BAD BOY

Xtreme / Express User's Guide

bitstorm.com
support@bitstorm.com

Table of Contents

Web Management GUI

To access the Web Management GUI, open a browser and type 'http://192.168.100.1' (without the quotes) into the address bar. The Web Management GUI consists of a page with three tabs:

Link Setup contains the controls for a wireless network configuration, which define access point selection and data security options.

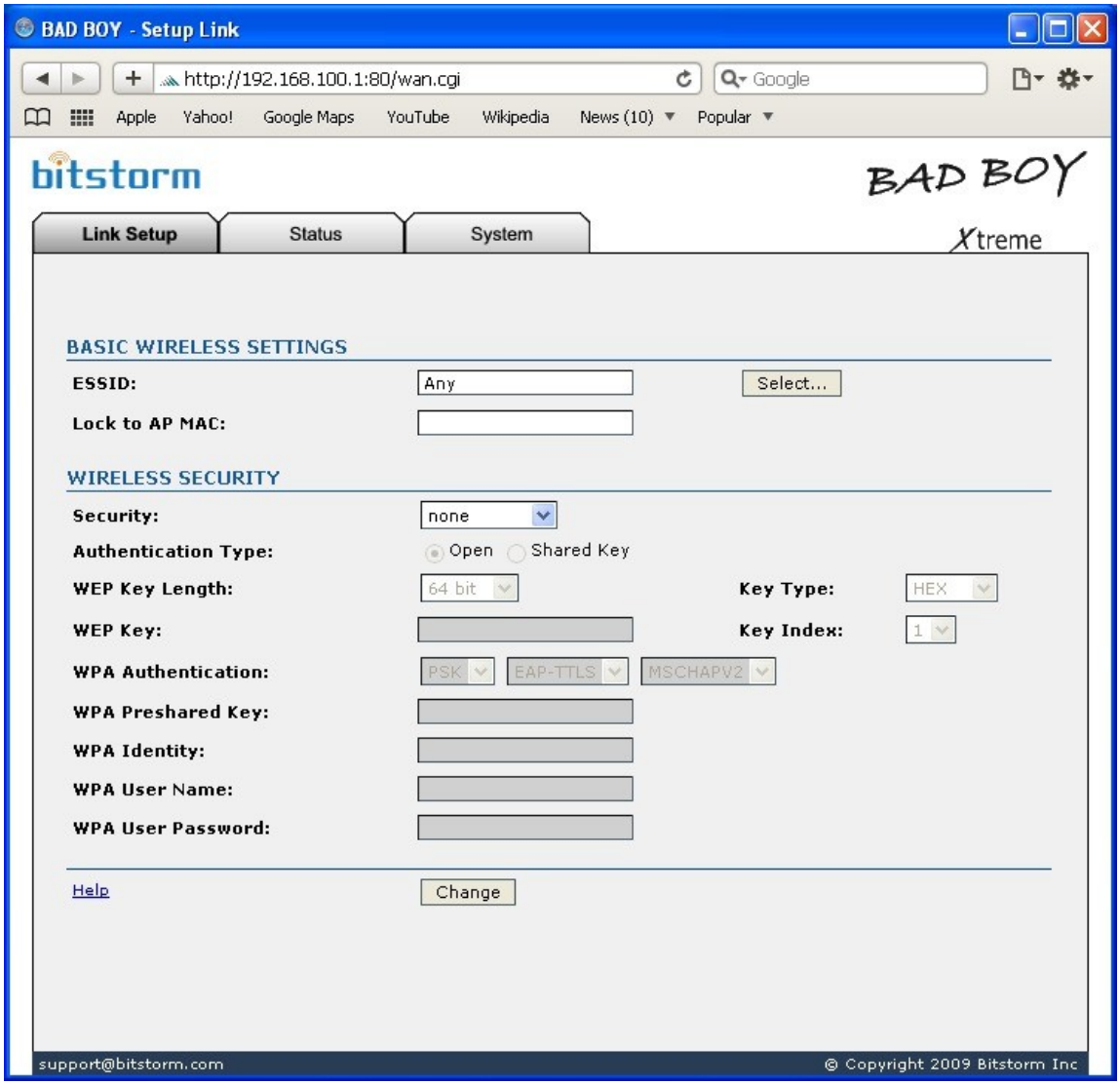
Status displays current status of the device and the statistical information.

