



# User's Guide

**ProSeries**  
**High Power AC1750 Wi-Fi Range Extender / Bridge**  
**REB175P**

**CONTENTS**

<b>INTRODUCTION .....</b>	<b>3</b>	Dashboard: WDS Settings .....	48
<b>GETTING STARTED .....</b>	<b>4</b>	<b>WI-FI SETTINGS.....</b>	<b>49</b>
Package Contents .....	4	2.4GHz Wi-F Settings: Status.....	49
LED Indicators .....	5	2.4GHz Wi-F Settings: Basic Settings.....	50
Side Panel Description .....	6	2.4GHz Wi-F Settings: Security.....	52
<b>MOUNTING INSTRUCTIONS.....</b>	<b>7</b>	2.4GHz Wi-F Settings: Output Power .....	55
<b>OPERATIONAL MODES (BASIC SETUP) .....</b>	<b>8</b>	2.4GHz Wi-F Settings: Site Survey .....	57
NETWORK BRIDGE OVERVIEW .....	9	2.4GHz Wi-F Settings: WDS.....	58
RANGE EXTENDER MODE OVERVIEW .....	17	2.4GHz Wi-F Settings: Access Schedule .....	60
FIREWALL RANGE EXTENDER MODE (WWAN)		2.4GHz Wi-F Settings: Advanced Settings .....	60
OVERVIEW .....	26	5.0GHz Wi-F Settings: Status.....	63
WDS-BRIDGE MODE OVERVIEW .....	35	5.0GHz Wi-F Settings: Basic Settings.....	64
<b>DASHBOARD .....</b>	<b>44</b>	5.0GHz Wi-F Settings: Security.....	66
Dashboard: System Status .....	44	5.0GHz Wi-F Settings: Site Survey .....	70
Dashboard: Operational Modes: .....	45	5.0GHz Wi-F Settings: WDS.....	71
Dashboard: Basic Setup .....	46	5.0GHz Wi-F Settings: Access Schedule .....	73
Dashboard: Connected Devices .....	47	5.0GHz Wi-F Settings: Advanced Settings .....	74

WPS Settings.....	76	IDS (Intrusion Detection System) .....	98
MAC Address Filtering .....	77	<b>ADMINISTRATION .....</b>	<b>99</b>
RADIUS Server .....	79	System Status.....	99
Internal RADIUS Server .....	81	Device Statistics .....	100
RADIUS Accounts .....	83	System Clock .....	102
WMM / QoS.....	84	Advanced Settings.....	103
<b>NETWORK SETTINGS.....</b>	<b>85</b>	System Logs.....	105
Local Network .....	85	Alarm and LED Settings .....	106
VLAN .....	88	Upgrade Firmware .....	107
Domain Redirect .....	89	Save / Reload Settings.....	109
Internet Network (WAN) .....	90	Password Settings .....	111
<b>ADVANCED SETTINGS .....</b>	<b>94</b>	<b>TECHNICAL SPECIFICATIONS .....</b>	<b>112</b>
Port Forwarding.....	94	<b>DEFAULT SETTINGS.....</b>	<b>113</b>
Port Filtering .....	95	<b>TROUBLESHOOTING &amp; SUPPORT INFO .....</b>	<b>114</b>
DMZ (Demilitarized Zone).....	96	<b>WARRANTY &amp; REGULATORY INFORMATION ..</b>	<b>129</b>
Denial of Service .....	97		

## *INTRODUCTION*

Thank you for purchasing this Amped Wireless product. At Amped Wireless we strive to provide you with the highest quality products through innovation and advanced technology. We pride ourselves on delivering products that outperform the competition and go beyond your expectations. If you have any questions please feel free to contact us. We'd love to hear from you and thank you for your support!

Email: [sales@ampedwireless.com](mailto:sales@ampedwireless.com)

Call: 888-573-8830

Web: [www.ampedwireless.com](http://www.ampedwireless.com)

## *GETTING STARTED*

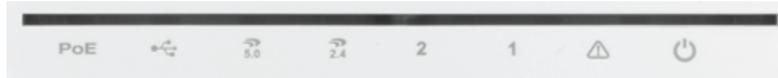
### **Package Contents**

Check to make sure you have all the contents within your package:

- ProSeries High Power AC1750 Wi-Fi Range Extender / Bridge
- 3 x Detachable High Gain 3dBi Antennas
- Magnetic Mounting Kit & Mounting Template
- Setup Guide
- CD: User's Guide
- Ethernet Cable
- Power Adapter

## LED Indicators

*From left to right:*



**PoE:** Indicates when there is an active PoE connection on the LAN1 wired port. LED will remain on.

**USB:** Indicates when there is a USB device is attached to the USB port.

**5.0GHz Wi-Fi:** Blinks rapidly when Wi-Fi data traffic is transmitted or received over the wireless network.

**2.4GHz Wi-Fi:** Blinks rapidly when Wi-Fi data traffic is transmitted or received over the wireless network.

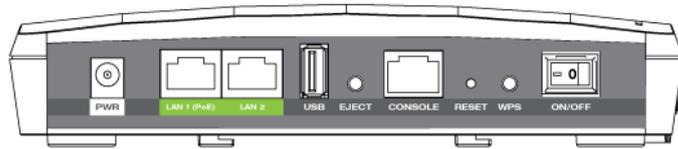
**Wired Port 2:** Indicates when a networking device is connected to wired port (LAN2) on the Range Extender / Bridge. The LED will blink rapidly when wired data traffic is transmitted or received.

**Wired Port 1:** Indicates when a networking device or modem is connected to wired port (LAN1) on the Range Extender / Bridge. The LED will blink rapidly when wired data traffic is transmitted or received.

**Status:** Blinks when the Range Extender / Bridge is booting up or resetting.

**Power (PWR):** Indicates when the Range Extender / Bridge is powered on. The LED will remain on.

## Side Panel Description



**PWR:** Power adapter port. 12V 4A.

**LAN1 (PoE):** Gigabit RJ-45 port with Power over Ethernet input. Connect wired devices or to a PoE switch to use the Range Extender / Bridge without the power adapter.

**LAN2:** Gigabit RJ-45 local network port for expanding your network.

**USB:** Attach USB devices to save or load settings, upgrade firmware, save system logs or load boot files.

**Eject:** To safely eject an attached USB device.

**Console:** Connect to a management console for diagnostics. (i.e. HyperTerminal)

**WPS:** Enables Wi-Fi Protected Setup's push button configuration.

**On/Off:** Device power on/off switch.

## MOUNTING INSTRUCTIONS

### Magnetic Mounting

The mounting kit included with the Range Extender / Bridge provides a convenient method to mount the Range Extender / Bridge on a wall or ceiling. Once you have chosen the location for where you want to install the Range Extender / Bridge, locate the Mounting Template. Use it to mark the screw hole locations onto your wall.

Once the screw holes have been marked, locate the Magnetic Mounting Kit and use the included screws to fasten the two magnetic plates to the wall.

Once the plates are fastened, attach the Range Extender / Bridge to the wall plates and check that the magnets are firmly holding the Range Extender / Bridge to the wall.

### Wall Mounting

In addition to the Magnetic Mounting Kit, the Range Extender / Bridge can also be mounted using the standard wall mounting clips on the bottom of the device.



### *OPERATIONAL MODES (BASIC SETUP)*

The Range Extender / Bridge features four different operational modes that can be configured via the web menu:

- Network Bridge
- Range Extender
- Firewall Range Extender
- WDS-Bridge

## NETWORK BRIDGE OVERVIEW

A Network Bridge creates a connection between two separate networks wirelessly. The Network Bridge connects to a Wi-Fi network (either 2.4 or 5.0GHz network) of the existing network and provides wired connections to expand the network further. All devices connected to the Client Bridge are on the same subnet and local network as the existing network. Note: The Network Bridge does not create another Wi-Fi network to connect to, it only provides wired connections to expand a network.



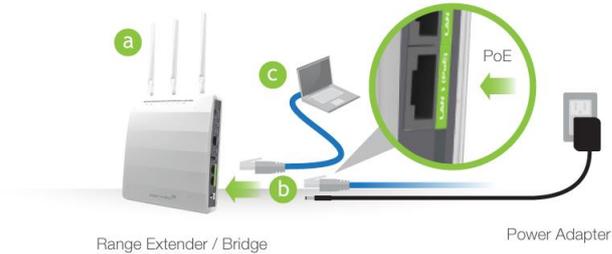
## NETWORK BRIDGE MODE BASIC SETUP

### Find an optimal setup location for your Network Bridge

Place the Network Bridge in a location where it can receive a strong signal from the Source Network. The better the connection the faster the bridged network speeds will be.



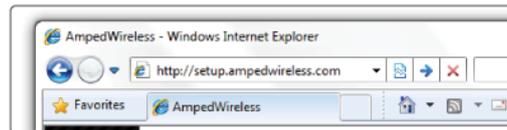
## Attach Antennas, Power On & Connect to your Computer



- a) Attach the included antennas to the antenna ports on the Network Bridge.
- b) Power on the Network Bridge by attaching either the power adapter to the Bridge and plugging in the other end into a power outlet **or** attaching a PoE Ethernet cable to the LAN1 port on the side panel and the other end to an active PoE switch.
- c) Connect to the Network Bridge with your computer by attaching an Ethernet cable to the LAN2 port on the side panel.

Open your Web Browser

- a) Open your web browser.
- b) Type <http://setup.ampedwireless.com> into the web address bar.



<http://setup.ampedwireless.com>

If the web menu fails to open, type in the following IP address into your web address bar:

<http://192.168.80.240>

**Note:** If you have problems accessing the Web Menu... Disable third-party firewalls such as Norton, Zone Alarm or Windows Defender. Check to see that your computer is not connected to other wireless networks.

- c) When prompted, enter the login and password:

LOGIN:	admin
PASSWORD:	admin



## Select the Operational Mode

- a) After the web menu appears, select **Dashboard** from the navigation menu on the top of the page.
- b) Select **Operational Mode** from the left hand navigation.
- c) Using the dropdown menu, select **Network Bridge Mode** for the Operational Mode and click **Apply**.
- d) When the web menu has reloaded, select **Basic Setup**.



## Basic Setup Wizard

Confirm that Bridge Mode is the mode that you wish to configure and Click **Next** to begin.

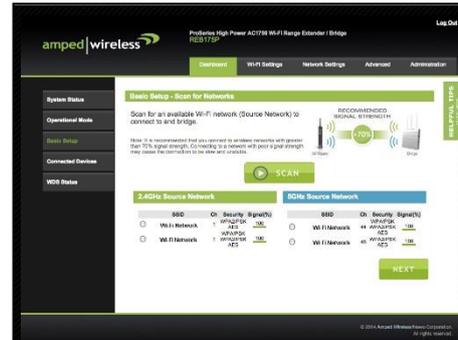
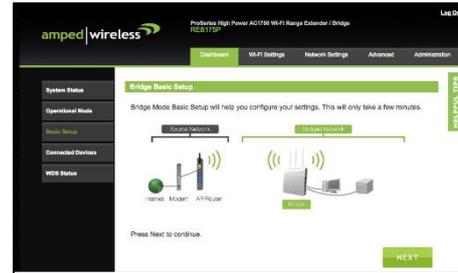
### Scan for a Source Network to Connect to and Bridge

Click **Scan** to find available networks. Select the Source Network that you wish to connect to and bridge.

**Note:** It is recommended that you select a Source Network with a signal strength greater than 70% for the most reliable connection. Poor signal connections may cause slow speeds or dropped connections.

Click **Next** to continue.

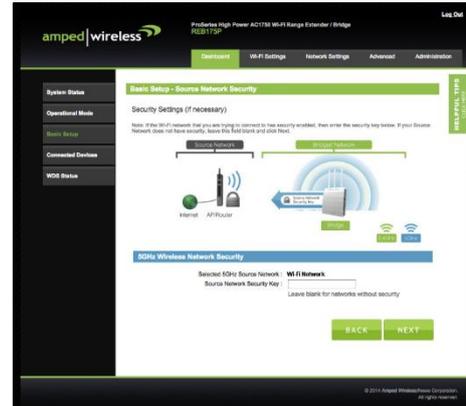
**Note:** If you do not see your desired Source Network, click Scan again, or move the Network Bridge to another location and Scan again as the Bridge may be out of range.



**Source Network Security Settings (if necessary)**

If the Source Network chosen has security enabled, you will need to enter the security key here. If the Source Network does not have security enabled, leave the security field blank.

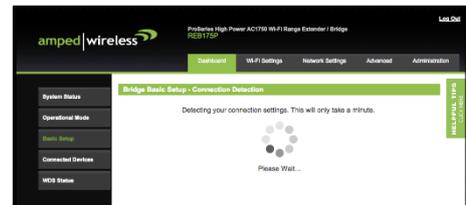
Click **Next** to apply the settings.



DO NOT LEAVE OR REFRESH THIS PAGE

Allow the configuration to complete and the Basic Setup Wizard will automatically redirect you to the next step

If there are problems with your configuration, the Basic Setup Wizard will inform you of the issues with your configuration. If there are no problems, you will see the Setup Summary page.

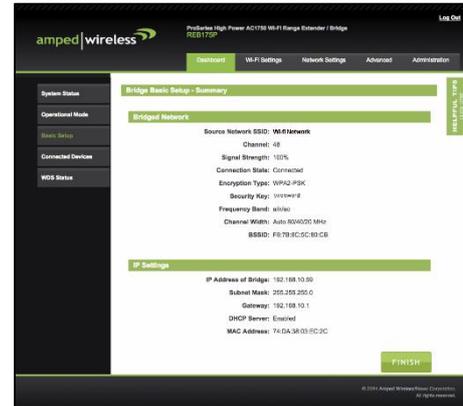


## Setup Summary

Once the Network Bridge has rebooted, it will load the Setup Summary page and provide you with the details of your setup. It is recommended that you print this page for your records.

Open a new web browser window and check that you have access to the Internet.

Additional settings can be configured using the navigation menu on the top of the Web Menu.



## RANGE EXTENDER MODE OVERVIEW

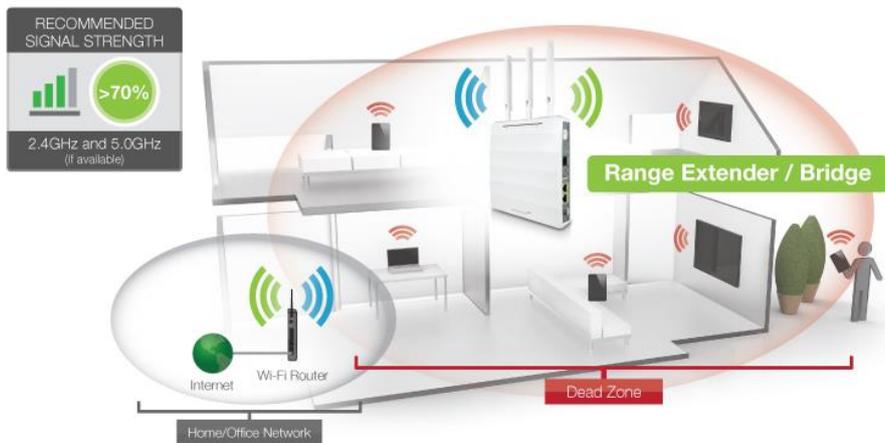
Range Extender mode expands the range of any standard Wi-Fi router by repeating the signal (2.4GHz and 5.0GHz) and redistributing it in a new, extended location. In addition, to creating a new extended Wi-Fi network for devices to connect to, the Range Extender also provides additional wired connections for bridging additional network devices to the existing network. All devices connected to the Range Extender are on the same subnet and local network as the existing network.



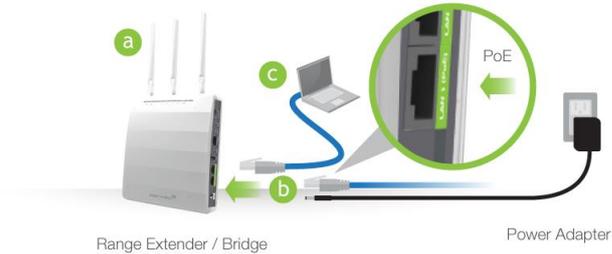
## RANGE EXTENDER MODE BASIC SETUP

### Find an optimal setup location for your Range Extender

Place the Range Extender in a location between your Source Network's wireless access point/router and your wireless dead zone. It's recommended that you place the Range Extender in a location where it can receive a strong signal from the Source Network's wireless access point/router.



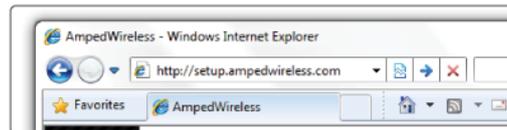
## Attach Antennas, Power On & Connect to your Computer



- a) Attach the included antennas to the antenna ports on the Range Extender.
- b) Power on the Range Extender by attaching either the power adapter to the Range Extender and plugging in the other end into a power outlet **or** attaching a PoE Ethernet cable to the LAN1 port on the side panel and the other end to an active PoE switch.
- c) Connect to the Range Extender with your computer by attaching an Ethernet cable to the LAN2 port on the side panel.

Open your Web Browser

- a) Open your web browser.
- b) Type <http://setup.ampedwireless.com> into the web address bar.



<http://setup.ampedwireless.com>

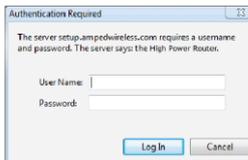
If the web menu fails to open, type in the following IP address into your web address bar:

<http://192.168.80.240>

**Note:** If you have problems accessing the Web Menu... Disable third-party firewalls such as Norton, Zone Alarm or Windows Defender. Check to see that your computer is not connected to other wireless networks.

