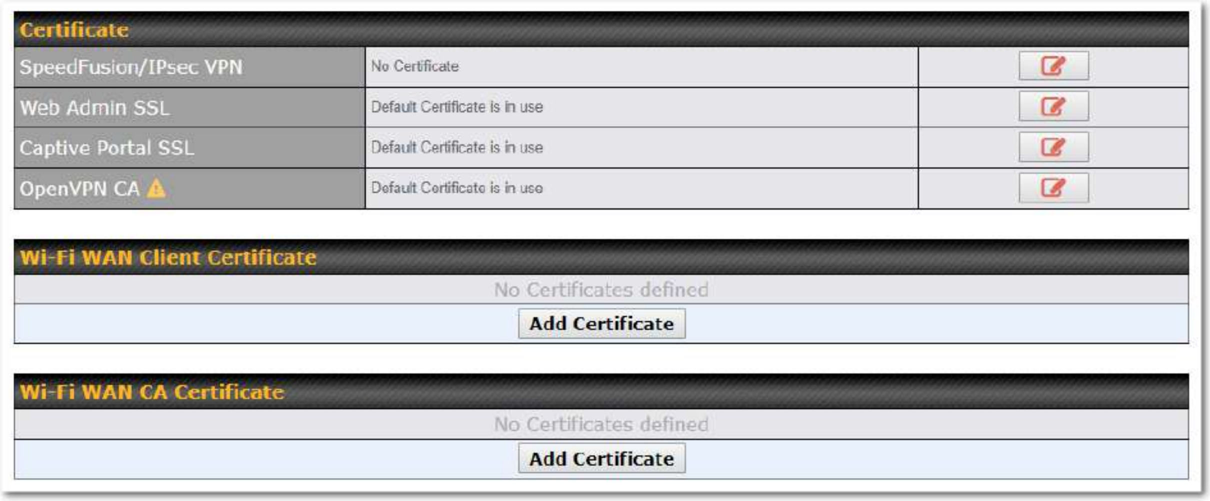
24.3 Certificate Manager



Certificate		
SpeedFusion/IPsec VPN	No Certificate	✎
Web Admin SSL	Default Certificate is in use	✎
Captive Portal SSL	Default Certificate is in use	✎
OpenVPN CA ⚠	Default Certificate is in use	✎

Wi-Fi WAN Client Certificate
No Certificates defined
Add Certificate

Wi-Fi WAN CA Certificate
No Certificates defined
Add Certificate

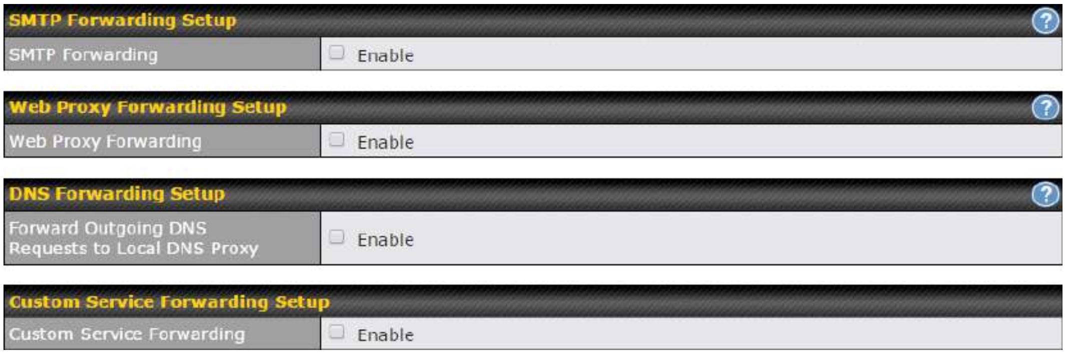
This section allows for certificates to be assigned to the local VPN, Web Admin SSL, Captive Portal SSL, OpenVPN CA, Wi-Fi WAN Client certificate and Wi-Fi WAN CA Certificate.

The following knowledge base article describes how to create self-signed certificates and import it to a Peplink Product.

https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/

24.4 Service Forwarding

Service forwarding settings are located at **Advanced > Misc. Settings > Service Forwarding**.



