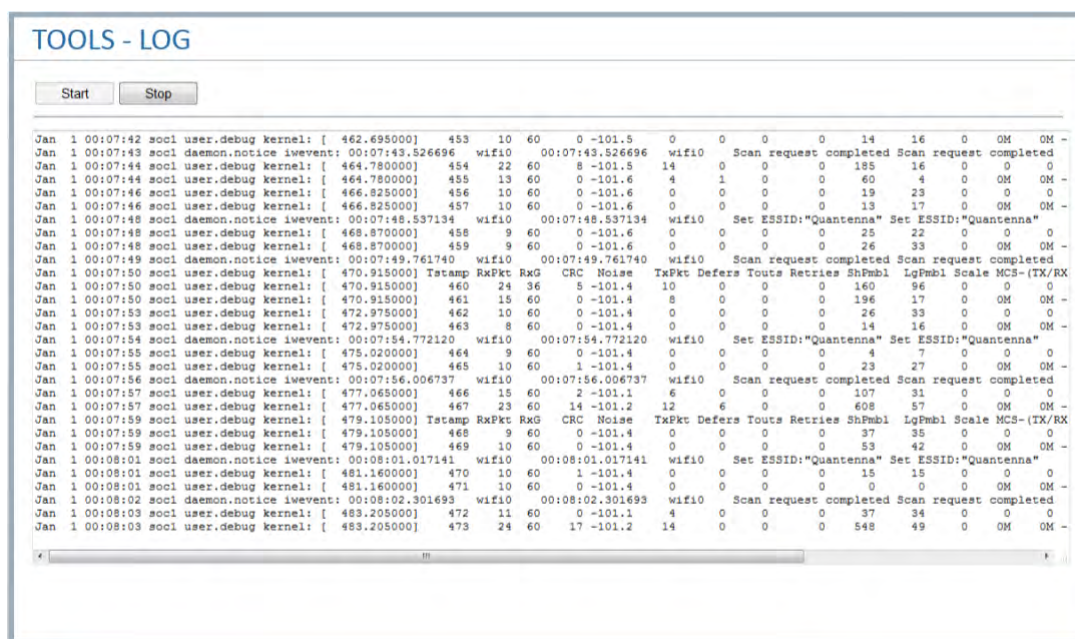


			encryption
<b>Passphrase</b>	The passphrase applies to this MBSS SSID		

## Chapter 7 Tools

### 7.1 Tools – Log

This page has the ability to directly view the PHY statistics of the device.



[http://<address>/tools\\_log.php](http://<address>/tools_log.php)

Pressing the "Start" button will start a 10 second polling log. This data can be useful to assist in debugging the system.

After selecting "Start", the page will look similar to the image above. The logging will stop after pressing the "Stop" button. If the IP address is changed or if the device is shut off, this page will give an error message if logging was in progress. To recover the session, please press the "Start" button again.

This interface takes data from an internal OS file, so intermittently; there may be management messages that show up in this log.

Metric	Description	Comments
Tstamp	This is the system time of	

	the measurement taken from the internal system clock	
<b>RxPkts</b>	This represents the number of packets that were successfully received over 1 second intervals. Each line represents 1 second of time.	
<b>RxGain</b>	This is the higher receiver gain value that was recorded on successfully received packets during this measurement interval. If no packets were received, this may be an invalid number.	The maximum value of RxGain is 62
<b>CRC</b>	This is the number of CRC errors received over the 1 second measurement interval	If (CRC/Rx Packets) > 10-20%, then the channel condition or link quality is poor. This is possibly due to interference, another Wi-Fi network or being too far for the current configuration to be reliable.
<b>Noise</b>	This is the MAX receiver noise floor as measured over this 1 second interval	This value is an internal noise calculation, not external. In normal operation it will vary between 20 and 70.
<b>TxPkts</b>	This is the number of successfully transmitted packets over the last 1 second interval.	

<b>Defers</b>	This number counts the number of times an attempted transmission was deferred due to the medium being busy. This is helpful in determining if an environment is very busy.	Defers are common in busy WiFi environments
<b>Tout</b>	This is an indicator of Tx packet timeout	Timeouts are not common. The Packet could not find a time slot to transmit.
<b>Retries</b>	This counts the number of transmission retries that have occurred over the last one second. This is primarily due to the lack of acknowledgements from the partner device.	On the transmit side, note that the general packet flow for error is as follows:  Defer Retry Timeout
<b>ShPre</b>	This counts the number of Short Preamble Detection Errors	These are very common in high throughput conditions
<b>LgPre</b>	This counts the number of Long Preamble Detection errors	The wireless received a signal which passed the short preamble, but failed the more complex long preamble. These are less common than short preamble errors.
<b>Rate</b>	This is a legacy measurement for rate and is currently not used	

## 7.2 Tools – Admin

This page is for administration of the user passwords.