- c) When prompted, enter the login and password:

LOGIN:	admin
PASSWORD:	admin



## Select the Operational Mode

- a) After the web menu appears, select **Dashboard** from the navigation menu on the top of the page.
- b) Select **Operational Mode** from the left hand navigation.
- c) Using the dropdown menu, select **Range Extender Mode** for the Operational Mode and click **Apply**.
- d) When the web menu has reloaded, select **Basic Setup**.



## Basic Setup Wizard

Confirm that Range Extender Mode is the mode that you wish to configure and Click **Next** to begin.

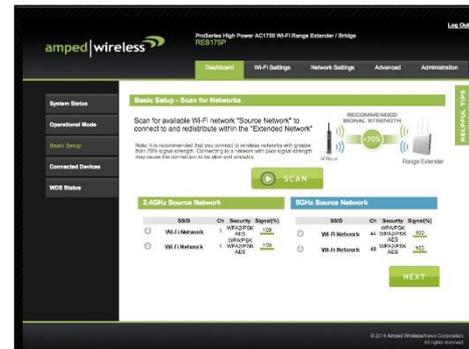
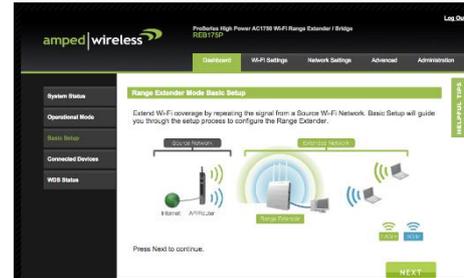
### Scan for a Source Network to Connect to Extend

Click **Scan** to find available networks. Select the Source Network(s) that you wish to repeat. If you have a dual band router/access point, select BOTH the 2.4GHz and 5.0GHz network names.

**Note:** It is recommended that you select a Source Network with a signal strength greater than 70% for the most reliable connection. Poor signal connections may cause slow speeds or dropped connections.

Click **Next** to continue.

**Note:** If you do not see your desired Source Network, move the Range Extender closer to the router and scan again as it may be out of range.



### Source Network Security Settings (if necessary)

If the Source Network chosen has security enabled, you will need to enter the security key here. If you selected a dual band network to repeat, you will need to enter both security keys here.

If the Source Network does not have security enabled, leave the security field blank.

Click **Next** to continue.



## Configure Settings for your Extended Network

The default Wi-Fi network ID of your Extended Networks are:  
[Amped\\_REB\\_5.0](#) and [Amped\\_REB\\_2.4](#)

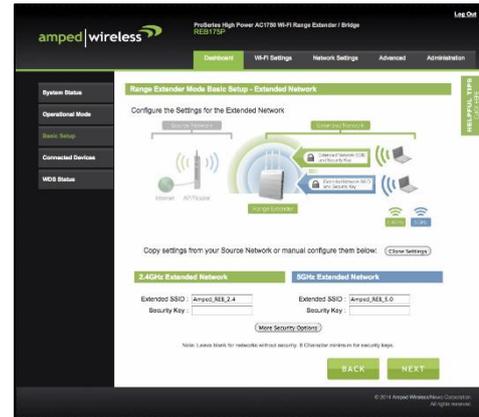
If you choose to “Clone” the settings from your Source Network, the wizard will copy the SSID and security key of your Source Network.

You can also manually enter a new network ID and security key. The new security keys must be 8-characters minimum.

Click [Next](#) to apply your settings.

DO NOT LEAVE OR REFRESH THIS PAGE  
 Allow the configuration to complete and the Basic Setup Wizard will automatically redirect you to the next step.

If there are problems with your configuration, the Basic Setup Wizard will inform you of the issues with your configuration. If there are no problems, you will see the Setup Summary page.



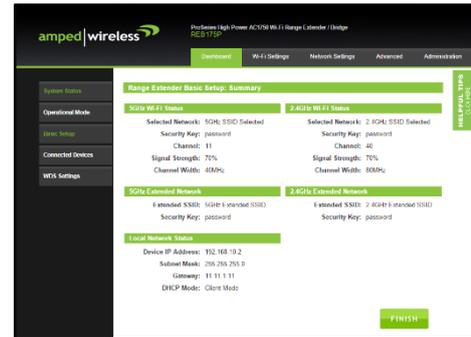
## Setup Summary

Once the Range Extender has rebooted, it will load the Setup Summary page and provide you with the details of your setup. It is recommended that you print this page for your records.

If you haven't already positioned your Range Extender in an optimal location, you may do so now. All Range Extender settings are saved and can be safely powered off for relocation.

You may also attach any wired network devices to the wired port on the side of the Range Extender.

Additional settings can be configured using the navigation menu on the top of the Web Menu.



### ***FIREWALL RANGE EXTENDER MODE (WWAN) OVERVIEW***

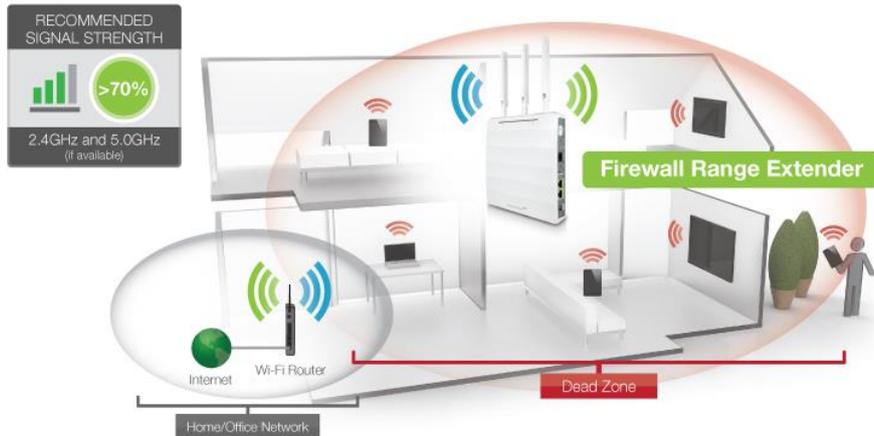
Firewall Range Extender mode functions similarly to a router that connects to a Wi-Fi network instead of wired to a modem. It is a Range Extender that creates a secure firewall between the Source Network and the Extended Network. In addition to a firewall, the Firewall Range Extender also features its own DHCP server for assigning IP addresses to connecting users. All devices connected to the Extended Network (wired and wireless) are protected from the Source Network and the Internet. The Extended Network and Source Network are two completely separate networks.

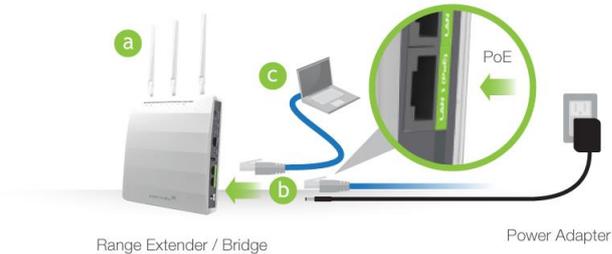


## FIREWALL RANGE EXTENDER MODE BASIC SETUP

### Find an optimal setup location for your Range Extender

Place the Firewall Range Extender in a location between your Source Network's wireless access point/router and your wireless dead zone. It's recommended that you place the Firewall Range Extender in a location where it can receive a strong signal from the Source Network's wireless access point/router.

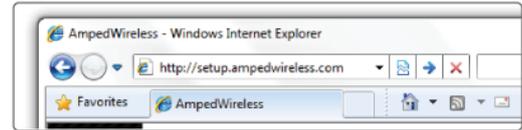


**Attach Antennas, Power On & Connect to your Computer**

- d) Attach the included antennas to the antenna ports on the Firewall Range Extender.
- e) Power on the Firewall Range Extender by attaching either the power adapter to the Firewall Range Extender and plugging in the other end into a power outlet **or** attaching a PoE Ethernet cable to the LAN1 port on the side panel and the other end to an active PoE switch.
- f) Connect to the Firewall Range Extender with your computer by attaching an Ethernet cable to the LAN2 port on the side panel.

Open your Web Browser

- a) Open your web browser.
- b) Type <http://setup.ampedwireless.com> into the web address bar.



If the web menu fails to open, type in the following IP address into your web address bar:

<http://192.168.80.240>



**Note:** If you have problems accessing the Web Menu... Disable third-party firewalls such as Norton, Zone Alarm or Windows Defender. Check to see that your computer is not connected to other wireless networks.

- c) When prompted, enter the login and password:

LOGIN: admin  
PASSWORD: admin



## Select the Operational Mode

- a) After the web menu appears, select **Dashboard** from the navigation menu on the top of the page.
- b) Select **Operational Mode** from the left hand navigation.
- c) Using the dropdown menu, select **Firewall Range Extender Mode** for the Operational Mode and click **Apply**.
- d) When the web menu has reloaded, select **Basic Setup**.



## Basic Setup Wizard

Confirm that Firewall Range Extender Mode is the mode that you wish to configure and Click **Next** to begin.

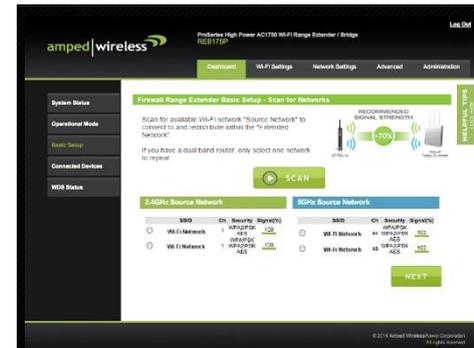
### Scan for a Source Network to Connect to Extend

Click **Scan** to find available networks. Select the Source Network that you wish to repeat.

**Note:** It is recommended that you select a Source Network with a signal strength greater than 70% for the most reliable connection. Poor signal connections may cause slow speeds or dropped connections.

Click **Next** to continue.

**Note:** If you do not see your desired Source Network, move the Firewall Range Extender closer to the router and scan again as it may be out of range.



**Source Network Security Settings (if necessary)**

If the Source Network chosen has security enabled, you will need to enter the security key here. If you selected a dual band network to repeat, you will need to enter both security keys here.

If the Source Network does not have security enabled, leave the security field blank.

Click **Next** to continue.



## Configure Settings for your Extended Network

The default Wi-Fi network ID of your Extended Networks are:

[Amped\\_REB\\_5.0](#) and [Amped\\_REB\\_2.4](#)

If you choose to “Clone” the settings from your Source Network, the wizard will copy the SSID and security key of your Source Network.

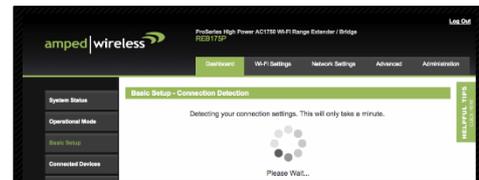
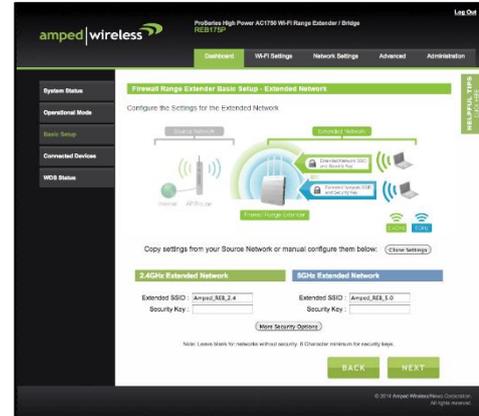
You can also manually enter a new network ID and security key. The new security keys must be 8-characters minimum.

Click **Next** to apply your settings.

**DO NOT LEAVE OR REFRESH THIS PAGE**

Allow the configuration to complete and the Basic Setup Wizard will automatically redirect you to the next step

If there are problems with your configuration, the Basic Setup Wizard will inform you of the issues with your configuration. If there are no problems, you will see the Setup Summary page.



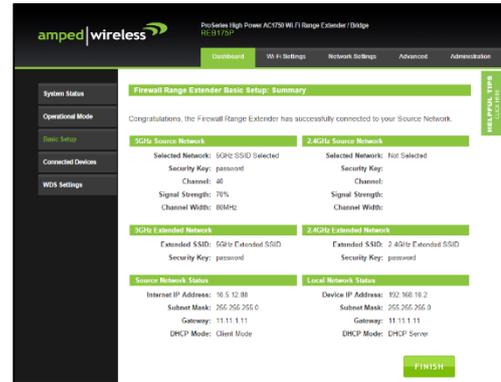
## Setup Summary

Once the Firewall Range Extender has rebooted, it will load the Setup Summary page and provide you with the details of your setup. It is recommended that you print this page for your records.

If you haven't already positioned your Firewall Range Extender in an optimal location, you may do so now. All settings are saved and can be safely powered off for relocation.

You may also attach any wired network devices to the wired port on the side of the Range Extender

Additional settings can be configured using the navigation menu on the top of the Web Menu.



### WDS-BRIDGE MODE OVERVIEW

WDS (Wireless Distribution System) Bridge mode enables the wireless interconnection of Access Points using WDS mode, and Network Bridges using WDS mode. A WDS-Bridge connects wirelessly to a WDS-Access Point and expands the existing network by creating additional wired ports to expand the network with by adding network switches, computers or servers and more. Devices connected to the WDS-Bridge are on the same local network as those connected to the Source network.

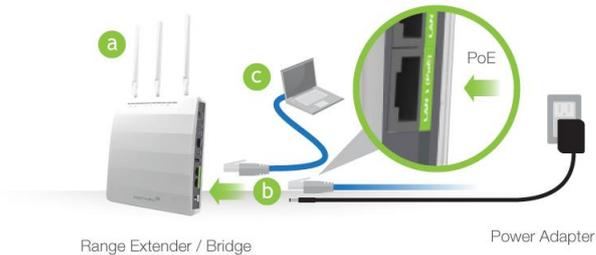


## WDS-BRIDGE MODE BASIC SETUP

### Find an optimal setup location for your WDS-Bridge

Place the WDS-Bridge in a location where it can receive a strong signal from the Source Network. The better the connection the faster the bridged network speeds will be.

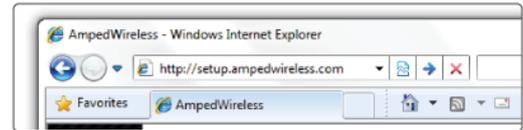


**Attach Antennas, Power On & Connect to your Computer**

- a) Attach the included antennas to the antenna ports on the WDS-Bridge.
- b) Power on the WDS-Bridge by attaching either the power adapter to the Bridge and plugging in the other end into a power outlet or attaching a PoE Ethernet cable to the LAN1 port on the side panel and the other end to an active PoE switch.
- c) Connect to the WDS-Bridge with your computer by attaching an Ethernet cable to the LAN2 port on the side panel.

### Open your Web Browser

- a) Open your web browser.
- b) Type <http://setup.ampedwireless.com> into the web address bar.



<http://setup.ampedwireless.com>

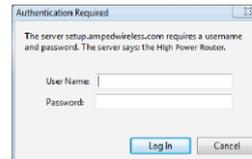
If the web menu fails to open, type in the following IP address into your web address bar:

<http://192.168.80.240>

**Note:** If you have problems accessing the Web Menu... Disable third-party firewalls such as Norton, Zone Alarm or Windows Defender. Check to see that your computer is not connected to other wireless networks.

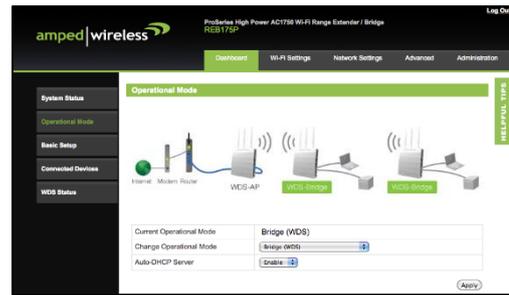
- c) When prompted, enter the login and password:

LOGIN:	admin
PASSWORD:	admin



### Select the Operational Mode

- a) After the web menu appears, select **Dashboard** from the navigation menu on the top of the page.
- b) Select **Operational Mode** from the left hand navigation.
- c) Using the dropdown menu, select **WDS-Bridge Mode** for the Operational Mode and click **Apply**.
- d) When the web menu has reloaded, select **Basic Setup**.



## Basic Setup Wizard

Using the dropdown menu select which Wi-Fi frequency you wish to configure for WDS - AP mode:

- 2.4GHz Only
- 5GHz Only
- Both 2.4GHz and 5GHz

After you have made your selection, click **Next** to begin.

For the purpose of this User's Guide, we will provide instructions and screenshots for a dual band configuration (both 2.4GHz and 5GHz).



## WDS Settings

WDS - Bridge mode requires additional Access Points also functioning in WDS - AP mode. A WDS enabled Bridge connects to another WDS-Access Point via MAC addresses. Enter the MAC addresses of the Access Points with WDS enabled into the corresponding fields that you wish to connect to.

For WDS connections to work properly, the MAC address associations must also be configured on each individual WDS enabled Access Point or Bridge, not just the one you are currently configuring. For example, if you are connecting three WDS APs or Bridges, AP/Bridge 1 must have AP/Bridge 2 and AP/Bridge 3's MAC address configured, while AP/Bridge 2 has AP/Bridge 1's and AP/Bridge 3's MAC, and AP/Bridge 3 has AP/Bridge 1's and AP/Bridge 2's MAC configured.

Encryption can be used to secure your WDS connections. If you choose to use encryption (recommended), it is important that you set the same security key setting on all connected WDS enabled Access Points. Click **Next** to continue.