SMTP Forwarding Setup

SMTP Forwarding	□ Enable

Web Proxy Forwarding Setup

Web Proxy Forwarding	□ Enable

DNS Forwarding Setup

Forward Outgoing DNS Requests to Local DNS Proxy	□ Enable

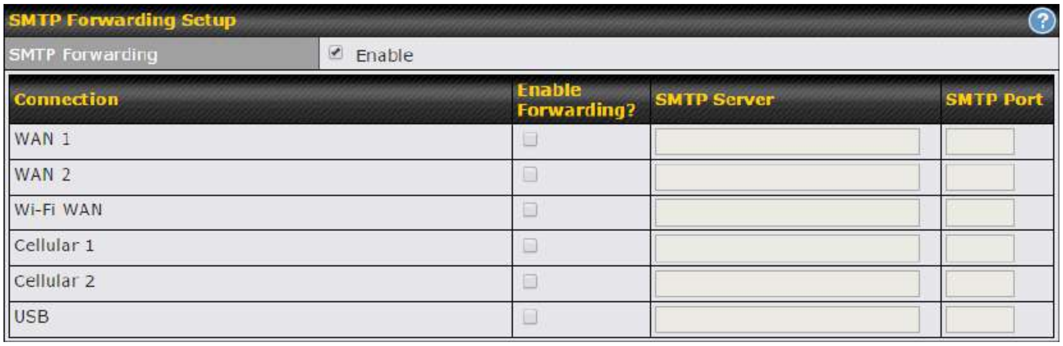
Custom Service Forwarding Setup

Custom Service Forwarding	□ Enable

Service Forwarding	
SMTP Forwarding	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting **Enable**.
Web Proxy Forwarding	When this option is enabled, all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings** will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting **Enable**.
DNS Forwarding	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down.
Custom Service Forwarding	When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number.

24.4.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP connections are blocked except those connecting to the ISP's. Pepwave routers support intercepting and redirecting all outgoing SMTP connections (destined for TCP port 25) via a WAN connection to the WAN's corresponding SMTP server.



SMTP Forwarding Setup

SMTP Forwarding	☑ Enable

Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	□		
WAN 2	□		
Wi-Fi WAN	□		
Cellular 1	□		
Cellular 2	□		
USB	□		

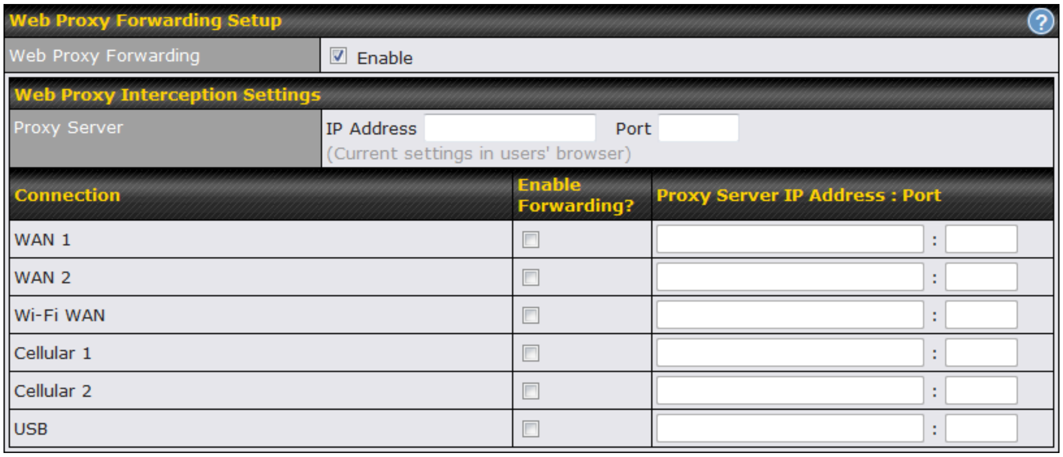
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

The Pepwave router will intercept SMTP connections. Choose a WAN port according to the outbound policy, and then forward the connection to the SMTP server if the chosen WAN has enabled forwarding. If the forwarding is disabled for a WAN connection, SMTP connections for the WAN will be simply be forwarded to the connection's original destination.

Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 14.2**).

24.4.2 Web Proxy Forwarding



Web Proxy Forwarding Setup

Web Proxy Forwarding	☑ Enable

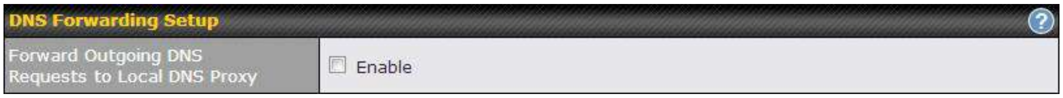
Web Proxy Interception Settings

Proxy Server	IP Address Port (Current settings in users' browser)

Connection	Enable Forwarding?	Proxy Server IP Address : Port
WAN 1	□	:
WAN 2	□	:
Wi-Fi WAN	□	:
Cellular 1	□	:
Cellular 2	□	:
USB	□	:

When this feature is enabled, the Pepwave router will intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**, choose a WAN connection with reference to the outbound policy, and then forward them to the specified web proxy server and port number. Redirected server settings for each WAN can be set here. If forwarding is disabled for a WAN, web proxy connections for the WAN will be simply forwarded to the connection's original destination.

24.4.3 DNS Forwarding

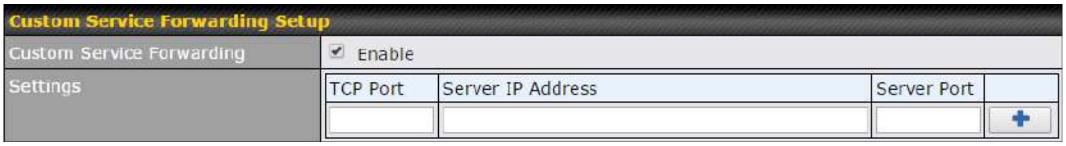


DNS Forwarding Setup

Forward Outgoing DNS Requests to Local DNS Proxy	□ Enable

When DNS forwarding is enabled, all clients’ outgoing DNS requests will also be intercepted and forwarded to the built-in DNS proxy server.

24.4.4 Custom Service Forwarding



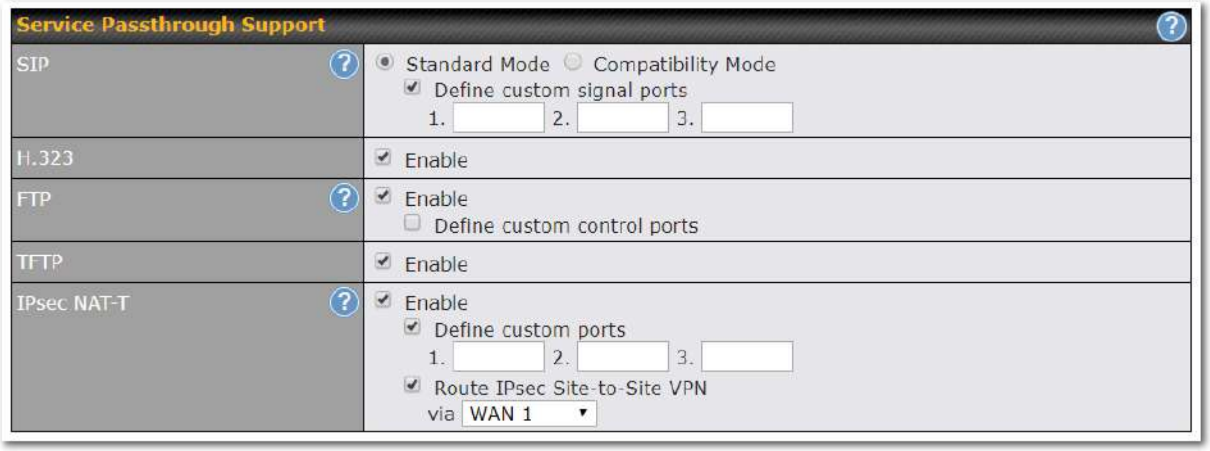
Custom Service Forwarding Setup

Custom Service Forwarding	☑ Enable			
Settings	TCP Port	Server IP Address	Server Port	
				+

After clicking the **enable** checkbox, enter your TCP port for traffic heading to the router, and then specify the IP Address and Port of the server you wish to forward to the service to.