System contains controls for administrator account management, interface language, configuration backup or restore and system maintenance.

To conveniently and easy access the Web Management GUI in the future, you can create a favourites item in your browser.

Link Setup tab

The Link Setup tab contains everything needed by the operator to setup the wireless part of the link. This includes wireless security.



Basic Wireless Settings

ESSID: Specify the ESSID of the Access Point which the BAD BOY should associate to. There can be several Access Points with the same ESSID. If the ESSID is set to "Any", BAD BOY will connect to any available Access Point.

SELECT: Click this button to display a page that displays all of the detected Access Points. See Survey page further on in this document.

Lock to AP MAC: This allows BAD BOY to always maintain connection to a particular Access Point with a specific MAC. This is useful as sometimes there can be a number of identically named SSID's (AP's) with different MAC addresses. With Lock to AP MAC specified the station will lock to the Access Point with that MAC address and not roam between other Access Points with the same ESSID.

Wireless Security

Note: This section is only relevant when connecting to Access Points that require security settings to permit connection. You do not need to enter any security information if the associated Access Point security is 'none'.

This section enables you to set parameters that control how BAD BOY associates to a wireless device and encrypts/decrypts data.

Choose the security method according to the Access Point security policy. BAD BOY should be authorized by Access Point in order to get access to the network and all the user data transferred between BAD BOY and Access Point will be encrypted if wireless security methods are used.

Security: BAD BOY supports WEP, WPA, and WPA2 security options. Select the security mode of your wireless network:

WEP – enable WEP encryption. WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encrypting data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes. WPA™/WPA2™ security methods should be used when possible.

WPA – enable WPA™ security mode. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

WPA™ and *WPA2*™ support the following ciphers for data encryption:

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

CCMP (commonly known as AES) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm.

WPA – enable WPA™ security mode.

WPA-TKIP – enable WPA™ security mode with TKIP support only.

WPA-AES – enable WPA™ security mode with AES support only.

WPA2 – enable WPA2™ security mode.

WPA2-TKIP – enable WPA2™ security mode with TKIP support only.

WPA2-AES – enable WPA2™ security mode with AES support only.

Authentication Type: field relates only to the WEP security option. One of the following authentication modes should be selected if WEP security method is used:

Open Authentication – BAD BOY is authenticated automatically by AP (selected by default).

Shared Authentication – BAD BOY is authenticated after the challenge, generated by AP.

WEP Key Length: 64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The *128-bit* option will provide a bit higher level of wireless security.

Key Type: *HEX* (selected by default) or *ASCII* option specifies the character format for the WEP key if WEP security method is used.

WEP Key: WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used:

For **64-bit** – specify WEP key as 10 HEX (0-9, A-F or a-f) characters (e.g. 00112233AA) or 5 ASCII characters.

For **128-bit** – specify WEP key as 26 HEX (0-9, A-F or a-f) characters (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Key Index: allows specifying the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of 1, 2, 3 or 4.

WPA Authentication: one of the following WPA™ key selection methods should be specified if WPA™ or WPA2™ security method is used:

PSK – WPA™ or WPA2™ with Pre-shared Key method (selected by default).

EAP – WPA™ or WPA2™ with EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in Enterprise networks. Note: BAD BOY Web Management GUI supports only EAP-TTLS authentication method.

WPA Pre-shared Key: the pass phrase for WPA™ or WPA2™ security method should be specified if the *Pre-shared Key* method is selected. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

WPA Identity: identification credential (also known as *identity*) used by the supplicant for EAP authentication.