The screenshot shows the configuration page for a Z4300 MAC address (11:22:33:44:55:66) in Bridge mode. The page is titled "WDS - Bridge Mode Basic Setup - Z4300 Configuration". It includes a navigation menu on the left with options like System Status, Operational Mode, Basic Setup, Connected Devices, and WDS Settings. The main content area contains the following fields:

- This device's Z4300 MAC Address: 11:22:33:44:55:66
- WDS Connection 1: MAC Address: [input field]
- WDS Connection 2: MAC Address: [input field]
- WDS Connection 3: MAC Address: [input field]
- WDS Connection 4: MAC Address: [input field]
- Select the encryption type: Encryption Type: AES (dropdown menu)
- Security Key: [input field]

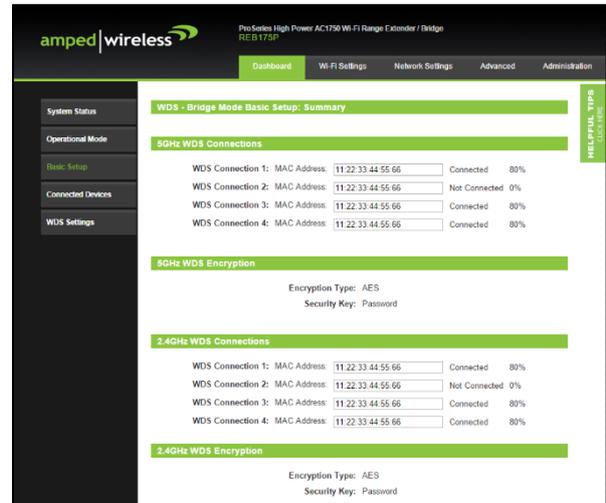
Below this section, there is a similar configuration area for a 5200 MAC address (11:22:33:44:55:66) with four WDS connection fields and encryption options. At the bottom right, there are "BACK" and "NEXT" buttons.

## Setup Summary

Once the WDS-Bridge has rebooted, it will load the Setup Summary page and provide you with the details of your setup. It is recommended that you print this page for your records.

The Summary will display the status of each WDS connection and the signal strength of each connection. Connections with lower signal strength connections may perform slower. It is recommended to have a signal of at least 70% for the best performance.

Additional settings can be configured using the navigation menu on the top of the Web Menu.



## MORE SETTINGS

The Range Extender / Bridge has many additional features and settings that can be configured via the Web Menu. To access these settings start with the navigation menu located on the top of the Web Menu. Once the desired menu is selected, additional navigational options will appear on the left hand side. Select the sub menus from here to access the specific settings for each option.

**Helpful Tips:** Each page will have a link to access tips and general information regarding the features for the current page. The information will be very useful in configuring the Range Extender / Bridge and will serve as a User's Guide for the current page. To access it, click the **Helpful Tips** link at the top right corner of each page.



**Note:** Not all settings and features are available for all operational modes. As you change from one operational mode to another some features and settings will be greyed out and cannot be accessed as they do not apply to the selected operational mode. For example, Firewall Range Extender mode has firewall settings that are not available in any other mode. When using any other mode, those settings will not be configurable.

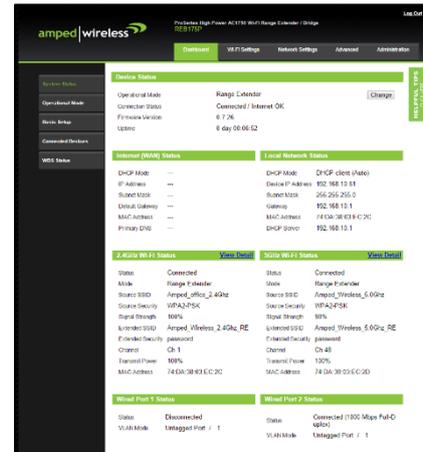
DASHBOARD

Dashboard: System Status

The Dashboard System Status will provide you with the current status of the Range Extender / Bridge. It provides you with glance at general setup information such as the current operational mode, firmware version and uptime of the Range Extender / Bridge. From here you can quickly change the operational mode by clicking the “Change” button to the right of the operational mode.

In addition to the operational mode, the System Status also provides you with information regarding your Source Network, Extended Networks, if available for your operational mode, as well as the details for your network IP settings.

At the bottom of the page you will find details about the Wired Port settings.



## Dashboard: Operational Mode

The Operational Mode page lets you change the operating mode of the Range Extender / Bridge. As described earlier, the Range Extender / Bridge features four different modes:

- Network Bridge
- Range Extender
- Firewall Range Extender
- WDS-Bridge



From this page you can view your current operational mode or change the operational mode to any of the modes above. For descriptions on the features of each mode please see the operational mode overviews described in the Operational Modes (Basic Setup) section of this User's Guide. Selecting an operational mode from the dropdown menu will also provide you with a diagram and overview of the operational mode selected. Once you have chosen a mode, click Apply to apply the changes.

The Auto-DHCP Server feature automatically manages the IP addresses within your network. When connected to a network that has a DHCP server enabled, the Range Extender/Bridge will automatically obtain an IP from the network's DHCP server and disable the DHCP server on the Range Extender / Bridge to avoid any IP assignment conflicts. For users that are not familiar with how this works, it is recommended to leave Auto-DHCP server enabled on this page.

## Dashboard: Basic Setup

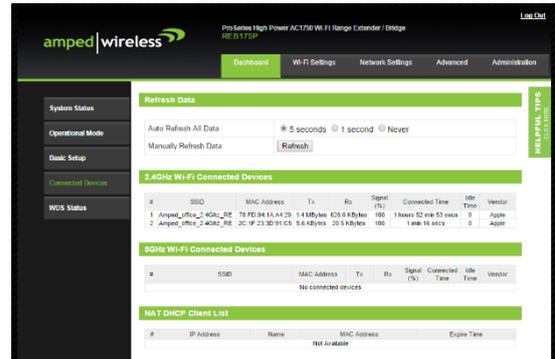
The Basic Setup page will provide you with a simple, step by step, wizard for configuring basic settings of the current operational mode. As you change from one operational mode to another, the Basic Setup menu will also change to cater to the settings for the selected operational mode. For more details regarding Basic Setup, please view the Operational Mode (Basic Setup) section of this User's Guide.



**Dashboard: Connected Devices**

View the details of certain devices connected to the Range Extender / Bridge. Since this menu may constantly change as devices connect and disconnect from the network, a page refresh option is available to automatically update the data at set intervals.

Connected devices are separated by those connected to the 2.4GHz Wi-Fi networks or 5.0GHz Wi-Fi networks. If the current operational mode is Firewall Range Extender mode, this page will also show those devices that are connected to the Firewall Range Extender and have been provided an IP address assignment from the DHCP server of the Firewall Range Extender.



## Dashboard: WDS Settings

If the Range Extender / Bridge has been set to WDS-Bridge operational mode, the WDS settings page will give you a glance at the status of current WDS connections. The page provides you with information for each frequency: 2.4GHz and 5.0GHz depending on your WDS configurations. Each section will display information for each WDS connection such as their connection state and signal strength in addition to identifying each connection by its MAC address. If encryption is used for the connections, that is displayed as well.

There are also shortcuts to access the configuration menu your WDS settings in case you wish to make changes.

The screenshot shows the 'WDS Settings' page in the amped wireless dashboard. The page is titled 'ProSeries High Power AC1750 Wi-Fi Range Extender / Bridge' and 'REB175P'. The navigation menu includes 'Dashboard', 'Wi-Fi Settings', 'Network Settings', 'Advanced', and 'Administration'. The left sidebar has options for 'System Status', 'Operational Mode', 'Basic Setup', 'Connected Devices', and 'WDS Settings'. The main content area is divided into sections for 2.4GHz and 5GHz WDS settings.

**2.4GHz WDS Status**

WDS Mode	Disabled
Device MAC Address	74 DA 38 03 EC 2C

**2.4GHz WDS Connections**

MAC Address	Status	Signal
WDS Connection 1	None	Not Connected 0%
WDS Connection 2	None	Not Connected 0%
WDS Connection 3	None	Not Connected 0%
WDS Connection 4	None	Not Connected 0%

**2.4GHz WDS Encryption**

Encryption Type	None
-----------------	------

**5GHz WDS Status**

WDS Mode	Disabled
Device MAC Address	74 DA 38 03 EC 2D

**5GHz WDS Connections**

MAC Address	Status	Signal
WDS Connection 1	None	Not Connected 0%
WDS Connection 2	None	Not Connected 0%
WDS Connection 3	None	Not Connected 0%
WDS Connection 4	None	Not Connected 0%

**5GHz WDS Encryption**

Encryption Type	None
-----------------	------

WI-FI SETTINGS

2.4GHz Wi-F Settings: Status

The 2.4GHz Wi-Fi Status page provides you with a glance at basic information for your 2.4GHz Wi-Fi settings such as the Status, mode, security type, SSID among other details.



## 2.4GHz Wi-F Settings: Basic Settings

The Basic Settings page allows you to adjust settings for your 2.4GHz Wi-Fi networks.

**Enable Wi-Fi Radio:** Disabling will turn off all 2.4GHz Wi-Fi activity. Users will no longer be able to connect wirelessly to your 2.4GHz network.

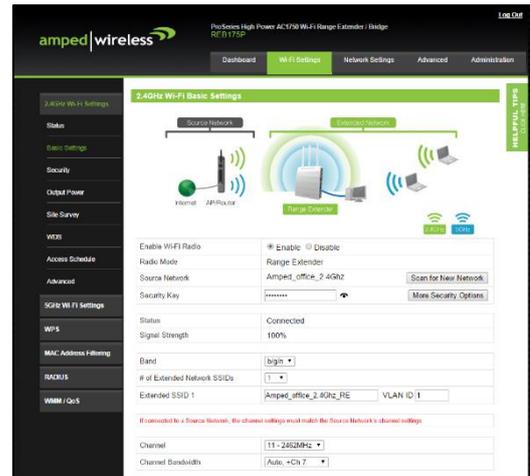
**Radio Mode:** The operational mode of the 2.4GHz radio.

**Source Network:** The SSID of the Source Network that the Range Extender / Bridge is extending or bridging.

**Scan for a New Network:** To change the Source Network and scan for a new one click this button.

**Status:** The current status of the Range Extender / Bridge and the Source Network.

**Signal Strength:** The signal strength quality between the Range Extender / Bridge and the Source Network. It is recommended that the signal strength is greater than 70% for optimal performance.



**Band:** Select the compatible Wi-Fi standard and speed for your wireless network. This is typically the same band as what the Source Network is operating on to ensure optimal performance.

**# of Extended Network SSIDs:** Select the number of different Extended Network SSIDs you wish to have on the 2.4GHz frequency. Each SSID will represent a network that Wi-Fi devices can see and connect to. The Range Extender allows up to 15 SSIDs per frequency. Each SSID can have a different name, VLAN assignment and security key. Additional SSIDs is sometimes referred to as Guest Networks. (VLAN available in Firewall Range Extender mode only)

**VLAN ID:** Available in Firewall Range Extender mode only. The VLAN ID is a feature that allows you to virtually map connected devices and secure access for each Extended Network SSID created. Devices that are connected to an SSID with a specific VLAN (Virtual Local Area Network) ID cannot access or see devices connected to SSIDs with a different VLAN ID. For example, if SSID 1 is assigned to VLAN 1 and SSID 2 is assigned to VLAN 2, then devices connected to SSID 1 will not be able to see or access devices or files on SSID 2 (VLAN 2). VLAN IDs can range between 1 and 4094.

**Channel:** Select the channel number of the 2.4GHz radio. When connected to a Source Network the channel number of the Range Extender / Bridge **MUST** match that of the Source Network for normal operation.

**Channel Bandwidth:** Select the channel width for the 2.4GHz radio. It is recommended to match the channel bandwidth of the Source Network for optimal operation.

## 2.4GHz Wi-F Settings: Security

The Extended Network Security page allows you to change the type of wireless security settings for your 2.4GHz Extended Wi-Fi networks.

These settings apply to Range Extender or Firewall Range Extender operational modes. If you are in Bridge Mode or WDS-Bridge mode these options will not be available as there are no Extended Networks in Bridge modes.

**Extended Network SSID Selection:** Using the drop down menu, you can select which Extended Network you wish to configure and may adjust the security settings below.

**Broadcast SSID:** Selecting Disable Broadcast SSID will hide the visibility of the selected Extended Network SSID. Users must manually enter the SSID to connect.

The screenshot displays the '2.4GHz Extended Network Wi-Fi Security Settings' page in the amped wireless web interface. The page title is 'PreSeries High Power AC1750 Wi-Fi Range Extender / Bridge'. The navigation menu includes 'Dashboard', 'Wi-Fi Settings', 'Network Settings', 'Advanced', and 'Administration'. The left sidebar shows a tree view with '2.4GHz Wi-Fi Settings' selected, containing sub-items: Status, Basic Settings, 2.4GHz, Output Power, Site Survey, WDS, Access Router, Advanced, 2.4GHz Wi-Fi Settings, WPS, MAC Address Filter, DNS, and WMM / QoS. The main content area is titled '2.4GHz Extended Network Wi-Fi Security Settings' and includes a sub-header '2.4GHz Extended Network Wi-Fi Security Settings' and a note: 'Select the specific Extended Network SSID from the dropdown menu below to configure the Security parameters for that network.' The settings are as follows:

Extended Network SSID	Ampeo_wifi_2_40w_RE
Broadcast SSID	Enable
Internet Access Only (Different Subnet)	Disable
Wireless Client Isolation	None
Load Balancing (Connected Device Limit)	50 / 100
Authentication Type	WPA/PSK
WPA Type	WPA2 Only
Encryption Type	AES
Key Renewal Interval	66 minutes(s)
Pre-shared Key Type	Password
Pre-shared Key	password
Additional Authentication	No Additional Authentication

Below the security settings is the '2.4GHz Wireless Advanced Settings' section:

Smart Handover	Enable
Smart Handover	Disable
RSSI Threshold	-88 dB
Bandwidth Restrictions	Disable
Bandwidth Restrictions	0 Mbps

**Internet Access Only:** Choose whether you wish to block Internet access for those devices connecting to the selected Extended Network SSID.

**Wireless Client Isolation:** Enabling this feature provides an extra layer of security by preventing devices connected to the selected Extended Network SSID to communicate with one another. This feature is useful in corporate environments or public hotspots.

**Load Balancing:** Limit the number of devices that can connect to the selected Extended Network SSID. This can assist in managing the bandwidth used by each Extended Network SSID. The maximum number of devices for each SSID is 50 devices.

**Smart Handover:** When multiple Range Extenders (REB175P) or Access Points (APR175P) are installed in an environment where devices roam over a larger area, Smart Handover allows the Range Extender to disconnect a connected device once the signal is crosses a defined RSSI decibel (signal receiving sensitivity) threshold to allow it to easily connect to the neighboring Range Extender. Note, some older Wi-Fi devices may not be compatible with the Smart Handover feature.

**Bandwidth Restriction:** When enabled, Bandwidth Restriction limits the amount of bandwidth provided to all devices connecting to the Extended Network SSID.

#### Authentication Method:

**None:** Authentication is disabled and devices are not required to enter a security key when connecting to the Extended Network SSID.

**WEP** is rated as a low level encryption and is compatible with all wireless devices and operating systems. Using WEP may slow down your wireless performance.

**WPA-PSK** is a medium level encryption and is supported by most wireless devices and operating systems.

**WPA-EAP** requires that the security key is renewed during a set interval.

**WPA2** is a high level encryption and is supported by most wireless devices and operating systems.

**WPA Mixed Mode** allows the use of both WPA and WPA2 at the same time.

If you are not sure which encryption type to use, we recommend you choose WPA/WPA2 Mixed Mode.

#### Additional Authentication Methods:

**MAC:** Restrict access from devices based on their MAC address stored on the MAC Address filter table.

**MAC + RADIUS:** Restrict access from devices based on their MAC address stored on the MAC Address filter table and based on MAC Address authentication via a RADIUS server.

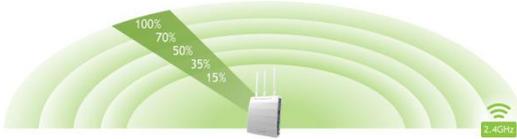
**RADIUS:** Restrict access from devices based on MAC Address authentication via a RADIUS Server.

### **2.4GHz Wi-F Settings: Output Power**

Adjust the output power of the Range Extender / Bridge to control the coverage distance of your 2.4GHz wireless network. For a smaller coverage area, you can select a lower output power. For the maximum wireless coverage, select the 100% selection.

**2.4GHz Wireless Coverage Controls (Transmit Output Power)**

Adjust the output power and range of your 2.4GHz Wi-Fi network. For a smaller coverage area, choose a lower output power percentage. For a larger coverage area, select a higher output power percentage.

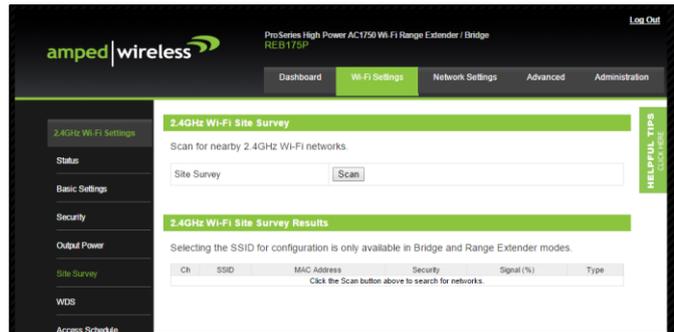


Transmit Output Power

Apply Cancel

## 2.4GHz Wi-F Settings: Site Survey

Scan for local Wi-Fi networks broadcasting within the vicinity of the Range Extender. This feature is useful in determining what other networks are around you and what their basic configurations are in addition to their signal strength in comparison to the Range Extender / Bridge. This feature can also be useful when setting up WDS-AP or WDS-Bridge operational modes when needing to identify the MAC address of other WDS enabled Access Points.