24.5 Service Passthrough

Service passthrough settings can be found at **Advanced > Misc. Settings > Service Passthrough**.



Service Passthrough Support	
SIP	● Standard Mode ○ Compatibility Mode ☑ Define custom signal ports 1. 2. 3.
H.323	☑ Enable
FTP	☑ Enable □ Define custom control ports
TFTP	☑ Enable
IPsec NAT-T	☑ Enable ☑ Define custom ports 1. 2. 3. ☑ Route IPsec Site-to-Site VPN via WAN 1

Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.

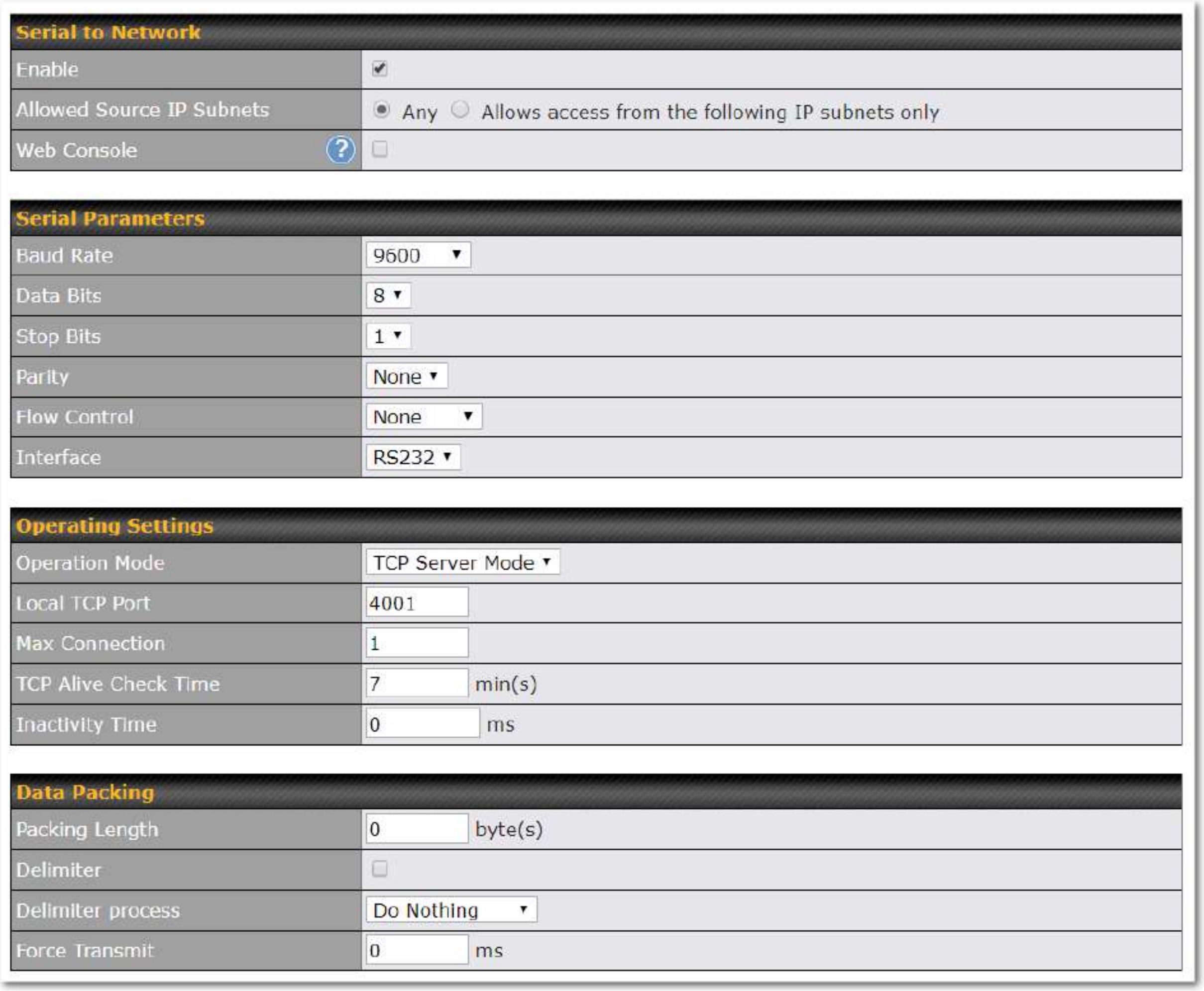
Service Passthrough Support	
SIP	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Pepwave router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled, and there are two modes for selection: **Standard Mode** and **Compatibility Mode**. If your SIP server's signal port number is non-standard, you can check the box **Define custom signal ports** and input the port numbers to the text boxes.
H.323	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.
FTP	FTP sessions consist of two TCP connections; one for control and one for data. In a multi-WAN situation, they must be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Pepwave router monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check **Define custom control ports** and enter the port numbers in the text boxes.
TFTP	The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select **Enable** if you want to enable TFTP passthrough support.