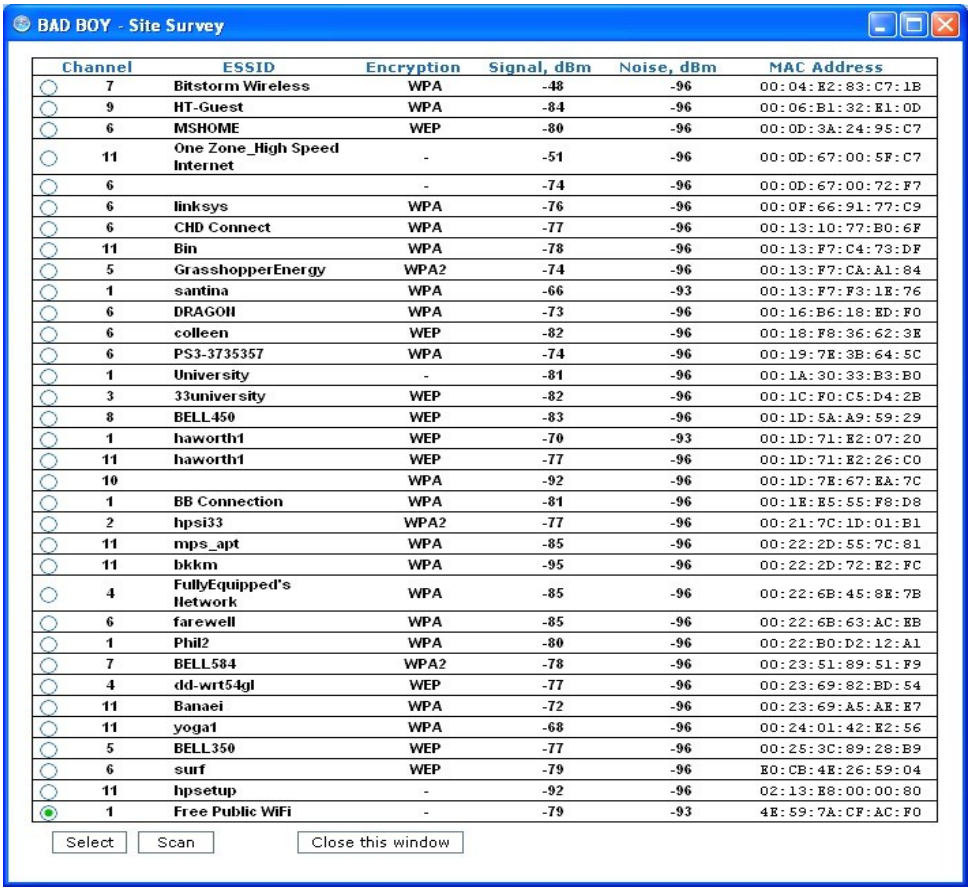
WPA User Name: identification credential (also known as *anonymous identity*) used by the supplicant for EAP tunneled authentication (EAP-TTLS) in unencrypted form.

WPA User Password: password credential used by the supplicant for EAP authentication.

Click Change button to save the changes for this tab and then click Apply to activate them.

Survey page

The Survey page lists all of the detected Access Points available at that location. You can click a column heading to sort the entries in ascending and descending order. To select an Access Point, click the Radio button at the start of the row and then click SELECT button at the bottom. Your selection will be automatically transferred back into the Link Setup tab.



Channel	ESSID	Encryption	Signal, dBm	Noise, dBm	MAC Address
7	Bitstorm Wireless	WPA	-48	-96	00:04:E2:83:C7:1B
9	HT-Guest	WPA	-84	-96	00:06:B1:32:E1:0D
6	MSHOME	WEP	-80	-96	00:0D:3A:24:95:C7
11	One Zone_High Speed Internet	-	-51	-96	00:0D:67:00:5F:C7
6		-	-74	-96	00:0D:67:00:72:F7
6	linksys	WPA	-76	-96	00:0F:66:91:77:C9
6	CHD Connect	WPA	-77	-96	00:13:10:77:B0:6F
11	Bin	WPA	-78	-96	00:13:F7:C4:73:DF
5	GrasshopperEnergy	WPA2	-74	-96	00:13:F7:CA:A1:84
1	santina	WPA	-66	-93	00:13:F7:F3:1E:76
6	DRAGON	WPA	-73	-96	00:16:B6:18:ED:F0
6	colleen	WEP	-82	-96	00:18:F8:36:62:3E
6	PS3-3735357	WPA	-74	-96	00:19:7E:3B:64:5C
1	University	-	-81	-96	00:1A:30:33:B3:B0
3	33university	WEP	-82	-96	00:1C:F0:C5:D4:2B
8	BELL450	WEP	-83	-96	00:1D:5A:A9:59:29
1	haworth1	WEP	-70	-93	00:1D:71:E2:07:20
11	haworth1	WEP	-77	-96	00:1D:71:E2:26:C0
10		WPA	-92	-96	00:1D:7E:67:EA:7C
1	BB Connection	WPA	-81	-96	00:1E:E5:55:F8:D8
2	hpsi33	WPA2	-77	-96	00:21:7C:1D:01:B1
11	mps_apt	WPA	-85	-96	00:22:2D:55:7C:81
11	bkkm	WPA	-95	-96	00:22:2D:72:E2:FC
4	FullyEquipped's Network	WPA	-85	-96	00:22:6B:45:8E:7B
6	farewell	WPA	-85	-96	00:22:6B:63:AC:EB
1	Phil2	WPA	-80	-96	00:22:B0:D2:12:A1
7	BELL584	WPA2	-78	-96	00:23:51:89:51:F9
4	dd-wrt54gl	WEP	-77	-96	00:23:69:82:BD:54
11	Banaei	WPA	-72	-96	00:23:69:A5:AE:E7
11	yoga1	WPA	-68	-96	00:24:01:42:E2:56
5	BELL350	WEP	-77	-96	00:25:3C:89:28:B9
6	surf	WEP	-79	-96	E0:CB:4E:26:59:04
11	hpsetup	-	-92	-96	02:13:E8:00:00:80
1	Free Public WiFi	-	-79	-93	4E:59:7A:CF:AC:F0