## 2.4GHz Wi-F Settings: WDS

WDS Settings are only available in the WDS-Bridge (WDS-Bridge) operational mode. If you are not using the WDS-Bridge operational mode please disregard this section. WDS mode allows the Range Extender / Bridge to interconnect with other WDS enabled Access Points (such as the Amped Wireless APR175P ProSeries Wi-Fi Access Point/Router). WDS allows you to extend your network by adding additional wirelessly connected Range Extenders, also referred to as a repeater, in addition to Bridges.

For WDS connections to work properly, the MAC address associations must also be configured on each individual WDS enabled Access Point or Bridge, not just the one you are currently configuring. For example, if you are connecting two WDS-APs and one WDS-Bridge, AP 1 must have AP 2's and the Bridge's MAC address configured, while AP 2 has AP 1's and the Bridge's MAC, and the Bridge has AP 1's and AP 2's MAC configured. Every WDS connected device must also be using the same wireless channel as all other WDS connected devices.

The screenshot shows the '2.4GHz WDS Settings' page in the Amped Wireless web interface. The page is titled 'ProSeries High Power AC175P Wi-Fi Range Extender / Bridge' and 'REB175P'. The navigation menu includes Dashboard, Wi-Fi Settings (selected), Network Settings, Advanced, and Administration. The left sidebar shows various settings categories: 2.4GHz Wi-Fi Settings, Basic Settings, Security, Output Power, Site Survey, WDS, Access Schedule, Advanced, 5GHz Wi-Fi Settings, WPS, MAC Address Filtering, VLANs, and WMM / QoS.

The main content area is divided into several sections:

- 2.4GHz WDS Settings:** Includes 'WDS Mode' set to 'Disable' and 'Device MAC Address' set to '74 DA 38 03 EC 2C'.
- 2.4GHz WDS Connections:** A table with columns for 'MAC Address', 'Status', and 'Signal'. It lists four WDS connections, all with a status of 'Not Connected' and a signal strength of '0%'.
- WDS Virtual LAN Assignments:** Includes 'VLAN Mode' set to 'Untagged Port' and a note '(Please enter at least one MAC Address)'. The 'VLAN ID' is set to '1'.
- 2.4GHz WDS Password:** Includes 'Encryption' set to 'None' and a note '(Please enter at least one MAC Address)'. There are 'Apply' and 'Reset' buttons at the bottom right.

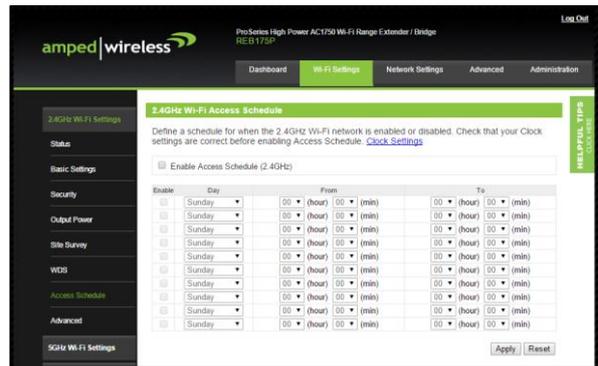
Encryption can be used to secure your WDS connections. If you choose to use encryption (recommended), it is important that you set the same security key setting on all connected WDS enabled Range Extenders and Bridges.

**Note:** When using WDS, it is recommended that you configure the IP address of each WDS connected device to use the same IP subnet and/or ensure that there is only one active router or DHCP server on the network.

## 2.4GHz Wi-F Settings: Access Schedule

Access Schedules will enable or disable your 2.4GHz wireless access at a set time based on your predefined schedule. This feature is often used for restricting access to all users (such as children, employees, guests) during specific times of the day for parental control or security reasons.

- Enable Access Schedule
- Select which days you wish for your 2.4GHz Wi-Fi to be available
- Select the time frame during that day that you wish for your 2.4GHz Wi-Fi to be available
- Apply Changes



**Note:** Make sure you have already configured your Time Zone Settings in order for your schedule to work correctly. Time Zone Settings can be adjusted from the web menu under Administration > System Clock.

## 2.4GHz Wi-F Settings: Advanced Settings

Advanced Wireless Settings should only be adjusted by technically advanced users. It is not recommended that novice users adjust these settings to avoid degrading wireless performance.

**Contention Slot:** Used for contention windows in WMM mode. For more information please go to the WMM section of this User's Guide.

**Preamble Type:** Defines the length of the Cyclic Redundancy Check for communication between the Range Extender and roaming wireless users.

**Guard Interval:** Used to ensure that data transmissions do not interfere with each other. Shorter guard intervals can help to improve overall performance by marginally increasing data rates.

**802.11g Protection:** Increases reliability, but reduces bandwidth.

**802.11n Protection:** Increases reliability, but reduces bandwidth (Provides more bandwidth than 802.11g Protection).

The screenshot shows the '2.4GHz Wi-Fi Advanced Settings' page in the Amped Wireless web interface. The page is titled '2.4GHz Wi-Fi Advanced Settings' and includes a navigation menu on the left with options like Status, Basic Settings, Security, Output Power, Site Survey, WDS, Access Schedule, Advanced, 2.4GHz Wi-Fi Settings, WPS, MAC Address Filtering, and GUIDE. The main content area displays various settings for 2.4GHz Wi-Fi, including Contention Slot (Short), Preamble Type (Short), Guard Interval (Short GI), 802.11g Protection (Enable), 802.11n Protection (Enable), DTM Period (1), RTS Threshold (2347), Fragment Threshold (2346), Multicast Rate (Auto), Beacon Interval (100), Station Idle Timeout (60), WLAN Proxy for Power Saving (Disable), and WLAN Integrity (Enable). The page also includes 'Apply' and 'Cancel' buttons at the bottom right.

**DTIM Period:** Adjusts the delivery traffic indication method period.

**RTS Threshold:** Adjusts the size of RTS data packets. Lower values reduce throughput, but allow the system to recover quicker from interference/collisions. Higher values provide the fastest throughput.

**Fragment Threshold:** The default and recommended setting is at 2346, meaning the Range Extender will never fragment any frames that it sends to wireless users.

**Multicast Rate:** Adjust the transfer rate for multicast packets or choose the “auto” setting.

**Beacon Interval:** Indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Range Extender to synch the wireless network.

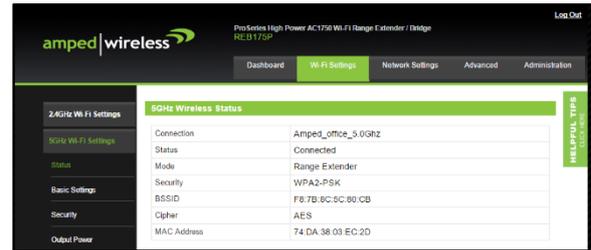
**Station Idle Timeout:** This feature will disconnect connected devices that are no longer active based on a set interval of time.

**WLAN Proxy for Power Saving:** The Range Extender will send an Address Resolution Protocol (ARP) packet instead of STA packets to map IP addresses so that network devices do not need to awake from power saving mode to reply to the ARP packages from the Range Extender. This feature only works when the Range Extender's DHCP server is enabled.

**WLAN Integrity:** This feature will ping the target IP/URL every 60 seconds to verify that a connection is active. If the ping fails five times consecutively, all of the SSIDs for the 2.4GHz radio will all be disabled. Thereafter, the Range Extender will continue to ping the target IP every 60 seconds and will automatically turn on all SSIDs once the ping is successful. By default the Target IP will be the DNS or Gateway IP of the active Internet connection.

### 5.0GHz Wi-F Settings: Status

The 5.0GHz Wi-Fi Status page provides you with a glance at basic information for your 5.0GHz Wi-Fi settings such as the Status, mode, security type, SSID among other details.



## 5.0GHz Wi-F Settings: Basic Settings

The Basic Settings page allows you to adjust settings for your 5.0GHz Wi-Fi networks.

**Enable Wi-Fi Radio:** Disabling will turn off all 5.0GHz Wi-Fi activity. Users will no longer be able to connect wirelessly to your 5.0GHz network.

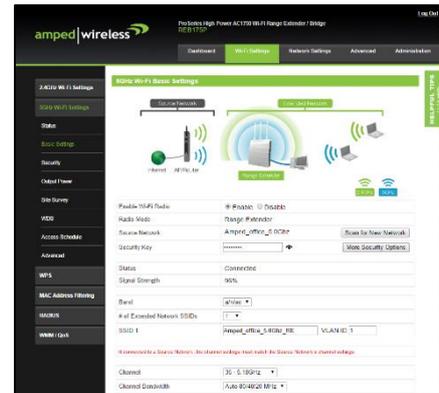
**Radio Mode:** The operational mode of the 5.0GHz radio.

**Source Network:** The SSID of the Source Network that the Range Extender is extending or bridging.

**Scan for a New Network:** To change the Source Network and scan for a new one click this button.

**Status:** The current status of the Range Extender / Bridge and the Source Network.

**Signal Strength:** The signal strength quality between the Range Extender / Bridge and the Source Network. It is recommended that the signal strength is greater than 70% for optimal performance.



**Band:** Select the compatible Wi-Fi standard and speed for your wireless network. This is typically the same band as what the Source Network is operating on to ensure optimal performance.

**# of Extended Network SSIDs:** Select the number of different Extended Network SSIDs you wish to have on the 5.0GHz frequency. Each SSID will represent a network that Wi-Fi devices can see and connect to. The Range Extender allows up to 15 SSIDs per frequency. Each SSID can have a different name, VLAN assignment and security key. Additional SSIDs is sometimes referred to as Guest Networks. (VLAN available in Firewall Range Extender mode only)

**VLAN ID:** Available in Firewall Range Extender mode only. The VLAN ID is a feature that allows you to virtually map connected devices and secure access for each Extended Network SSID created. Devices that are connected to an SSID with a specific VLAN (Virtual Local Area Network) ID cannot access or see devices connected to SSIDs with a different VLAN ID. For example, if SSID 1 is assigned to VLAN 1 and SSID 2 is assigned to VLAN 2, then devices connected to SSID 1 will not be able to see or access devices or files on SSID 2 (VLAN 2). VLAN IDs can range between 1 and 4094.

**Channel:** Select the channel number of the 5.0GHz radio. When connected to a Source Network the channel number of the Range Extender **MUST** match that of the Source Network for normal operation.

**Channel Bandwidth:** Select the channel width for the 5.0GHz radio. It is recommended to match the channel bandwidth of the Source Network for optimal operation.

### 5.0GHz Wi-F Settings: Security

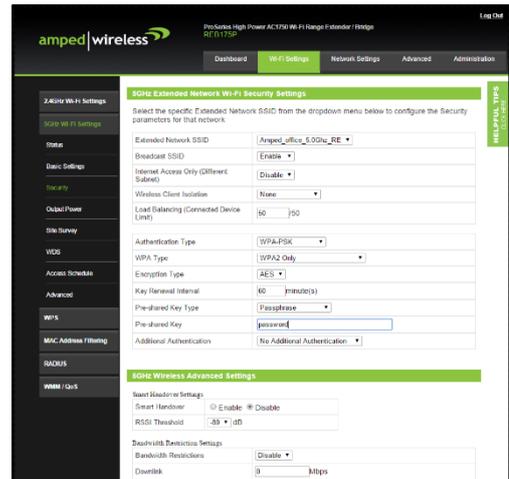
The Extended Network Security page allows you to change the type of wireless security settings for your 5.0GHz Extended Wi-Fi networks.

These settings apply to Range Extender or Firewall Range Extender operational modes. If you are in Bridge Mode or WDS-Bridge mode these options will not be available as there are no Extended Networks in Bridge modes.

**Extended Network SSID Selection:** Using the drop down menu, you can select which Extended Network you wish to configure and may adjust the security settings below.

**Broadcast SSID:** Selecting Disable Broadcast SSID will hide the visibility of the selected Extended Network SSID. Users must manually enter the SSID to connect.

**Internet Access Only:** Choose whether you wish to block Internet access for those devices connecting to the selected Extended Network SSID.



**Wireless Client Isolation:** Enabling this feature provides an extra layer of security by preventing devices connected to the selected Extended Network SSID to communicate with one another. This feature is useful in corporate environments or public hotspots.

**Load Balancing:** Limit the number of devices that can connect to the selected Extended Network SSID. This can assist in managing the bandwidth used by each Extended Network SSID. The maximum number of devices for each SSID is 50 devices.

**Smart Handover:** When multiple Range Extenders (REB175P) or Access Points (APR175P) are installed in an environment where devices roam over a larger area, Smart Handover allows the Range Extender to disconnect a connected device once the signal crosses a defined RSSI decibel (signal receiving sensitivity) threshold to allow it to easily connect to the neighboring Range Extender. Note, some older Wi-Fi devices may not be compatible with the Smart Handover feature.

**Bandwidth Restriction:** When enabled, Bandwidth Restriction limits the amount of bandwidth provided to all devices connecting to the Extended Network SSID.

**Authentication Method:**

**None:** Authentication is disabled and devices are not required to enter a security key when connecting to the Extended Network SSID.

**WEP** is rated as a low level encryption and is compatible with all wireless devices and operating systems. Using WEP may slow down your wireless performance.

**WPA-PSK** is a medium level encryption and is supported by most wireless devices and operating systems.

**WPA-EAP** requires that the security key is renewed during a set interval.

**WPA2** is a high level encryption and is supported by most wireless devices and operating systems.

**WPA Mixed Mode** allows the use of both WPA and WPA2 at the same time.

If you are not sure which encryption type to use, we recommend you choose WPA/WPA2 Mixed Mode.

#### Additional Authentication Methods:

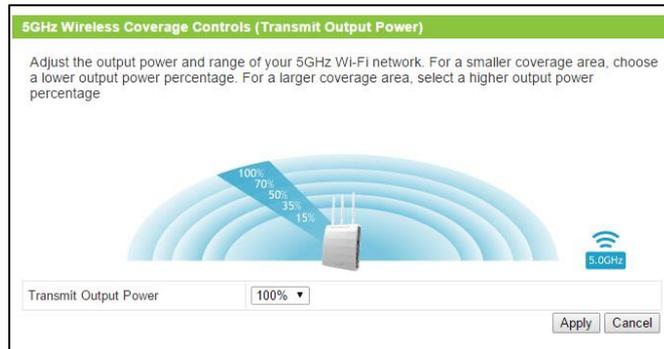
**MAC:** Restrict access from devices based on their MAC address stored on the MAC Address filter table.

**MAC + RADIUS:** Restrict access from devices based on their MAC address stored on the MAC Address filter table and based on MAC Address authentication via a RADIUS server.

**RADIUS:** Restrict access from devices based on MAC Address authentication via a RADIUS Server

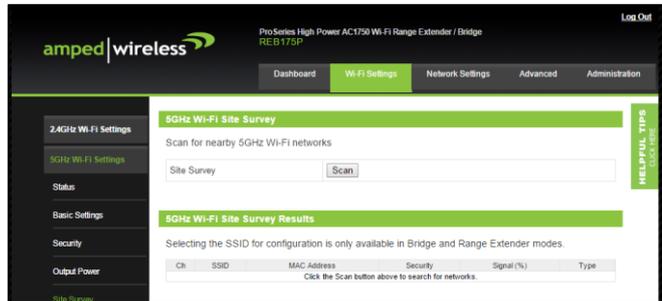
**5.0GHz Wi-F Settings: Output Power**

Adjust the output power of the Range Extender to control the coverage distance of your 5.0GHz wireless network. For a smaller coverage area, you can select a lower output power. For the maximum wireless coverage, select the 100% selection.



## 5.0GHz Wi-F Settings: Site Survey

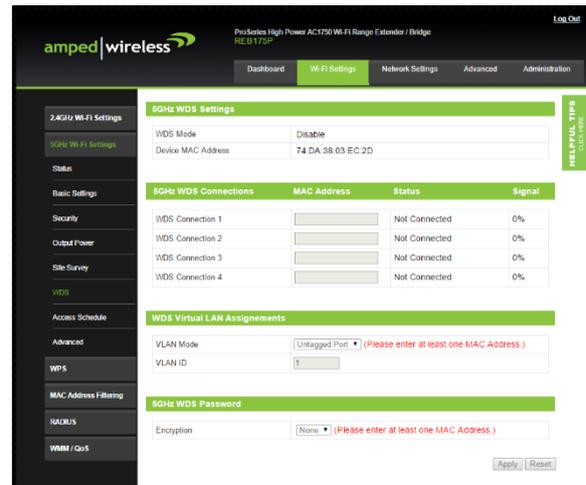
Scan for local Wi-Fi networks broadcasting within the vicinity of the Range Extender. This feature is useful in determining what other networks are around you and what their basic configurations are in addition to their signal strength in comparison to the Range Extender / Bridge. This feature can also be useful when setting up WDS-AP or WDS-Bridge operational modes when needing to identify the MAC address of other WDS enabled Access Points.



### 5.0GHz Wi-F Settings: WDS

WDS Settings are only available in the WDS-Bridge (WDS-Bridge) operational mode. If you are not using the WDS-Bridge operational mode please disregard this section. WDS mode allows the Range Extender / Bridge to interconnect with other WDS enabled Access Points (such as the Amped Wireless APR175P ProSeries Wi-Fi Access Point/Range Extender). WDS allows you to extend your network by adding additional wirelessly connected Range Extenders, also referred to as a repeater, in addition to Bridges.