IPsec NAT-T	This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default. You may add more custom data ports that your IPsec system uses by checking **Define custom ports**. If the VPN contains IPsec site-to-site VPN traffic, check **Route IPsec Site-to-Site VPN** and choose the WAN connection to route the traffic to.

24.6 UART

Selected Pepwave MAX routers feature a RS-232 serial interface on the built-in terminal block. The RS-232 serial interface can be used to connect to a serial device and make it accessible over an TCP/IP network.

The serial interface can be enabled and parameters can be set on the web admin page under **Advanced > UART**. Make sure they match the serial device you are connecting to.



Serial to Network	
Enable	☑
Allowed Source IP Subnets	● Any ○ Allows access from the following IP subnets only
Web Console	☐

Serial Parameters	
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Interface	RS232

Operating Settings	
Operation Mode	TCP Server Mode
Local TCP Port	4001
Max Connection	1
TCP Alive Check Time	7 min(s)
Inactivity Time	0 ms

Data Packing	
Packing Length	0 byte(s)
Delimiter	☐
Delimiter process	Do Nothing
Force Transmit	0 ms

There are 4 pins i.e. TX, RX, RTS, CTS on the terminal block for serial connection and they correspond to the pins in a DB-9 connector as follows:

DB-9	**Pepwave MAX Terminal Block**
Pin 1	–
Pin 2	Rx (rated -+25V)
Pin 3	Tx (rated -+12V)
Pin 4	–
Pin 5	–
Pin 6	–
Pin 7	RTS
Pin 8	CTS
Pin 9	–

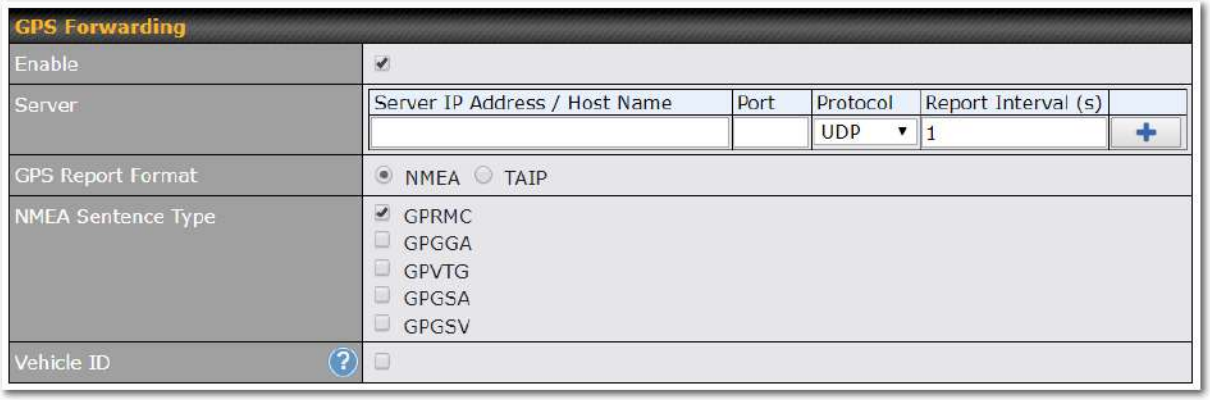
The RS232 serial interface is not an isolated RS232. External galvanic isolation may be added if required.