Channel: The channel number that the associated Access Point is using.

ESSID: The ESSID (name) of the Access Point. More than one Access Point can be using the same ESSID at the same time.

Encryption: This is the security that has been setup for the associated Access Point.

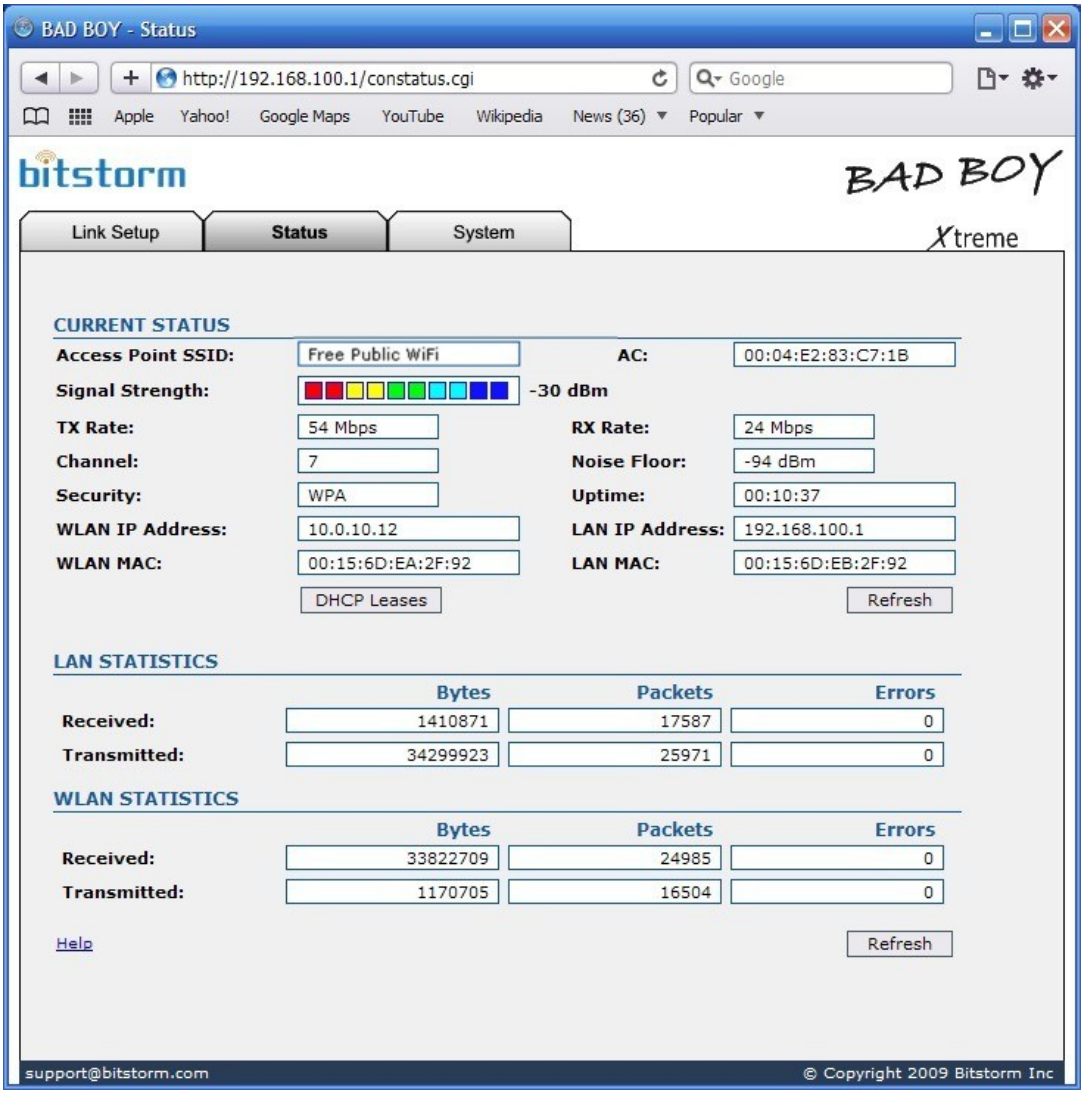
Signal, dBm: Signal strength specified in dBm. The higher the number the better (i.e. -45 is a stronger signal than -78).