For WDS connections to work properly, the MAC address associations must also be configured on each individual WDS enabled Access Point or Bridge, not just the one you are currently configuring. For example, if you are connecting two WDS-APs and one WDS-Bridge, AP 1 must have AP 2's and the Bridge's MAC address configured, while AP 2 has AP 1's and the Bridge's MAC,



and the Bridge has AP 1's and AP 2's MAC configured. Every WDS connected device must also be using the same wireless channel as all other WDS connected devices.

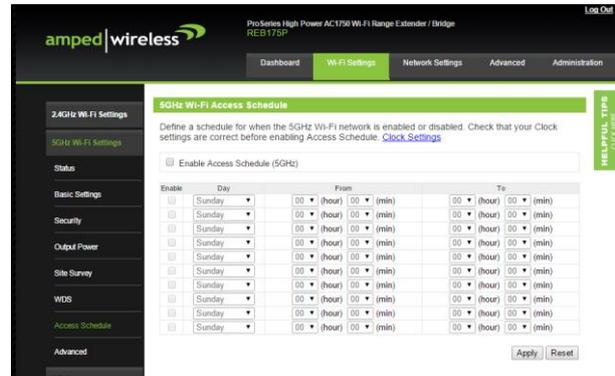
Encryption can be used to secure your WDS connections. If you choose to use encryption (recommended), it is important that you set the same security key setting on all connected WDS enabled Range Extenders and Bridges.

**Note:** When using WDS, it is recommended that you configure the IP address of each WDS connected device to use the same IP subnet and/or ensure that there is only one active Range Extender or DHCP server on the network.

### 5.0GHz Wi-F Settings: Access Schedule

Access Schedules will enable or disable your 5.0GHz wireless network access at a set time based on your predefined schedule. This feature is often used for restricting access to all users (such as children, employees, guests) during specific times of the day for parental control or security reasons.

- a. Enable Access Schedule
- b. Select which days you wish for your 5.0GHz Wi-Fi to be available
- c. Select the time frame during that day that you wish for your 5.0GHz Wi-Fi to be available
- d. Apply Changes



**Note:** Make sure you have already configured your Time Zone Settings in order for your schedule to work correctly. Time Zone Settings can be adjusted from the web menu under Administration > System Clock.

### 5.0GHz Wi-F Settings: Advanced Settings

Advanced Wireless Settings should only be adjusted by technically advanced users. It is not recommended that novice users adjust these settings to avoid degrading wireless performance.

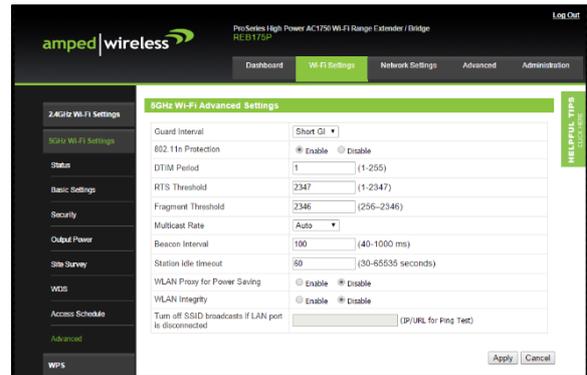
**Guard Interval:** Used to ensure that data transmissions do not interfere with each other. Shorter guard intervals can help to improve overall performance by marginally increasing data rates.

**802.11n Protection:** Increases reliability, but reduces bandwidth (Provides more bandwidth than 802.11g Protection).

**DTIM Period:** Adjusts the delivery traffic indication method period.

**RTS Threshold:** Adjusts the size of RTS data packets. Lower values reduce throughput, but allow the system to recover quicker from interference/collisions. Higher values provide the fastest throughput.

**Fragment Threshold:** The default and recommended setting is at 2346, meaning the Range Extender will never fragment any frames that it sends to wireless users.



**Multicast Rate:** Adjust the transfer rate for multicast packets or choose the “auto” setting.

**Beacon Interval:** Indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Range Extender to synch the wireless network.

**Station Idle Timeout:** This feature will disconnect connected devices that are no longer active based on a set interval of time.

**WLAN Proxy for Power Saving:** The Range Extender will send an Address Resolution Protocol (ARP) packet instead of STA packets to map IP addresses so that network devices do not need to awake from power saving mode to reply to the ARP packages from the Range Extender. This feature only works when the Range Extender's DHCP server is enabled.

**WLAN Integrity:** This feature will ping the target IP/URL every 60 seconds to verify that a connection is active. If the ping fails five times consecutively, all of the SSIDs for the 5.0GHz radio will all be disabled. Thereafter, the Range Extender will continue to ping the target IP every 60 seconds and will automatically turn on all SSIDs once the ping is successful. By default the Target IP will be the DNS or Gateway IP of the active Internet connection.

## WPS Settings

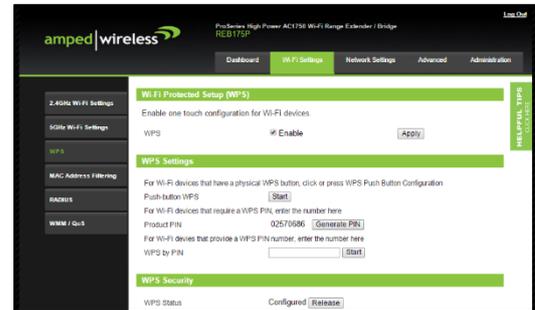
WPS is a Wi-Fi feature created to make Wi-Fi setup simple and easy. Some wireless Range Extenders / Bridges and adapters support this feature with varying names (i.e. one touch setup or WPS).

You may enable WPS setup here by selecting the type of WPS setup you wish to use. The Range Extender / Bridge supports all types of WPS setup:

Option A: Push button: You may push the WPS button on the web menu or use the physical button on the side panel of the Range Extender / Bridge.

Option B: PIN: Some wireless devices use PIN number to access wireless network. If your wireless device requests for a PIN number, use the PIN code located here.

Option C: Enter PIN: If your wireless device has a PIN number, locate the number and enter it into the field. Press Start PIN when ready.

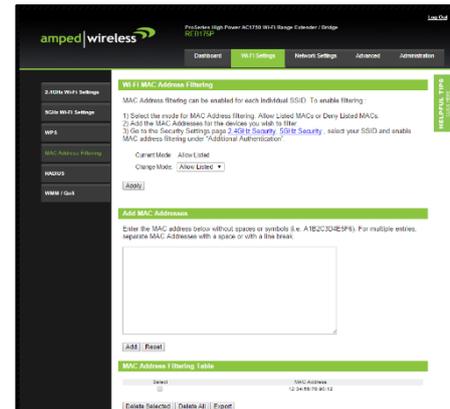


## MAC Address Filtering

MAC Address Filtering allows you to deny access or allow access to specific users connecting to the network. Each networking device has a unique address called a MAC address (a 12 digit hex number). By inputting the MAC address into the field, you can define whether that device is allowed into your network or not allowed. A MAC Address may sometimes be referred to as a Physical Address. Most networking devices have their MAC Address located on a label on the actual device.

For Windows computers with internal networking adapters, the MAC Address can be found by viewing the Network Connection Details of the network adapter. The MAC Address will be listed as the Physical Address.

Be sure to enter the MAC Address without any symbols. For example, a MAC Address of 78-DD-78-AA-78-BB would be entered as 78DD78AA78BB.



Note: Each Wi-Fi Network (WLAN/SSID) must also have MAC Filters selected as Additional Authentication methods in order for MAC Filtering to work. This can be configured here: Wi-Fi Settings > 2.4GHz or 5.0GHz Wi-Fi Settings > Security.

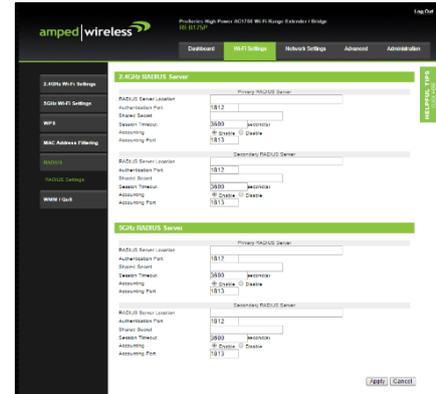
## RADIUS: RADIUS Server

RADIUS servers provide an additional layer of security by requiring that devices be authenticated before gaining access to a network. Authentication normally includes the use of a user name and password that is verified on a predefined database also known as the RADIUS server. The Range Extender supports the use of primary and secondary (backup) RADIUS servers for each frequency: 2.4GHz and 5.0GHz. The Range Extender also provides an internal RADIUS server in the event that an external RADIUS server is not available.

The Internal RADIUS server is only available when the Range Extender / Bridge is in Firewall Range Extender Mode.

Note: Each Wi-Fi Network (WLAN/SSID) must also have RADIUS servers selected as Additional Authentication methods in order for the RADIUS Servers to work. This can be configured here: Wi-Fi Settings > 2.4GHz or 5.0GHz Wi-Fi Settings > Security.

RADIUS Type: Select to use an Internal or external RADIUS server.



**RADIUS Server:** If an external RADIUS server is selected, enter the IP address of the server here.

**Authentication Port:** Set the UDP port used by the server to authenticate (Between 1-65535).

**Shared Secret:** This is the shared password used by both your Range Extender and the RADIUS server. The RADIUS server must also be using this exact password to ensure communication between the two. Enter a password (between 1-99 characters in length).

**Session Timeout:** Set a duration when a connected device's session will timeout. (Between 0-86400) The timeout time begins once the connected device ceases activity with the Range Extender.

**Accounting:** Enable or disable RADIUS accounting.

**Accounting Port:** Set the UDP port used by the server for accounting purposes. (Between 1-65535)

## RADIUS: Internal RADIUS Server

The Internal RADIUS server is only available for Firewall Range Extender mode.

If you chose to use the Internal RADIUS server on the RADIUS Server settings menu you will need to configure the Firewall Range Extender's Internal, built-in, RADIUS server using this page.

Internal Server	<input checked="" type="checkbox"/> Enable
EAP Internal Authentication	<input type="text"/>
EAP Certificate File Format	PKCS#12 (*.pfx/*.p12)
EAP Certificate File	<input type="text"/> Upload
Shared Secret	<input type="text"/>
Session-Timeout	3600 second(s)
Termination-Action	<input type="radio"/> Reauthentication (RADIUS-Request) <input checked="" type="radio"/> Not-Reauthentication (Default) <input type="radio"/> Not-Send

Internal Server: Enable or disable the Internal Server.

EAP Internal Authentication: Select the EAP authentication type from this menu.

EAP Certificate File Format: Accepted certificate file formats are: .pfx and .p12

EAP Certificate File: Upload an EAP Certificate file if you have one available. If no certificate is uploaded the Range Extender will use a self-generated certificate.

**Shared Secret:** This is the shared password used by both your Range Extender and the RADIUS server. The RADIUS server must also be using this exact password to ensure communication between the two. Enter a password (between 1-99 characters in length).

**Session Timeout:** Set a duration when a connected device's session will timeout. (Between 0-86400) The timeout time begins once the connected device ceases activity with the Range Extender.

**Termination Action:** Select how the Internal RADIUS server handles a termination action:

Re-authentication: Sends a RADIUS request to the Range Extender

Not-Re-authentication: Sends a default termination action to the Range Extender

Not-Send: No termination action is sent to the Range Extender

**Note:** Each Wi-Fi Network (WLAN/SSID) must also have RADIUS servers selected as Additional Authentication methods in order for the RADIUS Servers to work. This can be configured here: Wi-Fi Settings > 2.4GHz or 5.0GHz Wi-Fi Settings > Security.

## RADIUS: RADIUS Accounts

If you chose to use the Internal RADIUS server on the RADIUS Server settings menu you will need to add User Accounts to authenticate devices that are logging into your network. Enter the name of each user in the User Accounts field. For multiple entries, separate each User Account by a comma or a space. When you are done, click Add.

Note: Each Wi-Fi Network (WLAN/SSID) must also have RADIUS servers selected as Additional Authentication methods in order for the RADIUS Servers to work. This can be configured here: Wi-Fi Settings > 2.4GHz or 5.0GHz Wi-Fi Settings > Security.

**RADIUS User Accounts**

Enter the User Accounts associated to the Internal RADIUS Server below. For multiple entries, please separate each User Account by a comma or a space. For example: Account\_A, Account\_B, Account\_C. When you are done, click Add.

**User Account List**

Serial	User Name	Password	Customize
No user entries			

## WMM / QoS

WMM, also known as Wi-Fi Multimedia, prioritizes multimedia (audio, video and voice) data going over Wi-Fi to ensure that they receive the needed bandwidth to perform undeterred. Using QoS, also known as Quality of Service) WMM prioritizes data packets in the following order: Voice, Video, Best Effort, and Background. The details for each are:

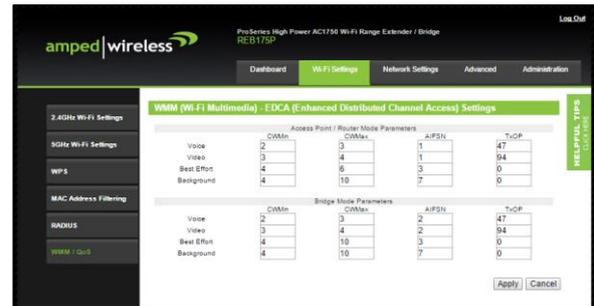
Voice – Includes Voice over IP and audio streaming media packets

Video – Any streaming video

Best Effort – General Internet applications

Background – Low priority Internet applications, such as FTP

If you are an advanced user, the values for each of these prioritizations can be further adjusted and optimized. This is not recommended if you do not understand WMM and its technicalities.



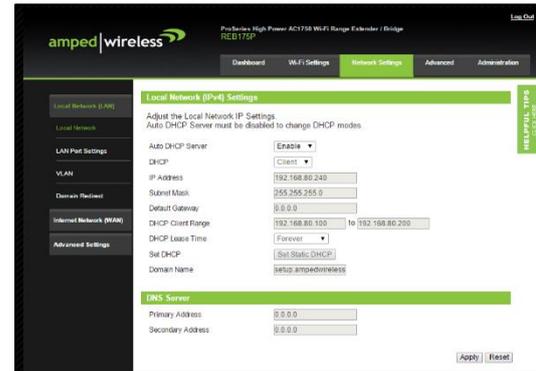
## NETWORK SETTINGS

### Local Network (LAN): Local Network (IPv4)

These settings are for your Range Extender / Bridge's local network only and do not apply to your Source Network.

DHCP: The Range Extender / Bridge includes a feature to help manage the IP addresses within your network automatically. When connected to a network, the Range Extender / Bridge will obtain an IP address from your Source Network or Range Extender / Bridge and act as a DHCP Client. However, when there is no connection available, the Range Extender / Bridge will act as a DHCP Server. You may also manually control the IP settings of the Range Extender / Bridge by choosing Client, Server or Static IP from the DHCP drop down menu.

**Note:** If you choose to use a Static IP address for the Range Extender / Bridge, you will no longer be able to access the web menu using <http://setup.ampedwireless.com>. You must use the assigned IP address to access the web menu.



**IP Address:** The IP address of the Range Extender / Bridge.

**Subnet Mask:** The subnet of the Range Extender / Bridge.

**Default Gateway:** The access point to another network, normally a Router.

**DHCP Client Range:** The range of IP addresses provided by the DHCP server is defined by this field. You can limit how many IP addresses are used in your network by setting a smaller or larger range.

**DHCP Lease Time:** The amount of time each device is given a specific IP is decided by the DHCP lease time. After the Lease Time expires, the DHCP server will assign another IP address to the device.

**Set Static DHCP:** This allows specific devices to be given a specific IP address each time the device connects to the network. The DHCP server will always assign the same IP address to the same device. This feature is often used for shared devices such as network printers or servers.

**Auto DHCP Server:** The Auto-DHCP Server feature automatically manages the IP addresses within your network. When connected to a network that has a DHCP server enabled, the Range Extender/Bridge will automatically obtain an IP from the network's DHCP server and disable the DHCP server on the Range Extender / Bridge to avoid any IP assignment conflicts. For users that are not familiar with how this works, it is recommended to leave Auto-DHCP server enabled on this page.

### Local Network (LAN): LAN Port Settings

Configure settings for your Range Extender's two wired local network ports.

Enable / Disable – Turn the specific wired port on or off

Speed & Duplex – Select a speed for the port

Flow Control – Enable to allow the Range Extender / Bridge to automatically manage data requests to the wired port and avoid packet collisions

802.3az – Power saving feature that disables the port when not in use to reduce power usage

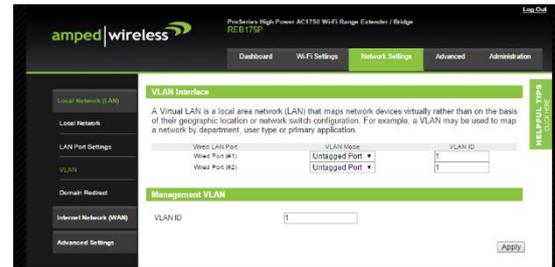
LAN Port Settings (Wired Ports)			
Configure the behavior of the wired ports			
Wired LAN Port	Enable	Speed and Duplex	Flow Control
Wired Port (#1)	Enabled ▾	Auto ▾	Enabled ▾
Wired Port (#2)	Enabled ▾	Auto ▾	Enabled ▾

## Local Network (LAN): VLAN

Virtual Local Area Networks, also known as VLANs, is a feature that allows you to virtually map connected devices and secure access for each wired port. VLAN is available in Firewall Range Extender mode only.