Be sure to check whether your serial cable is a null modem cable, commonly known as crossover cable, or a straight through cable. If in doubt, swap Rx and Tx, and RTS and CTS, at the other end and give it another go.

Once connected, your serial device should be accessible on your Pepwave MAX router LAN IP address at the specified TCP port.

24.7 GPS Forwarding

Using the GPS forwarding feature, some Pepwave routers can automatically send GPS reports to a specified server. To set up GPS forwarding, navigate to **Advanced > Misc. Settings > GPS Forwarding**.



GPS Forwarding

Enable	☑
Server	Server IP Address / Host Name: (blank) Port: (blank) Protocol: UDP ▾ Report Interval (s): 1 +
GPS Report Format	● NMEA ○ TAIP
NMEA Sentence Type	☑ GPRMC □ GPGGA □ GPVTG □ GPGSA □ GPGSV
Vehicle ID ?	□

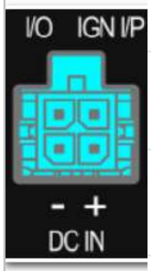
GPS Forwarding	
Enable	Check this box to turn on GPS forwarding.
Server	Enter the name/IP address of the server that will receive GPS data. Also specify a port number, protocol (**UDP** or **TCP**), and a report interval of between 1 and 10 seconds. Click + to save these settings.
GPS Report Format	Choose from NMEA or TAIP format for sending GPS reports.
NMEA Sentence Type	If you've chosen to send GPS reports in NMEA format, select one or more sentence types for sending the data (**GPRMC**, **GPGGA**, **GPVTG**, **GPGSA**, and **GPGSV**).
Vehicle ID	The vehicle ID will be appended in the last field of the NMEA sentence. Note that the NMEA sentence will become customized and non-standard.
TAIP Sentence Type/TAIP ID (optional)	If you've chosen to send GPS reports in TAIP format, select one or more sentence types for sending the data (**PV—Position / Velocity Solution** and **CP—Compact Velocity Solution**). You can also optionally include an ID number in the **TAIP ID** field.

24.8 Ignition Sensing

Ignition Sensing detects the ignition signal status of a vehicle it is installed in.

This feature allows the cellular router to start up or shut down when the engine of that vehicle is started or turned off.
The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