Noise, dBm: The level at which the background noise is detected for the associated Access Point. Ideally, this value should be as high as possible for best usage (i.e. -96).

MAC: The MAC address of the Access Point. This value is useful if you wish to LOCK to AP MAC on the Link Setup tab.

Status tab

The Status tab displays a summary of link status information, current values of basic configuration settings, network settings and traffic statistics of all the interfaces. There are no data entry fields on this tab.



Current Status

Access Point SSID: The Name of the 802.11 Service Set (established by the Host Access Point) the device is connected to. Displays the BSSID of the Access Point where the device has associated.

AP MAC: displays the MAC address of the Access Point where the device has associated. MAC (Media Access Control) is a unique HW identifier on each 802.11 radio. It consists of two parts:

An Organizationally Unique Identifier (OUI)

Network Interface Controller (NIC) sequence.

The manufacturer list of a given MAC address is provided here: http://standards.ieee.org/regauth/oui/index.shtml

Signal Strength: displays the received wireless signal level (client-side). The represented value coincides with the graphical bar. Signal Strength is measured in dBm (the Decibels referenced to 1 mw). The conversion is defined as dBm=10log10(P/1mW). So, 0dBm would be 1mW and –72dBm would be .0000006mW. A signal strength of –85dBm or better is recommended for stable links.

TX Rate and RX Rate: displays the current 802.11 data transmission (TX) and data reception (RX) rate. Data rates at 1,2,5.5,11Mbps (802.11b) and 6,9,12,18,24,36,48,54Mbps (802.11g) are possible. Typically, the higher the signal, the higher the data rate and consequently the higher the data throughput. For the max data throughput (54Mbps) a -70dBm or better signal is typically required.

Channel: This is the 802.11 channel number that corresponds to the operating frequency. Device uses the selected channel to transmit and receive data.

Noise Floor: displays the current value of the noise level in dBm. Noise Floor is taken into account while evaluating the signal quality (Signal-to-Noise Ratio).

Security: This is the current security setting. The "none" value is displayed if wireless security is disabled. WEP, WPA or WPA2 values are displayed if that corresponding wireless security method is used. More information is provided in the *Link Setup* section.

Uptime: This is the running total time the device has been operating since last power up (hard-reboot) or software upgrade. The time is expressed in days, hours, minutes and seconds.

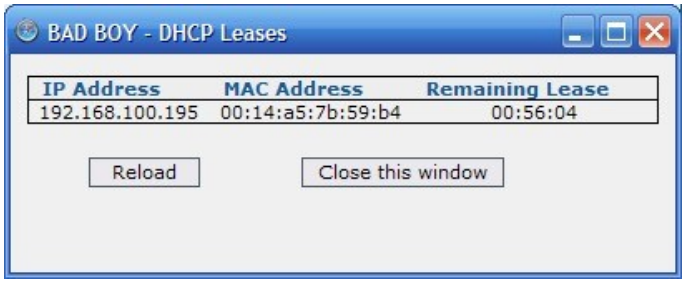
WLAN IP Address: displays the current IP address of the WLAN (Wireless) interface.

LAN IP Address: displays the current IP address of the LAN (Ethernet) interface.

WLAN MAC: displays the MAC address of the WLAN (Wireless) interface.

LAN MAC: displays the MAC address of the LAN (Ethernet) interface.

DHCP Leases: button that will display the IP and MAC address and remaining lease time for all connected users.