**VLAN ID:** Devices that are connected to a wired port with a specific VLAN (Virtual Local Area Network) ID cannot access or see devices connected to SSIDs or wired ports with a different VLAN ID. For example, if Wired Port #1 is assigned to VLAN 1 and Wired Port #2 is assigned to VLAN 2, then devices connected to Wired Port #1 will not be able to see or access devices or files on Wired Port #2 (VLAN 2). VLAN IDs can range between 1 and 4094.

**Tagged / Untagged** – VLAN enabled ports are generally categorized as tagged or untagged. This is also referred to as trunk or access. The purpose of tagging a port is to pass traffic for multiple VLANs, whereas an untagged port accepts traffic for only a single VLAN. For example, if you are connecting a switch to one of the Wired Ports on the Range Extender / Bridge, this would generally be a tagged port since it will be connecting to a network with multiple VLANs. To successfully configure a tagged port both ends must have the following in common: encapsulation and VLAN settings. Both sides should be configured identically for the VLAN to work properly.



### Local Network (LAN): Domain Redirect

Domain Redirect allows access to the web interface via a simple web URL: <http://setup.ampedwireless.com> Disabling Domain Redirect will require that you access the web menu using the IP address instead of the web URL. It is recommended that you note your IP address before disabling this mode, or refrain from disabling Domain Redirect. If you are no longer able to access the web menu and you do not have the IP address of your device a hardware reset will be required.

#### Domain Redirect

Domain redirect allows access to the web interface via a simple web URL :  
<http://setup.ampedwireless.com>  
Disabling Domain Redirect will require that you access the web menu using the IP address of this device. It is recommended that you note your IP address before changing this mode. If you are no longer able to access the web menu, you will need to perform a hardware reset.

Domain Redirect

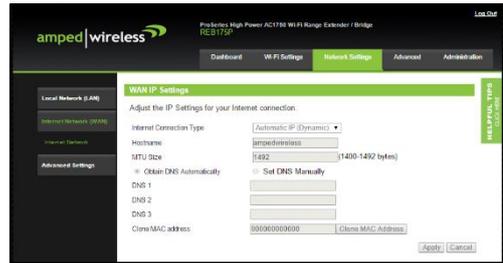
Enable  Disable

## Internet Network (WAN): Internet Network (WAN) IPv4

WAN settings only apply to Firewall Range Extender mode.

The Firewall Range Extender Basic Setup will assist in the initial configuration of your WAN settings, however, in the case that you wish to adjust settings manually, the options on this page provides you with the tools to do this easily.

Select your WAN Connection type from the drop down menu:



The screenshot displays the 'WAN IP Settings' page in the amped|wireless web interface. The page title is 'WAN IP Settings' and it includes a sub-header 'Adjust the IP Settings for your Internet connection.' The interface features a navigation menu on the left with options for 'Local Network (LAN)', 'Internet Network (WAN)', 'Internet Network', and 'Advanced Settings'. The main content area contains the following fields and options:

- Internet Connection Type: A dropdown menu set to 'Automatic IP (Dynamic)'.
- Hostname: A text input field containing 'ampedwireless'.
- MTU Size: A text input field containing '1492'.
- Obtain DNS Automatically: A radio button that is selected.
- Set DNS Manually: An unselected radio button.
- DNS 1, DNS 2, and DNS 3: Three empty text input fields.
- Clone/MAC address: A text input field containing '00:00:00:00:00:00' and a 'Clone MAC Address' checkbox.
- Buttons: 'Apply' and 'Cancel' buttons at the bottom right.

**Manual IP (Static):** For Internet connections where the Internet provider does not provide you with an IP address automatically. If you know the IP address and DNS settings that your Internet provider uses, select this option.

**Automatic/Dynamic (DHCP):** This is the configuration type most often used by Internet providers. Automatic configurations are used by both DSL and Cable as well as other providers. Under the Automatic Configuration method, the Internet provider will assign your Firewall Range Extender an Internet IP address automatically.

If for some reason you do not get an IP address and you know that your Internet provider uses DHCP, try resetting your modem. Remove the power adapter from the modem as well as the backup battery (if

available). Wait about 30 seconds and then power the modem back on. You can run through the Basic Setup Wizard again to see if that fixes your Internet connection issues.

**DNS Settings:** Domain name server settings can be set automatically by your Internet service provider or set manually to a DNS server of your choice.

**Clone MAC Address:** The Firewall Range Extender can use a MAC address that you define as its own. This is often used when an Internet Provider only authorizes one MAC address to access the Internet. Cloning the MAC address will make it so that the cloned MAC address is the only MAC address seen by the Internet Provider.

## Advanced Settings

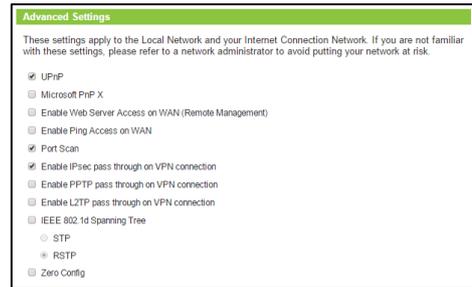
These settings apply to the Local Network and your Internet Connection Network. If you are not familiar with these settings, please refer to a network administrator to avoid putting your network at risk.

**Enable uPnP:** Universal Plug and Play is a network feature that allows uPnP enabled devices to “just work” with each other when connected to the same network. UPnP can work across different network media, such as an Ethernet connection or wireless connection. With UPnP enabled, network devices may change security settings within the Firewall Range Extender’s firewall to allow access over the Internet. By default, UPnP is disabled to avoid exposing your network to security issues.

**Enable Web Server Access on WAN (Remote Management):** Allows access to the Web Menu over the Internet.

**Enable Ping Access on WAN:** Allows users to ping the WAN interface IP address from the Internet.

**Port Scan:** Monitors requests to a range of server port addresses to block incoming DoS attacks.



Enable IPsec pass through on VPN connection: Allows the IP security protocol suite to pass through on a VPN connection.

Enable PPTP pass through on VPN connection: Allows the PPTP protocol suite to pass through on a VPN connection.

Enable L2TP pass through on VPN connection: Allows the L2TP protocol suite to pass through on a VPN connection.

802.1d Spanning Tree (STP): A network protocol that ensures a loop-free topology for networks that have Ethernet bridges. The STP prevents bridge loops and allows a network design to include redundant links to provide automatic backup paths if active links fails.

Zero Configuration: Assigns an IP address (169.254.x.x) to any connected device that cannot obtain an IP address or when there is no DHCP server present on the network. This allows all devices to have the same subnet to enable communication with each other. Connecting devices must be in DHCP Client mode (not Static) for this feature to work.

## ADVANCED SETTINGS

Many of the features in the Advanced Settings menu are available only in Firewall Range Extender operational mode.

### Port Forwarding

Port Forwarding is only available in Firewall Range Extender mode.

Port Forwarding is a rule that tells the Range Extender that if a specific type of request comes in on a specific port, then that request should be forwarded to a specific device on the private network.

Port Forwarding is often used for setting up servers, cameras and other devices that require remote access.

**Enable Port Forwarding:** Enables designated ports to begin forwarding.

**IP Address:** The IP address of the device behind the Firewall that is being designated for Port Forwarding.

**Protocol:** Select UDP, TCP or Both for the protocols to be forwarded.

**Port Range:** Select a range of ports for the designated IP address that you wish to be forwarded.

**Comment:** Create a name that you can use to easily identify this Port Forwarding entry.

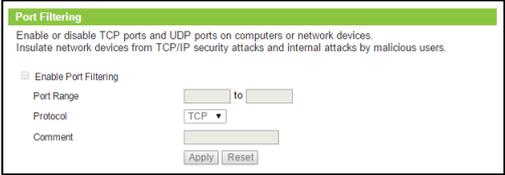
## Port Filtering

Port Filtering is only available in Firewall Range Extender mode.

Port Filtering is a security measure that prevents users from using specific ports for reasons other than what those ports were originally intended for. For example, TCP port 21 is traditionally used for FTP. However, there is nothing stopping a user from using port 21 for purposes other than FTP access. By enabling Port Filtering on TCP port 21, only FTP communications would be allowed. No other types of communication would be allowed on this port.

Hackers may sometimes scan for all open ports on your network as a method of hacking into your network. Port Filtering and other firewall features help to prevent this from happening.

To set up Port Filtering, select a range of ports you wish to filter. If you are trying to filter a single port, enter the port number twice (For example, Port 21: 21 – 21). Select the Protocol of the port you are filtering. If you do not know what protocol you wish to filter, select “Both”.



The screenshot shows a configuration window titled "Port Filtering". Below the title is a green header bar. The main content area contains the following text and controls:

- Enable or disable TCP ports and UDP ports on computers or network devices.  
Insulate network devices from TCP/IP security attacks and internal attacks by malicious users.
- Enable Port Filtering
- Port Range: [ ] to [ ]
- Protocol: [ TCP ▼ ]
- Comment: [ ]
- [ Apply ] [ Reset ]

## DMZ (Demilitarized Zone)

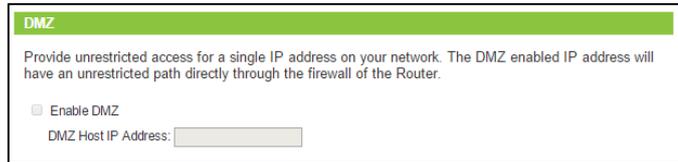
DMZ is only available in Firewall Range Extender mode.

A DMZ is a network location or IP Address that is not protected by the firewall. When enabling DMZ, it is important to note that the device on the IP Address designated as part of the DMZ does not have any protection from the Range Extender's firewall. The device's only security would be those built into the operating system.

As a general safety rule, devices placed on the DMZ should not have any other network connections to any other devices.

Enable DMZ: Enables the Demilitarized Zone.

DMZ Host IP Address: The designated IP Address of the network device to have unrestricted access through the Range Extender's Firewall.



**DMZ**

Provide unrestricted access for a single IP address on your network. The DMZ enabled IP address will have an unrestricted path directly through the firewall of the Router.

Enable DMZ

DMZ Host IP Address:

## Denial of Service

Denial of Service is only available in Firewall Range Extender mode.

A Denial of Service attack is an attempt by a user (or users) to make a server's or network's services unavailable. The user sends a server multiple requests with false return addresses.

The server will attempt to respond by sending a request back to the user; however, since the address is false, the server will wait for a response before closing the connection. When multiple requests like this occur, servers may often get overloaded with too many requests and stop functioning altogether. This is a typical DoS attack, although DoS attacks may not be limited to this type of attack.

The Firewall Range Extender can assist in preventing these types of attacks by scanning the network for patterns of activity that represent DoS attacks. If a pattern comes in frequently, the Firewall Range Extender can attempt to block messages containing that pattern and thus protect the server from becoming overloaded and unresponsive.

**Basic Denial of Service features**

Prevent specific DoS attacks from entering the network. A Denial of Service (DoS) attack is characterized by an explicit attempt by malicious users to prevent legitimate users from use of a specific internet service. To activate your protection, enable the DoS Prevention below and configure the specific settings.

Ping of Death	<input checked="" type="checkbox"/>
Discard Ping on WAN	<input checked="" type="checkbox"/>
Port Scan	<input checked="" type="checkbox"/>
Sync Flood	<input checked="" type="checkbox"/>

**Advanced Denial of Service features**

Ping of Death	40	packet(s)	per	second	burst	40
	<input checked="" type="checkbox"/> NMAP FIN / URG / PSH <input checked="" type="checkbox"/> Xmas tree <input checked="" type="checkbox"/> Another Xmas tree					
Port Scan	<input checked="" type="checkbox"/> Null scan <input checked="" type="checkbox"/> SYN / RST <input checked="" type="checkbox"/> SYN / FIN <input checked="" type="checkbox"/> SYN (only unreachable port)					
Sync Flood	40	packet(s)	per	second	burst	40

## IDS (Intrusion Detection System)

Monitor network activities for malicious activities and connection violations. IDS will allow you to block devices that repeatedly fail to connect. When “Block devices” is enabled and a device attempts to connect to the AP, but fails three times within sixty seconds, the device will be blocked for a duration of thirty minutes. (IDS works with WPA based authentication and 802.1x authentication. IDS will not work with networks using WEP security).

IDS can also email you to notify you of these failed login attempts. You will need to set up your email notification settings before notifications will work.

**IDS (Intrusion Detection System)**

Intrusion detection system (IDS) will monitor network activities for malicious activities or policy violations.

- Enable IDS (Intrusion detection system)
- Block devices that repeatedly fail to associate and authenticate
- Send IDS notifications to Email [Configure Email settings](#)

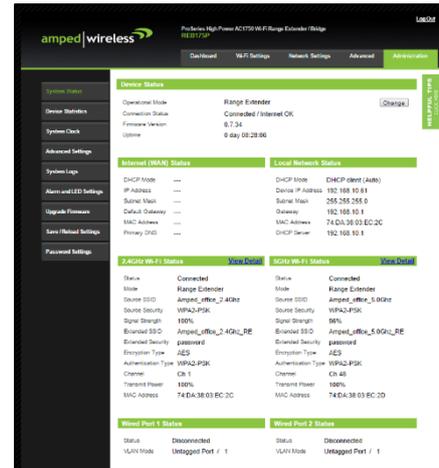
## ADMINISTRATION

### System Status

The Administration System Status will provide you with the current status of the Range Extender. It provides you with glance at general setup information such as the current operational mode, firmware version and uptime of the Range Extender. From here you can quickly change the operational mode by clicking the “Change” button to the right of the operational mode.

In addition to the operational mode, the System Status also provides you with information regarding your Source Network connection, Extended Networks and Local Network settings.

At the bottom of the page you will find details about the Wired Port settings.



## Device Statistics

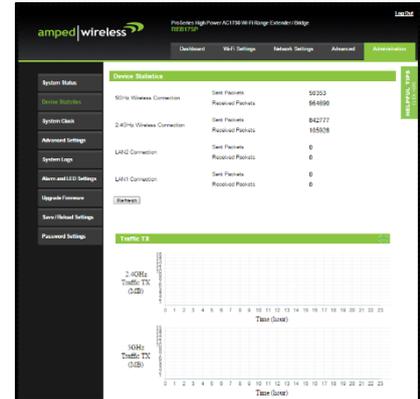
Device statistics shows the detailed information regarding the device and data activity for each connection type on the Range Extender / Bridge (Internet, Wireless and Wired).

The Wireless Connection statistics shows all data activity for both the 2.4GHz and 5.0GHz wireless networks separately.

The Wired Connection statistics shows all data activity for all users physically connected to the wired ports on the Range Extender / Bridge.

The Internet Connection statistics shows the data activity for all upload and download data over your Internet connection, this data normally displays when the Range Extender / Bridge is in Firewall Range Extender mode.

The time intervals for the statistics are by the hour so you may need to wait for the Range Extender / Bridge to be active for at least an hour to begin seeing data on the graphs.



Each report can be collapsed by clicking the ( - ) icon on the top right of each section. To enlarge the report simply click the ( + ) icon.

## System Clock

Maintain the internal clock for the Range Extender / Bridge by syncing with your computer's time or through a network time server. Your system clock settings need to be accurate in order for logs and wireless access schedules to work correctly. To sync with the Internet, a connection to a Source Network with an active Internet connection is required.

Maintain the system clock settings by syncing the system time with the time on your computer. The Router's clock is used to make sure your Access Schedules and logs function correctly and on time.

### System Clock

Current Time : May Month 16 Day 201 Year  
0 Hours 00 Minutes 00 Seconds

Sync with your computer :

### Sync with the Internet

Select a Time Zone : (GMT-08:00) Pacific Time (US & Canada); Tijuana

Enable Network Time Protocol (NTP) Updates

NTP server : 192.5.41.41 - North America  
 (Manual IP Setting)

## Advanced Settings

**Product Name:** The name of the product is used to easily identify the Range Extender / Bridge in the case where multiple Range Extender / Bridges are installed in the same location. Choose a name consisting of up to 32 characters.

**Management Protocol:** The Range Extender / Bridge supports multiple management interfaces. Check the interfaces that you wish to enable:

HTTP: Standard Internet web browser interface

HTTPS: Secured web based Internet web browser interface

TELNET: Virtual terminal connection using the telnet protocol and client

SSH: Client server model using the Secure Shell network protocol

SNMP: Simple Network Management Protocol: Supports v1, v2 and v3 protocols.



The screenshot shows the 'Advanced Settings' configuration page. The 'Product Name' field is set to 'Access Point 3'. Under 'Management Protocol', the checkboxes for HTTP and HTTPS are checked, while TELNET, SSH, and SNMP are unchecked. The 'SNMP Version' is set to 'v1/v2'. The 'SNMP Get Community' is 'public', and the 'SNMP Set Community' is 'private'. The 'SNMP Trap' is set to 'Disabled', and the 'SNMP Trap Community' is 'public'. The 'SNMP Trap Manager' field is empty.

If the SNMP Management Protocol is selected you may configure the following settings for SNMP settings:

SNMP Version: Select the SNMP version for your SNMP manager

SNMP Get Community: Enter the Get Community name for SNMP-GET requests

SNMP Set Community: Enter the SNMP Set Community name for SNMP-SET requests

SNMP Trap: Enable or disable SNMP trap to notify managers or network errors

SNMP Trap Community: Enter the SNMP Trap Community name for SNMP-TRAP requests

SNMP Trap Manager: Specify the IP address for the SNMP Manager

## System Logs

The System Log is useful for viewing the activity and history of the Range Extender / Bridge. The System Log is also used by Amped Wireless technicians to help troubleshoot your Range Extender when needed. It is recommended that you enable all logs in the event that troubleshooting is required.