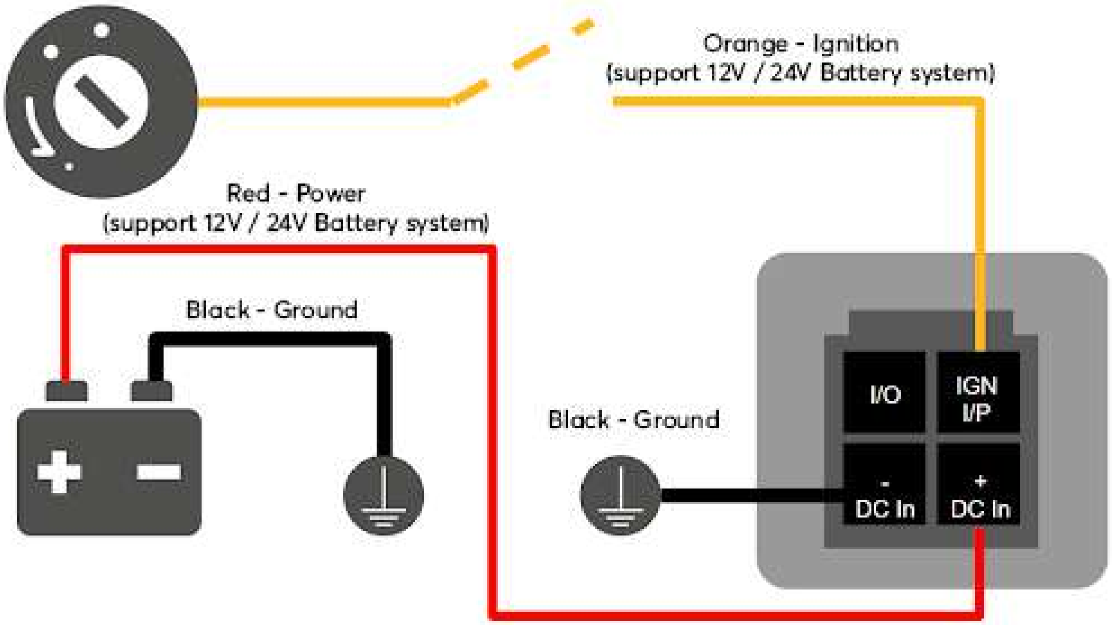
Ignition Sensing installation

	Function		Colour Wire
	I/O	optional *	Brown
	**IGN I/P**	connected to positive feed on the ignition **	Orange
	DC IN -	connected to permanent negative feed (ground)	Black
	DC IN +	connected to permanent positive feed (power)	Red

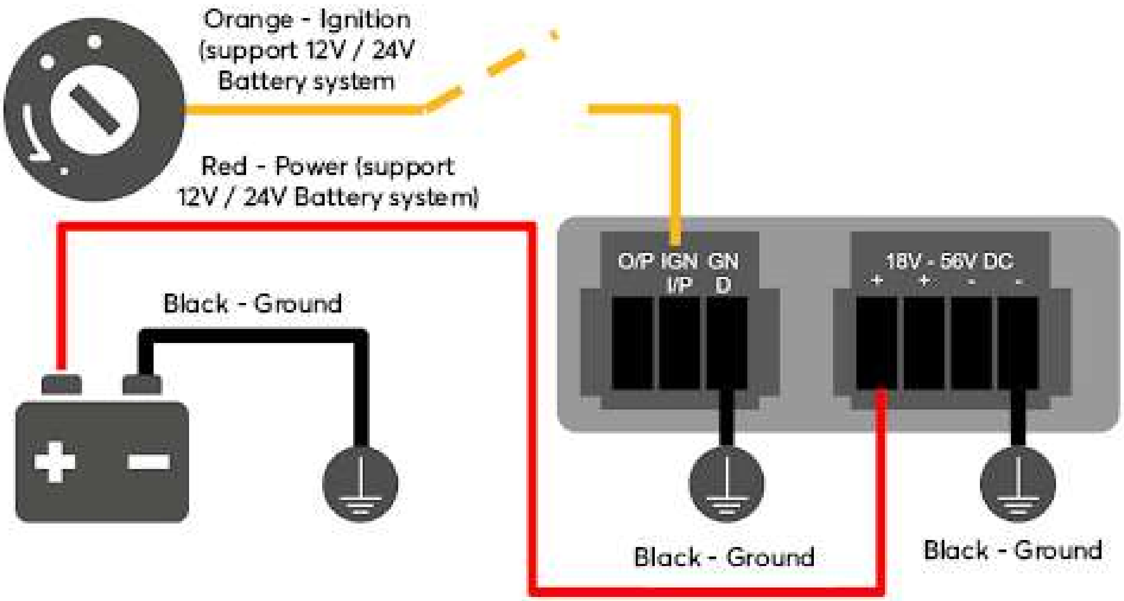
* Currently not functional; will be used for additional features in future firmware.

** Connecting IGN I/P is optional and is needed only if the Ignition Sensing feature is configured.

Connectivity diagram for devices with 4-pin connector



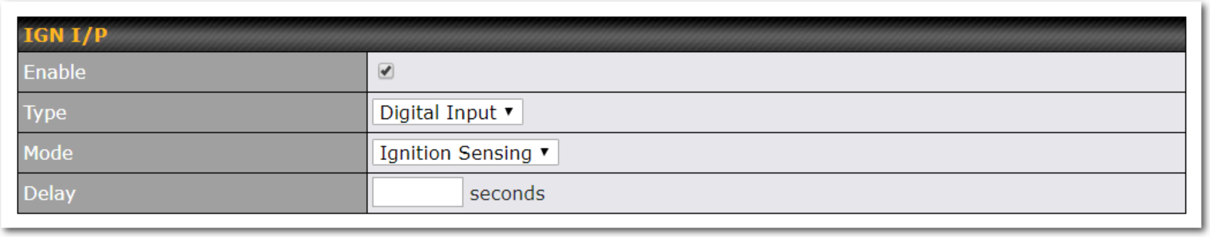
Connectivity diagram for devices with terminal block connection