Statistics Reporting

LAN Statistics: section displays the detailed receive and transmit statistics (*Bytes*, *Packets*, *Errors*) of the *LAN* (Ethernet) interface. This statistics represents the total amount of data and packets transferred through the Ethernet interface in either direction.

Both unicast IP traffic (conversations between two hosts using HTTP, SMTP, SSH and other protocols) and broadcast traffic (addressing all hosts in a given network range with a single destination IP address) is accumulated.

As long as there is some network traffic being generated or passed through the *LAN* interface, Received and Transmitted *Bytes* and *Packets* count values will continue increasing. *Errors* value represents the total number of transmitted and received packets for which an error occurred in the link layer. High values of Errors may indicate network hardware faults or incorrect configuration.

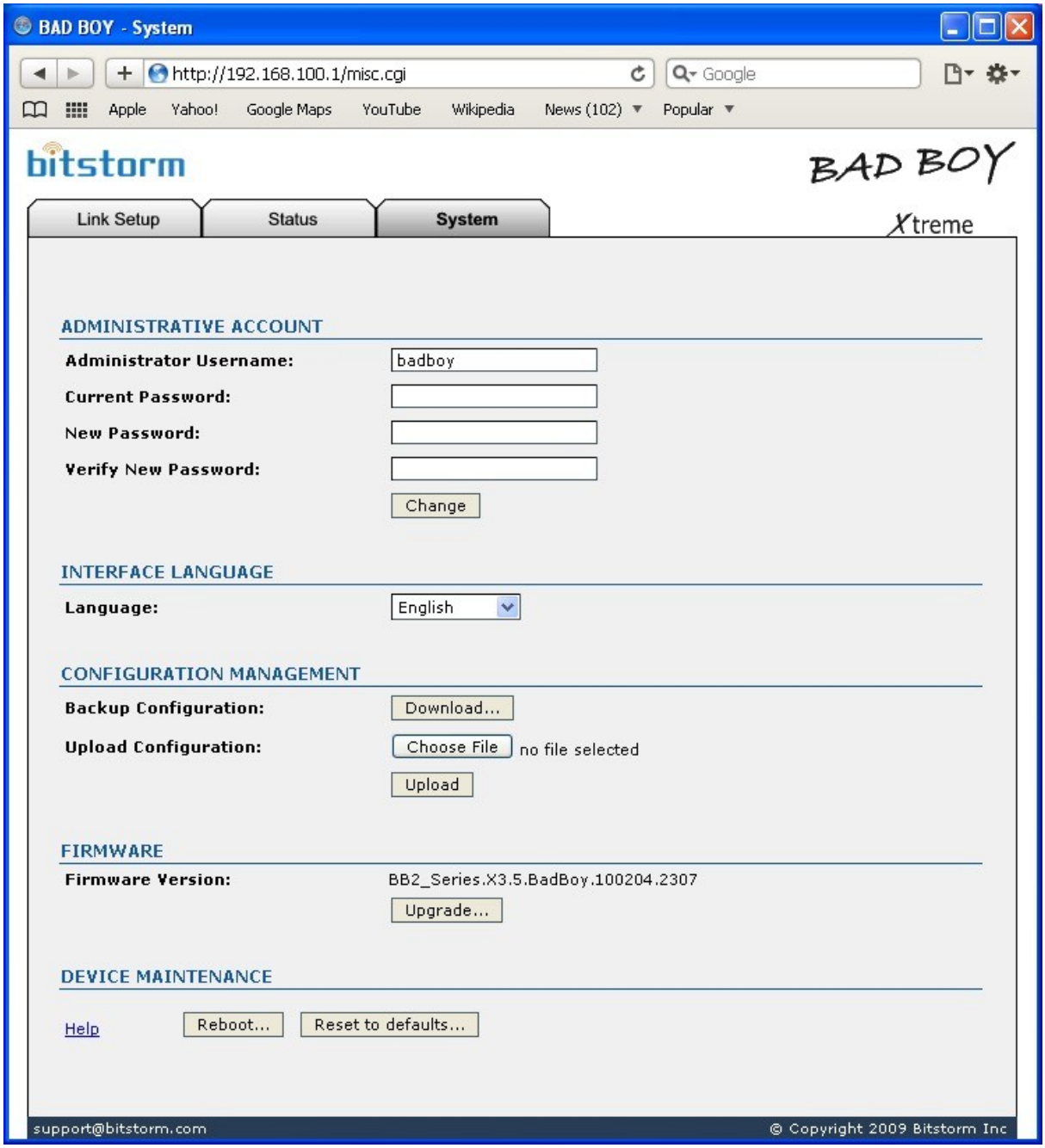
WLAN Statistics: section displays the detailed receive and transmit statistics (*Bytes*, *Packets*, *Errors*) of the *WLAN* wireless interface.