**System Log Server:** Enable or disable the use of a System Log Server for storing system logs onto another computer.

**Transfer Logs:** Enter the IP address of a System Log Server if you wish to use.

**Copy Logs to USB Drive:** Enable and attach a USB drive to the USB port to store files locally on a USB drive.

**Send Logs to Email:** Enable to send logs to a designated Email address.

**Email Settings:** If you have enabled logs to be sent via Email, you will need to configure the outgoing Email server settings to successfully send logs via Email. Enter the settings for your Email server here.

View network and system activity for your Router.

### System Logs Settings

System Log Server:  Enable

Transfer Logs:

Copy Logs to USB Drive:  Enable

Send Logs to Email:  Enable

Email Settings

SMTP Server:  SMTP Port:

Senders Email:  Receivers Email:

SSL:  Disable

Account:  Password:

### Logs

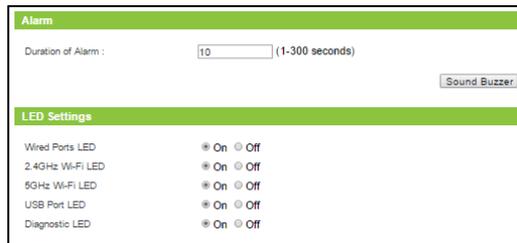
```

May 16 00:00:51 [SYSTEM] WLANP_4G_Best channel selection start switch to channel 4
May 16 00:00:48 [SYSTEM] WLAN[S] Best channel selection start switch to channel 35 + 40 + 44 + 48
May 16 00:00:45 [SYSTEM] LAN_PoPo[0] link is changed to 100Mbps-Full-Duplex
May 16 00:00:33 [SYSTEM] LAN_PoPo[0] link status is changed to down
May 16 00:00:29 [SYSTEM] WLAN[S] Channel = AutoSelect
May 16 00:00:28 [SYSTEM] WLAN[S] Wireless Mode = 11AC/n-TXO
May 16 00:00:28 [SYSTEM] WLANP_4G_Channel = AutoSelect
May 16 00:00:28 [SYSTEM] WLANP_4G_Wireless Mode = 11NG+n-TXO/n-TXO
  
```

**Alarm and LED Settings**

The Range Extender / Bridge features an internal audio alarm which can be used for multiple purposes. The alarm can be used to easily identify the location of a Range Extender / Bridge. You can also set the duration for the sound.

LED lights can also be turned on or off. Select the LED lights that you wish to remain on or off during normal usage.



## Upgrade Firmware

Amped Wireless continuously updates the firmware for all products in an effort to constantly improve our products and their user experiences. When connected to an active connection with Internet access, the Range Extender / Bridge can automatically check for new firmware updates that are available by pressing **Check Now**. Follow the prompts to complete the upgrade process.

Before upgrading the firmware, remember to always save your current settings first by going to the [Save/Reload Settings page](#). The firmware upgrade process will reset the settings of the Range Extender / Bridge to default settings.

Manual Firmware Upgrade: In the case that the Range Extender / Bridge does not have access to the Internet, you can manually upgrade the firmware by downloading the firmware file from the Amped Wireless Elite Support website. The firmware update is downloaded as a zip file and you will need to have an unzipping

The Wi-Fi Access Point / Router uses software (firmware) to operate. In the event that a new firmware file is available you may update it here. During the upgrade process DO NOT power off the device to avoid damage to the Wi-Fi Access Point / Router.

Current Firmware Version: 0.7.23  
Build Time: Fri Nov 28, 2014

**Important:**  
Before upgrading firmware, always save your current settings from the Save/Reload Settings page.

Check for New Firmware Updates:  
(Internet connection required.) **CHECK NOW**

**Upgrade Firmware**

Update Firmware from:  A file on your computer  
 A file on your USB drive (No USB device connected)

**Manually Upgrade Firmware from a File**

Check the [Support Website](#) to see if there are any updates available for this product.

Select File:  No file chosen

program to open the file. Inside the file will be a text document with details on the current firmware release and instructions on how to upgrade the firmware.

To manually upgrade your firmware:

- a. Download the file from the [www.ampedwireless.com/support](http://www.ampedwireless.com/support) website and remember the location where you saved it. You can save the file to a USB drive and attach the USB drive to the Range Extender / Bridge, or you may save the file to your PC desktop and choose the file from the web menu. Firmware files may also be provided by Amped Wireless support reps.
- b. Click Browse and locate the file.
- c. Click Upload to begin upgrading.

**Note:** Firmware files normally have a `.bin` file extension.

## Save / Reload Settings

Saving your current settings allows you to back-up your current settings which may be reloaded at a later time.

You can save or load settings from your computer or from a USB drive attached to the Range Extender / Bridge.

To save settings, click Save. For added security, you can also choose to encrypt the saved settings with a password. If you choose to do so, you will need to enter this password in the future when you choose to reload the saved settings.

To reload previously saved settings, click Choose File and find the file that you previously saved on your PC or USB drive. If you have previously encrypted the file, you will need to enter a password here.

You may also reset the Range Extender / Bridge's settings to factory settings by pressing Reset. By resetting the Range Extender / Bridge you will lose all previous configurations.

Save your current configurations to a file or reload previously saved configurations. If needed, you may also reset your Access Point to factory default settings.

### Save/Reload Settings

Using Device  
 Using your Computer  
 Using your USB device

Save Settings  
  Encrypt the configuration file with a password:

Reload Settings  
 No file chosen  
 Open the configuration file with a password:

### Factory Default/Reset

Reset settings to factory default settings. Note: all of your current configurations will be erased.

### Reboot

Reboot the Access Point. All current settings will be retained.

Rebooting the Range Extender / Bridge saves your current configurations and simply power cycles the Range Extender / Bridge.

## Password Settings

The default settings for the Range Extender are:

Login: admin

Password: admin

If you wish to enable a password to protect unauthorized access to the web menu, you may enter one here.

Prevent unauthorized access to your Router's web-based configuration menu by providing a user name and password. If no protection is necessary, leave these fields blank and you will not be prompted for a login and password when accessing this web menu.

**Password Settings**

Login Name :

Login Password : (4-32 Characters)

Confirm Password :

## **TECHNICAL SPECIFICATIONS**

Wireless Standard: 802.11a/b/g/n/ac

Frequency Band: 2.4 GHz, 5.0GHz

Wireless Speed: 2.4GHz: Up to 450Mbps

5GHz: Up to 1300Mbps

Amplifier: 3 x High Power 5GHz Amplifiers

3 x High Power 2.4GHz Amplifiers

3 x 5.0GHz Low Noise Amplifiers

3 x 2.4GHz Low Noise Amplifiers

Wireless Security:

- WEP, WPA, WPA2, WPA Mixed, WPS

Antennas:

- 3 x Detachable High Gain Antennas
- 3 x Reverse SMA Connector

Ports:

- 1 x RJ-45 10/100/1000 LAN port
- 1 x RJ-45 10/100/1000 PoE / LAN Port
- 1 x USB 2.0 Port

Mounting:

- Wall, Magnetic, Desktop

Warranty: 1 Year

Setup Requirements:

- Wired or wireless PC/Mac and an available 802.11b/g/n/ac wireless network
- Google Chrome, Internet Explorer (8.0 and up) or Safari web browser

## ***DEFAULT SETTINGS***

The default settings for your Range Extender / Bridge are listed here. If for some reason you need to return your Range Extender / Bridge back to default settings, hold down the Reset button on the back panel for 10 seconds. The Range Extender / Bridge will reset back to factory settings as listed below:

IP Address: 192.168.80.240

Web Menu Access: <http://setup.ampedwireless.com>

Login: admin

Password: admin

2.4GHz SSID: Amped\_REB\_2.4

5GHz SSID: Amped\_REB\_5.0

### *TROUBLESHOOTING & SUPPORT INFORMATION*

We are here to help. If you have any issues with your Range Extender / Bridge please contact us.

To contact Amped Wireless' Technical Support use one of the following methods:

Phone: 888-573-8820

Email: [techsupport@ampedwireless.com](mailto:techsupport@ampedwireless.com)

Web: [www.ampedwireless.com/support](http://www.ampedwireless.com/support)

## Troubleshooting

The tips in this guide are listed in order of relevance. Try solution (a) before trying solution (b), etc.

### Troubleshooting: Web Menu Access Issues

**I entered <http://setup.ampedwireless.com> and it failed to open the Web Menu.**

- a. Make sure your computer is connected to the Range Extender's Wi-Fi network: Amped\_REB\_2.4 or Amped\_REB\_5.0 (only for Range Extender and Firewall Range Extender Mode)
- b. Try to use a different web browser. We recommend the Google Chrome web browser.
- c. Try to open your web browser to the default IP address by putting this number into your web browser instead: 192.168.80.240
- d. Power off (unplug the power adapter from the Range Extender) the Range Extender and power it back on. Try again.
- e. Reset your Range Extender to default settings by holding the Reset Button (located on the back panel) for ten (10) seconds and try again.
- f. If steps (a) through (e) fail, disconnect your PC from all Wi-Fi networks. Attach an Ethernet cable between the Range Extender and your PC. Try to access <http://setup.ampedwireless.com> again.

**I could NEVER log on to the Range Extender or Firewall Range Extender wirelessly.**

- a. Check that your wireless adapter supports WPA2 or WPA wireless security. If it does not then you will need to change the wireless security on the Range Extender. Go to the Web Menu, select Wireless Settings and then Wireless Security. Select the Extended Network from the drop down menu and either disable security or downgrade the security to WEP. Try connecting again.
- b. The connection to the Source Network may be down. Use an Ethernet cable and connect directly to the Range Extender. Access <http://setup.ampedwireless.com> and run through the Basic Setup again. After you have successfully reset the Source Network connection, try connecting wirelessly again.

**I can no longer access the Web Menu or the Range Extender or Firewall Range Extender no longer responds.**

- a. Connect to your Range Extender and try to access <http://setup.ampedwireless.com> using your web browser.
- b. If you are advanced in networking troubleshooting, log onto your Source Router's web interface. Look for the DHCP client list and try to find the IP address of your Range Extender assigned by your source router. Once you have it, connect to the Range Extender using an Ethernet cable. Open your web browser and enter the IP address into the address bar.
- c. Reset the Range Extender back to default settings and try the Setup Wizard again. To reset the Range Extender back to default settings, push the Reset Button (on the back panel) down for five (5) to ten

(10) seconds then let go. After the Range Extender has fully reset, use an Ethernet cable and connect to the Range Extender. Login to the Web Menu at <http://setup.ampedwireless.com> and run through the Wizard.

### Troubleshooting: Source Network Connection Issues

#### **I cannot connect to my Source Network. I received an error when running Basic Setup.**

- a. Your Source Network may be secured. Double check that you have the correct security key to connect to the Source Network.
- b. Your Range Extender / Bridge may be located too far from your Source Network. Run through the Basic Setup Wizard again. On the SCAN page, your Source Network should show a signal strength of 70% or greater. If it does not, move the Range Extender / Bridge closer to your Source Network and try again.
- c. If you are connecting to a dual band router, both networks (2.4GHz and 5.0GHz) should have a signal strength of 70% or greater.
- d. Check that your antennas are connected to their corresponding antenna connectors. The number designated on the antenna (1-3) should match the number on the antenna connector (1-3).
- e. Check to see that your Source Network router's DHCP server is enabled. The Range Extender / Bridge needs to obtain an IP from your Source Network router.

**I cannot find my Source Network when scanning for wireless networks in the Basic Setup Wizard.**

- a. The Range Extender / Bridge may be out of range. Move the Range Extender / Bridge closer towards the wireless router and try Basic Setup again from the Web Menu. It is recommended that your Source Network shows a signal strength of 70% or greater in the Setup Wizard SCAN results.
- b. Go to the Wi-Fi Settings tab in the web menu and access the Wireless Coverage Controls for your specific wireless network (2.4GHz or 5.0GHz). Make sure the setting is at 100% and try again.
- c. Make sure that your Source Network's wireless SSID is broadcasting and not hidden. If your Source Network SSID is hidden, you will need to manually setup the Range Extender / Bridge through the Wi-Fi Settings > Basic Settings.

**My Range Extender / Bridge was working fine previously, but now I can no longer access the Internet through the Range Extender / Bridge. Or, I had a **POWER OUTAGE** and now the Range Extender / Bridge no longer works.**

The Range Extender / Bridge should automatically heal itself and reconnect to your wireless network. However, in the event that it does not and you are not able to access the Internet or your Source Network please try the following options:

- a. Reboot the Range Extender / Bridge, wait 3 minutes for the Range Extender /Bridge to reconnect to your network and try to access the Internet.
- b. The connection to your Source Network may have been dropped or the router settings may have changed. Changes to the router could be a result of several events, such as a power outage. When this occurs, connect to the Range Extender and access the setup menu using the web address: <http://setup.ampedwireless.com>. Run the Setup Wizard to reconnect the Range Extender to your network.
- c. The Range Extender / Bridge may be too far from your Source Router and not maintaining a signal strength of above 70%. Check the signal strength between the router and the Range Extender through the web menu (left side): Dashboard > System Status. The Signal Strength readout will be under the Source Wireless Network Settings section. This Signal Strength must be above 70%. If it is below, move the Range Extender / Bridge closer to your router, or reposition the Range Extender / Bridge.
- d. Check that your antennas are fastened tightly to the antenna connectors.
- e. Rescan for another network by accessing <http://setup.ampedwireless.com> to connect to and repeat or you may try to fix the issues with your Source Network and your home wireless router.
- f. Check to see that your home wireless router settings have not changed. Any changes to the SSID, security, or channel number from the original settings will disconnect the Range Extender / Bridge's connection to the Source Network. To solve this simply run the Basic Setup Wizard again from the web

menu and reconfigure your Source Network connection. You can also set a static channel number on your router to prevent this from happening again in the future.

- g. If you cannot access the setup menu, check to see that the Range Extender / Bridge is still on. Reboot the Range Extender / Bridge by unplugging the power adapter and plugging it back in. Check to see if your connection has been reestablished by viewing a website. If you do not have a connection, logon to <http://setup.ampedwireless.com> and configure a new Source Network connection.
- h. Check to see that the wireless router is still on. If it has been turned off please turn it back on. The Range Extender should automatically reconnect to your Source Network within 10 minutes.

**I have a dual-band router and I cannot extend the network (or both networks).**

- a. The Range Extender / Bridge will repeat or connect the 2.4GHz signal and the 5.0GHz signal from your router simultaneously in Range Extender Mode and WDS-Bridge mode only. If you are using another mode, the Range Extender / Bridge will only connect to a single network.
- b. When connecting to dual band networks in Range Extender or WDS-Bridge mode, the networks must have a signal strength of 70% or greater with the Range Extender / Bridge for a reliable connection. Make sure that your dual band router is close enough to the Range Extender / Bridge to receive a strong signal.

- c. Check to make sure that you have the correct security key for both the 2.4GHz and 5.0GHz network of your dual band router. These keys may sometimes be different from each other.
- d. Check that your antennas are fastened tightly to the antenna connectors.
- e. Ensure that your dual band router does not have any security features enabled, such as MAC address filtering. If it does, disable it and try again.

**I am connected to a Source Network, however, I do not have Internet access.**

- a. The Source Network itself may not have Internet access. Check to see that you have internet access by connecting directly to the Source Network first. If you are able to go online then this is not a problem. If you cannot go online, then the Source Network's Internet connection must first be resolved.
- b. You may have a DNS issue and the Range Extender / Bridge is not obtaining the IP settings from your Source Network. Try to reboot the Range Extender / Bridge. If that fails, then reboot the Source Router to see if that fixes it.
- c. There may be an IP conflict with your Source Network and your Extended Network. Try to adjust the IP Settings of your Extended or Bridged Network using IP values that are different from your Source Network.

**I can no longer connect to the Range Extender wirelessly.**

- a. Power on and off the Range Extender and try again.
- b. The connection to the Source Network may be down. Use an Ethernet cable and connect directly to the Range Extender / Bridge. Access <http://setup.ampedwireless.com> and run through the Basic Setup Wizard again. After you have successfully reset the Source Network connection, try connecting wirelessly again.

**The connection to the Source Network seems slow. File transfers take a long time to transfer.**

- a. You may be too far away from your Source Network. The closer the Range Extender / Bridge is to your Source Network, the better its connection will be. The Range Extender / Bridge must have a strong signal in order to repeat the signal with fast speeds and further range. Move the Range Extender / Bridge closer to your Source Network and try again.
- b. Check that your antennas are fastened tightly to the antenna connectors.
- c. You may be downloading from the Internet and not within your Source Network or Extended Network. Files transferred through the Internet are limited by your ISP speed and the data download speeds from the website that you are downloading from.
- d. Your computer may be using an older Wi-Fi adapter with lower speed limits and range capabilities (802.11b/g/n).

- e. To achieve 802.11ac Wi-Fi speeds for your extended network, it is necessary to extend an 802.11ac Wi-Fi router. Check that your source router is an 802.11ac router with speeds at or above AC1750. Extending a router with slower Wi-Fi speeds, such as 802.11n or AC750 or AC1200 will result in slower Wi-Fi speeds for your extended network.