**Status**

- Device
- Wireless
- Networking
- WDS
- MBSS

**Config**

- Wireless
- WPS
- MAC Filter
- Networking
- WDS
- MBSS

**Tools**

- Log
- Admin
- Restore

**System**

- Upgrade
- Reboot

### TOOLS - ADMIN

User Name:

Old Passphrase:

New Passphrase:

New Passphrase Again:

[http://<address>/tools\\_admin.php](http://<address>/tools_admin.php)

Menu Item	Description	Notes
<b>User Name</b>	The user name for login	Only for the login privilege
<b>Old Passphrase</b>	Enter the original password of the user name	
<b>New Passphrase</b>	Enter the new passphrase	
<b>New Passphrase</b>	Enter the new passphrase	It should be the same as

<b>Again</b>	again	the "New Passphrase"
--------------	-------	----------------------

## 7.3 Tools – Restore

The Tools Restore page is for users to restore all the configurations of the device to factory defaults.

**Status**

Device

Wireless

Networking

WDS

MBSS

**Config**

Wireless

WPS

MAC Filter

Networking

WDS

MBSS

**Tools**

Log

Admin

Restore

**System**

Upgrade

Reboot

TOOLS - RESTORE

Restore all configuration files to factory defaults and reboot?

Restore configuration files to default and reboot, but retain IP settings?

[http://<address>/tools\\_restore.php](http://<address>/tools_restore.php)

The Restore function also restores the password of the login user.

## Chapter 8 System

### 8.1 System – Upgrade

The System Upgrade page is for users to update the firmware on the device.

The screenshot shows a web interface titled "SYSTEM - UPGRADE". On the left is a sidebar with four main categories: "Status" (containing Device, Wireless, Networking, WDS, MBSS), "Config" (containing Wireless, WPS, MAC Filter, Networking, WDS, MBSS), "Tools" (containing Log, Admin, Restore), and "System" (containing Upgrade, Reboot). The "Upgrade" option under the "System" category is highlighted. The main content area has the title "SYSTEM - UPGRADE" at the top. Below the title, it says "Choose a file:" followed by a "Browse..." button and the text "No file selected.". Below this, there is an "Upgrade" button.

[http://<address>/system\\_upgrade.php](http://<address>/system_upgrade.php)

When you select the file and click "Upgrade", the "Upgrade" button will be disabled and the page will display "Loading the image file.....Please wait", please wait for 2 minutes. **Please be patient and do not power off the unit during this process. Do not close the update webpage.**

<b>Status</b> Device Wireless Networking WDS MBSS	<h2>SYSTEM - UPGRADE</h2> <p>Choose a file: <input type="text" value="C01_R02\WAP-5940-EM51-3671361CTU-C01_R02.bin"/> <input type="button" value="Browse..."/></p> <p><input type="button" value="Upgrade"/></p>
<b>Config</b> Wireless WPS MAC Filter Networking WDS MBSS	
<b>Tools</b> Log Admin Restore	
<b>System</b> Upgrade Reboot	

When the firmware has been upgraded successfully, you will be automatically directed to the reboot page.



## 8.2 System – Reboot

The System Reboot page is for users to reboot the device.

<b>Status</b> Device Wireless Networking WDS MBSS	<b>SYSTEM - REBOOT</b>
<b>Config</b> Wireless WPS MAC Filter Networking WDS MBSS	Are you sure to reboot?
<b>Tools</b> Log Admin Restore	<input type="button" value="YES"/>
<b>System</b> Upgrade Reboot	

[http://<address>/system\\_reboot.php](http://<address>/system_reboot.php)

### SYSTEM - REBOOT

---

Rebooting....

Click **here** if you are not redirected automatically after 60s

# Appendix A - Specifications

## Hardware Interface

- AP/Station Switch x 1,
- RJ-45 X 2 for Giga Ethernet port
- Reset Button X 1,
- WPS button X 1,
- Power switch X 1
- Power Jack X 1

## Standard

- 802.11a/n/ac
- 802.11i (WEP, WPA/WPA2, RADIUS)
- 802.11d
- 802.11e (WMM, WMM-PS)
- 802.11w
- 802.11h
- 802.11k
- 802.11r
- 802.11s(Draft)

## Rates are for 256 QAM

- 80MHz: 1.7Gbps
- 40MHz: 800Mbps
- 20MHz: 346.8Mbps

## Environment Condition

Operating temperature .....0 ~ 40 degrees Celsius

<b>NOTE:</b> Specifications are subject to change without notice.
-------------------------------------------------------------------