The statistics represents the total amount of unicast and broadcast IP data transferred between devices through the *WLAN* wireless interface in either direction.

As long as there is some network traffic being generated or passed through the *WLAN* wireless interface, Received and Transmitted Bytes, Packets and Error count values will continue increasing.

System tab

The System tab contains administrative options. This tab enables an operator to customize, reboot the device, set it to factory defaults, select the display language, backup or update the configuration and configure administrator's credentials.



Administrative Account

In this section you can modify the administrator password to protect your device from unauthorized reconfiguration. The default administrator's password should be changed on the very first system setup:

Administrator Username: enter a new username.

Current Password: required to authenticate a change to *Password* or *Administrator Username*.

Default administrator login credentials:

Username: **badboy**

Password: **badboy**

New Password: enter a new password to be used for administrator authentication.

Verify Password: re-entered the new password to verify its accuracy.

Click the Change button to save the changes and Apply to activate them.

Interface Language

BAD BOY supports multiple languages in the Web Management Interface GUI.

Language: change the look and feel of the Web Management GUI by renaming the labels of all the configuration settings and controls according to the translation for a particular language. The default language is English. The colours and the layout of all the web elements are not changed.

Configuration Management

Use the *Configuration Management* section controls to backup, restore or update the system configuration file:

Backup Configuration: click the Download button to save the current system configuration to a file.

Upload Configuration: click the Browse button to navigate to and select a previously saved configuration file or specify the full path to the configuration file location.

Activating the Upload button will transfer the new configuration file to the device. The settings of the new configuration will be visible in the *Link Setup* and *System* tabs of the Web Management GUI.

A new configuration will be effective after the *Apply* button is activated and system reboot cycle is completed. Previous system configuration is deleted after the *Apply* button is activated. It is highly recommended to backup the system configuration before uploading a new configuration.

Firmware Version

Use this section to review the current firmware version and update the device with a new version. The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

Firmware version: Displays the version of the current firmware of the BAD BOY system.

Upgrade: Button opens the Firmware Upload window if activated.

Current Firmware: Displays the version of the BAD BOY firmware which is currently operating.

Firmware File: Activate 'Browse' button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after 'Upload' button is activated.

Upload: Button will cause the selected file to be transferred to the device. Once there, it will be checked and any messages will be displayed.

Upgrade: Button should be clicked in order to proceed with firmware upgrade. Please be patient, as the firmware upgrade routine can take 3-7 minutes. BAD BOY Unleashed will be inaccessible until the firmware upgrade routine is completed.

Close this window: Closes the firmware upgrade window if activated. This action only closes the progress display. It will not cancel the firmware upgrade process once started.

CAUTION: Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions can render the device inoperable!

It is highly recommended to backup the system configuration before uploading new firmware.

Notes:

- All current wireless users will be disconnected during the firmware upgrade process. Connection should be restored automatically after completion but users may need to re-establish connection manually.
- During the firmware upgrade process, the LAN LED will blink and the signal strength LEDs will step up and down in sequence until complete.
- The entire process can take several minutes.
- If the update was performed while connected wirelessly, the connection to Unleashed will be lost during the firmware upgrade process. Re-establish connection only after upgrade is complete.

Device Maintenance

The buttons in this section are dedicated for device rebooting and resetting maintenance.