### Troubleshooting: Wireless Issues

**I am only getting 3 or 4 wireless signal bars on my wireless computer and I am within 10 feet of the Range Extender.**

- a. Step back at least 10 feet from the Range Extender and check your signal again. The Range Extender emits high power, long range Wi-Fi signals that may confuse your wireless adapter signal reading at close range. The speed and signal are at 100%, however your readout may not be displaying the data correctly.
- b. Check that your antennas are fastened tightly to the antenna connectors.
- c. The wireless channel that your network is running on may be congested. Change the wireless channel on your Source Router and reconnect the Range Extender.

**The range from the Range Extender seems low or the speed is slow.**

- a. Check to see that your wireless output settings are at 100%. Go to the Web Menu, Wi-Fi Settings and check the Wi-Fi Output Power settings. Make sure the output power is at 100%.
- b. Your Range Extender may be installed in a poor location. Avoid setting up your Range Extender in areas with high interference, such as, near fridges, microwaves, metallic objects and low surfaces. Install the Range Extender in a higher location if possible.

- c. Check the connections of the Antennas to the Range Extender. Tighten them if necessary.
- d. Check that your antennas are fastened tightly to the antenna connectors.
- e. The wireless channel that your network is using may be congested. Change the channel for the Source router's 2.4GHz network or 5.0GHz network. The Range Extender should automatically reconnect to your networks new settings, however if it does not, simply reconfigure the Range Extender to your network.
- f. The network adapter that you are using may have poor range, older technology with slower speeds or may need a driver update.
- g. Your computer may be using an older Wi-Fi adapter with lower speed limits and range capabilities (802.11b/g/n).
- h. To achieve 802.11ac Wi-Fi speeds for your extended network, it is necessary to extend an 802.11ac Wi-Fi router. Check that your Source Router is an 802.11ac router with speeds at or above AC1750. Extending a router with slower Wi-Fi speeds, such as 802.11n or AC750 or AC1200 will result in slower Wi-Fi speeds for your extended network.

### Troubleshooting: Web Menu Feature Issues

**My Wireless Access Schedule is being erratic and not working at the correct times.**

- a. You need to adjust your System Clock from the Administration web menu page.

**Wi-Fi Protected Setup (WPS) is not working. Push button configuration does not detect the connection.**

- a. The Range Extender / Bridge supports WPS connections however some companies may use proprietary code for their own push button configurations. Try connecting using the Windows wireless utility or Mac wireless utility instead.

**I have enabled Client Isolation and/or SSID Isolation, but I can still see the computers on my network.**

- a. Client Isolation and SSID isolation restricts network access for wireless devices only. If you have devices connected to the wired ports of the Range Extender / Bridge or Router they will not be isolated.
- b. To isolate the entire network from connecting wireless devices, enable the Internet Only feature when configuring security settings for your Wi-Fi network.

**Many of the features in the Web Menu are greyed out and cannot be selected. For example, in Advanced Features most features are not selectable.**

- a. Certain features such as Port Forwarding and DMZ are only available when the Range Extender / Bridge is in Firewall Range Extender mode. Ensure that you are using the proper operational mode for the feature you wish to enable.

**I have configured MAC Address Filtering and/or RADIUS servers, but they do not work for my Extended Network.**

- a. Each Wi-Fi Network (WLAN/SSID) must also have RADIUS servers or MAC Filters selected as an Additional Authentication method in order for the feature to work. This can be done via the Web Menu by accessing the Wi-Fi Settings tab and going to Security for either the 2.4GHz or 5.0GHz networks. Select the specific SSID that you wish to configure and apply the MAC or RADIUS server setting in Additional Authentication.

**I have enabled Smart Handover, but it does not seem to be handing over the devices properly.**

- a. Set the RSSI threshold to a lower number (i.e. 0 to -50) This will allow the Range Extender / Bridge to handover the device when the signal strength between the device and the Range Extender / Bridge is still moderately strong.

- b. Change the device to a device that supports the Smart Handover feature. Some older Wi-Fi adapters do not support the Smart Handover feature.

## **WARRANTY & REGULATORY INFORMATION**

### **The Amped Wireless (A division of Newo Corporation, Inc.) Limited Warranty**

**Warranty Period:** The Amped Wireless Limited Warranty is for one (1) year from the date of purchase for new products. Refurbished products carry the Limited Warranty for thirty (30) days after the date of purchase.

**Guarantee:** Amped Wireless warrants to the original purchaser that the hardware of this Amped Wireless product shall be free of defects in design, assembly, material, or workmanship.

**Conditions:** The Amped Wireless Limited Warranty is for repair or replacement only at the sole discretion of Amped Wireless. Amped Wireless does not issue any refunds for purchased product. In the event that Amped Wireless is unable to repair or replace a product (i.e. discontinued product), Amped Wireless will offer a credit toward the purchase of a similar product of equal or lesser value direct from Amped Wireless. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. Amped Wireless reserves the right to discontinue any of its products without notice, and disclaims any limited warranty to repair or replace any such discontinued product. Amped Wireless reserves the right to revise or make changes to this product, its documentation, packaging, specifications, hardware, and software without notice. If any portion of the Amped Wireless Limited Warranty is found to be unenforceable, its remaining provisions shall remain in effect. All costs of shipping the product to Amped Wireless shall be borne solely by the purchaser.

**Limitations:** IN NO EVENT SHALL AMPED WIRELESS' (NEWO CORPORATION'S) LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, ACCESSORIES OR ITS DOCUMENTATION. The Amped Wireless Limited Warranty does not apply if: (a) the product assembly has been opened or damaged, (b) the product or its software or firmware has been altered or modified, (c) the product has not been used and installed in accordance to Amped Wireless' instructions, (d) the product has been subjected to misuse, or negligence. Amped Wireless does not guarantee the continued availability of a third party's service for which this product's use or operation may require. The Amped Wireless Limited Warranty does not protect against acts of God, vandalism, theft, normal wear and tear, obsolescence and environmental damages such as, but not limited to, weather and electrical disturbances. The Amped Wireless Limited Warranty is the sole warranty for this product. There are no other warranties, expressed or, except required by law, implied, including the implied warranty or condition of quality, performance merchantability, or fitness for any particular purpose.

**How to Claim Warranty:** In the event that you have a problem with this product, please go to [www.ampedwireless.com/support](http://www.ampedwireless.com/support) to find help on solving your problem. In the event that you cannot and need to file a warranty claim, please call Amped Wireless' Elite Support or visit <http://www.ampedwireless.com/support/center.html#rma> to obtain a Support Ticket Number (obtained from Technical Support Reps), fill out a Return Authorization (RMA) form and obtain a Return Authorization (RMA) number. A dated proof of original purchase and the RMA number is required to process warranty claims. You are responsible for properly packaging and shipping the product at your cost and risk to Amped Wireless. The bearer of cost related to shipping repaired or replaced product back to the purchaser will be at the sole

discretion of Amped Wireless and determined based on the details of each RMA case. Customers outside of the United States of America are responsible for all shipping and handling costs including custom duties, taxes and all other related charges.

**Technical Support:** The Amped Wireless Limited Warranty is not related to the terms, conditions and policies of Amped Wireless Elite Support offerings. For questions regarding support, please contact [techsupport@ampedwireless.com](mailto:techsupport@ampedwireless.com)

## Regulatory Information

**FCC Statement and Declaration:** Amped Wireless declares that this device complies with Part 15 of the FCC Rules and Regulations. Operation of this device is subject to the following two (2) conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

**FCC Notice:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.

- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**FCC Caution and Safety Notices:** Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. Avoid use of this product near water or during an electrical storm as there may be a remote risk of electrical shock from lightning. This product may contain lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling. This device must always be used with a Listed Computer or device.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible. This device is restricted to indoor use when operated in the 5.15 to 5.25 GHz frequency range.

FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

**FCC Radiation Exposure Statement:** This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

**Industry Canada Statement:** This Class B digital apparatus complies with RSS-210 and ICES-003 of the Industry Canada Rules. Operation of this device is subject to the following two (2) conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

**Radiation Exposure Statement:** This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

The transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

**Déclaration d'Industrie Canada :** Cet appareil numérique de classe B est conforme aux réglementations RSS-210 et ICES-003 d'Industrie Canada. Le fonctionnement de cet appareil est sujet aux deux conditions suivantes:

- (1) Cet appareil ne peut pas causer de brouillage préjudiciable
- (2) Cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant provoquer un dysfonctionnement.

**Déclaration d'exposition à la radiation :** Cet équipement respecte les limites d'exposition aux rayonnements IC définies pour un environnement non contrôlé. Cet équipement doit être installé et mis en marche à une distance minimale de 20 cm qui sépare l'élément rayonnant de votre corps.

L'émetteur ne doit ni être utilisé avec une autre antenne ou un autre émetteur ni se trouver à leur proximité.

## ***LEGAL NOTICES & DISCLAIMERS***

### **Copyright Information and Trademark Usage Guidelines**

© 2015 Amped Wireless / Newo Corporation. All rights reserved. Amped Wireless, Newo Corporation, and the Amped Wireless logo are registered trademarks or trademarks of Newo Corporation. All non-Amped Wireless trademarks, logos, brands and products are trademarks or registered trademarks of their respective owners. Amped Wireless does not claim any relation. Mention of non-Amped Wireless products and brands are for information purposes only and does not constitute an endorsement or affiliation.

Amped Wireless authorizes you to copy materials published by Amped Wireless solely for non-commercial use within your organization in support of Amped Wireless products. No other use of this information is authorized. Any copy of these materials which you make shall retain all copyright and other proprietary notices in the same form and manner as on the original. Except as specified above, nothing contained herein shall be construed as conferring by implication, estoppel or otherwise any license or right under any patent, trademark or copyright of Amped Wireless or any third party.

All contents of this product, including Software, are protected by copyright, except as permitted herein. No portion of the information may be reproduced without prior written permission from Amped Wireless. The distribution, modification, publication and transmission of any content of this product for public or commercial purposes is strictly prohibited.

The Amped Wireless logo requires permission for use. For use of the Amped Wireless logo, please email [legal@ampedwireless.com](mailto:legal@ampedwireless.com). Use of Amped Wireless' trademarks requires the use of the proper trademark symbol in all usage cases.

The guidelines for trademark usage apply to all Amped Wireless customers, employees, vendors, consultants, licensees and any other third party.

### **Disclaimers**

Amped Wireless makes all attempts in providing accurate information on all media. However, Amped Wireless makes no warranty as to the accuracy of the information, including representations and warranties about the accuracy of product specifications, marketing material, product availability, new product launch dates and all other content herein. Amped Wireless reserves the right to update and change information without prior notice. All information provided is provided "AS IS" with all faults without warranty of any kind. Either expressed or implied. Amped Wireless and its suppliers disclaim all warranties, expressed or implied including, without limitation. Amped Wireless and its suppliers shall not be liable for any indirect, special, consequential, or incidental damages including, without limitation, lost profits or revenues, cost of replacement goods, loss or damage to data arising out of the use or inability to use any Amped Wireless product, damages resulting from use of or reliance on information present, even with prior notice to Amped Wireless.

All non-Amped Wireless trademarks, logos, brands and products are trademarks or registered trademarks of their respective owners. Amped Wireless does not claim any relation. Mention of non-Amped Wireless products and brands are for information purposes only and does not constitute an endorsement or affiliation.

Product wireless range specifications are based on performance test results. Actual performance may vary due to differences in operating environments, building materials and wireless obstructions. Performance may increase or decrease over the stated specification. Wireless coverage claims are used only as a reference and are not guaranteed as each wireless network is uniquely different.

Maximum wireless signal rates are derived from IEEE 802.11 standard specifications. Actual data throughput may vary as a result of network conditions and environmental factors.

Wi-Fi Range Extenders may not work with non-standard Wi-Fi routers or routers with altered firmware or proprietary firmware, such as those from third party sources or some Internet service providers. May not work with routers that do not comply with IEEE or Wi-Fi standards.

### Software Licenses / Disclaimers

This product contains Software (including firmware), licensed to you, the purchaser, by Amped Wireless. This also includes Software downloaded from an authorized website, such as [www.ampedwireless.com](http://www.ampedwireless.com) or from an authorized application market such as Google Play or Apple's App Store.

This license allows you to operate the Software in the manner described in the user's manual for the purchased product. You can make as many copies of the Software as needed for your personal use. Modifying or tampering of the Software, including but not limited to any Open Source Software, is solely at your own risk. Amped Wireless is not responsible for any such modification or tampering. Amped Wireless will not support or warrant any product in which you have or have attempted to modify the Software provided by Amped Wireless. You may not lease, sublicense, resell, redistribute or otherwise transfer the Software without written consent from Amped Wireless.

The Software is provided to you "as is" with all faults and without warranties of any kind. In particular, Amped Wireless does not guarantee that the Software will be error-free or that the Software will be free from system threats or attacks from viruses. Amped Wireless does not warrant that the Software will meet your expectations or that the software will be suitable for your particular situation. Amped Wireless warrants that any media (such as an included CD) on which the Software is provided to be free from defects. If you have an eligible warranty claim for defective media, Amped Wireless will replace the Software media.

IT IS YOUR RESPONSIBILITY TO BACK UP YOUR SYSTEM INCLUDING, WITHOUT LIMITATION, ANY DATA THAT YOU MAY USE OR POSSESS IN CONNECTION WITH THE PRODUCT. ANY MATERIAL, INFORMATION OR DATA DOWNLOADED OR OTHERWISE OBTAINED IS ACCESSED AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR PRODUCT, OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF SUCH MATERIAL, INFORMATION OR DATA.

AMPED WIRELESS IS NOT RESPONSIBLE FOR ANY DAMAGE TO THE PURCHASER'S COMPUTER SYSTEM OR DATA.

All title and copyrights in and to the Software and any copies thereof are owned by Amped Wireless or its partners/suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This license grants you no rights to use such content. You may not delete any copyright, trademark or other proprietary notices from the Software or documentation.

**Dispute Resolution / Arbitration**

This section describes how you agree to resolve any disputes with Amped Wireless regarding these Terms of Use or your purchase of any product from Amped Wireless and your use of that product. You and Amped Wireless agree to the following resolution process.

To begin with, you agree that any claim that you might have against us regarding these Terms of Use or your purchase of any Amped Wireless product or use of that product must be resolved through binding arbitration before the American Arbitration Association using its Commercial Arbitration Rules. The arbitrator shall have exclusive authority to the extent permitted by law to resolve all disputes arising out of or relating to the interpretation, applicability, enforceability, or formation of our agreement, including, but not limited to, any claim that all or part of this agreement is void or voidable. The arbitrator shall also have exclusive authority to the extent permitted by law to decide the arbitrability of any claim or dispute between you and Amped Wireless.

Because we prefer to resolve our issues with you directly, you agree to arbitrate with Amped Wireless only in your individual capacity, not as a representative or member of a class. As such, your claims may not be joined with any other claims and there shall be no authority for any dispute to be arbitrated on a class-action basis or brought by a purported class representative.

It is important that you understand that the arbitrator's decision will be binding and may be entered as a judgment in any court of competent jurisdiction. If the arbitrator rules against Amped Wireless, in addition to accepting whatever responsibility is ordered by the arbitrator, we will reimburse your reasonable attorneys' fees and costs.

It's important to us that we address any issues you might have promptly. To help us do that, you agree to begin any arbitration within one year after your claim arose; otherwise, your claim is waived.

Unless you and Amped Wireless agree otherwise, any arbitration hearings will take place in the county where you reside. If your claim is for \$10,000 or less, you may choose whether the arbitration will be conducted solely on the basis of documents submitted to the arbitrator, through a telephonic hearing, or by an in-person hearing as established by the AAA Rules. If your claim exceeds \$10,000, the right to a hearing will be determined by the AAA Rules.

If your claim against Amped Wireless is for less than \$10,000, Amped Wireless will pay all arbitration fees. If your claim against Amped Wireless is for \$10,000 or more, you are responsible for paying your own portion of the fees set forth in the AAA's fee schedule for consumer disputes, and Amped Wireless will pay all remaining arbitration fees. If you believe you cannot afford the AAA's fee, you may apply to the AAA for a waiver.

As an exception to this arbitration agreement, Amped Wireless is happy to give you the right to pursue in small claims court any claim that is within that court's jurisdiction as long as you proceed only on an individual basis.

We would hope that our customer service agents could resolve any disputes you have with us without resorting to arbitration. Before initiating any arbitration proceeding, you agree to first discuss the matter informally with Amped Wireless for at least 30 days. To do that, please send your full name and contact information, your concern and your proposed solution by mail to us at: 13089 Peyton Dr. #C307, Chino Hills, CA 91709; Attn: Legal Department.

This Agreement and the rights of the parties hereunder shall be governed by and construed in accordance with the laws of the State of California, exclusive of conflict or choice of law rules.

The parties acknowledge that this Agreement evidences a transaction involving interstate commerce. Notwithstanding the provision in the preceding paragraph with respect to applicable substantive law, any arbitration conducted pursuant to the terms of this Agreement shall be governed by the Federal Arbitration Act (9 U.S.C., Secs. 1-16).

**Mailing Address Only**

Amped Wireless 13089 Peyton Dr. #C307 Chino Hills, CA 91709

Email: [legal@ampedwireless.com](mailto:legal@ampedwireless.com)



tech support 888-573-8820  
e-mail [techsupport@ampedwireless.com](mailto:techsupport@ampedwireless.com)  
web [www.ampedwireless.com](http://www.ampedwireless.com)

Amped Wireless  
A Division of Newo Corporation  
Copyright © 2015 Amped Wireless / Newo Corporation. All rights reserved.  
Amped Wireless, Newo Corporation, and the Amped Wireless Logo are registered trademarks or trademarks of Newo Corporation.