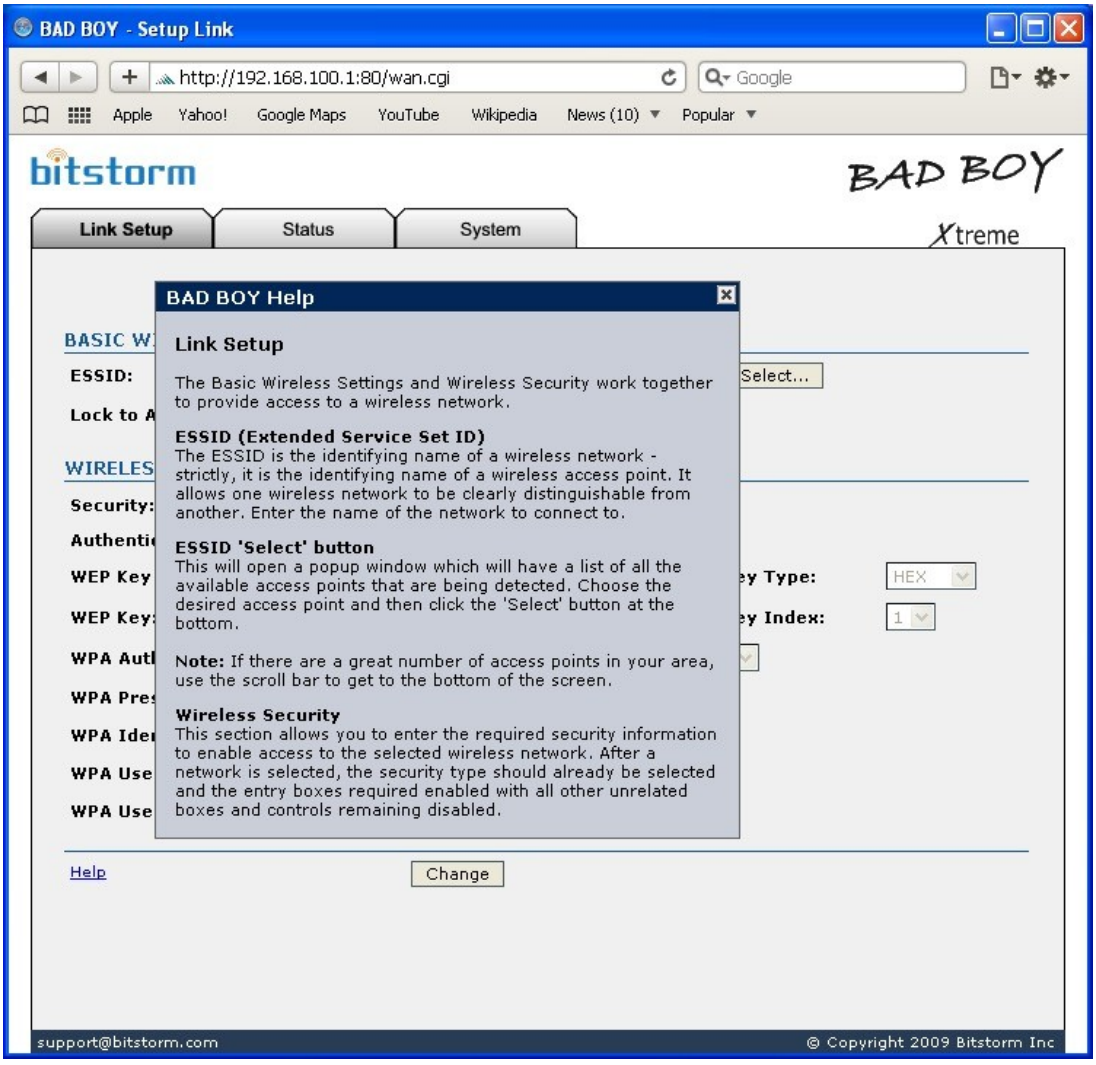
Reboot: activate *Reboot* in order to initiate a full reboot cycle of the device. The effect of Reboot is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: Activate 'Reset to Defaults' in order to initiate a device reset to factory default values. Reset initiates the system *Reboot* process (similar to the power off - power on cycle). The current system configuration will be deleted and the default system configuration (all system settings, no exceptions) will be reset to factory default values.

After the *Reset to Defaults* routine is completed, the BAD BOY Unleashed system will return to the IP configuration (192.168.100.1 / 255.255.255.0). If other settings need to be retained, it is highly recommended to backup the system configuration before the *Reset to Defaults* is initiated.

Help

The Link Setup, Status and System tabs have a Help link located in the lower left of each tab. When clicked, a movable popup window appears that provides information on the various fields and features for the current tab.



Bitstorm contact information is available by clicking on the Bitstorm logo in the upper left.

Contacting us

Address:	Bitstorm Inc. 33 University Ave. Suite 1407 Toronto, Ontario, Canada M5J 2S7
Website:	www.bitstorm.com
Phone:	1-647-724-8328
Skype:	bitstorm.inc
Email:	sales@bitstorm.com support@bitstorm.com