GPIO Menu

Note: This feature is applicable for certain models that come with a GPIO interface.

Ignition Sensing options can be found in **Advanced > Misc. Settings > GPIO.**
The configurable option for Ignition Input is **Delay;** the time in seconds that the router stays powered on after the ignition is turned off.

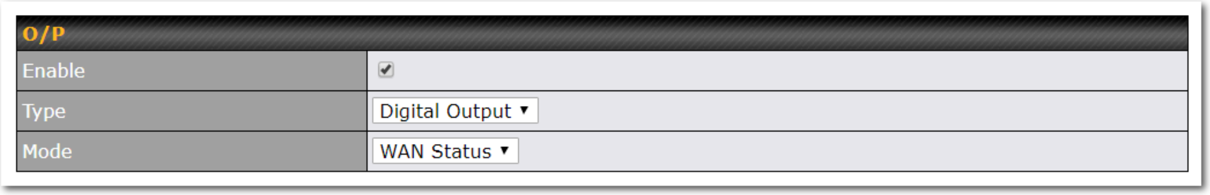


IGN I/P	
Enable	☑
Type	Digital Input ▾
Mode	Ignition Sensing ▾
Delay	____ seconds

The O/P (connected to the I/O pin on a 4 pin connector) can be configured as a digital input, a digital output, or an analog input.

Digital Input - the connection supports input sensing; it reads the external input and determines if the settings should be 'High' (on) or 'Low' (off).

Digital Output - when there is a healthy WAN connection, the output pin is marked as 'High' (on). Otherwise, it will be marked as 'Low' (off).



O/P	
Enable	☑
Type	Digital Output ▾
Mode	WAN Status ▾

Note: The Digital Output state (on/off) upon rebooting the device may vary depending on the model, eg. MAX BR1 MK2 = Persistent; MAX Transit Mini with ContentHub = Reset to default, etc.

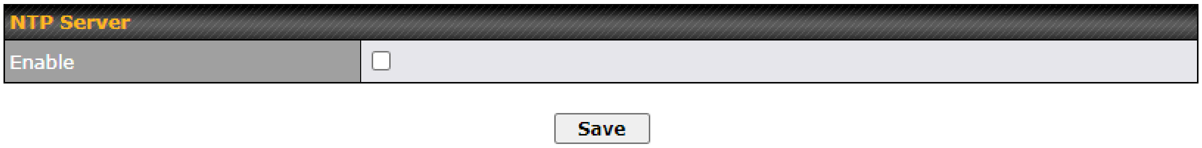
Analog Input - to be confirmed. In most cases, it should read the external input and determine the voltage level.

24.9 NTP Server

Pepwave routers can now serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time.

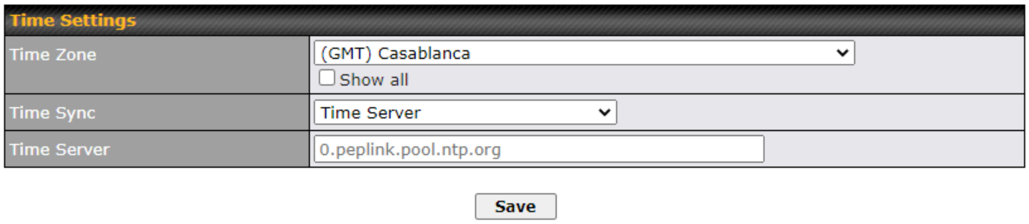
Compatible with: BR1 ENT, BR1 Pro CAT-20/5G, 700 HW3, HD2/4, Transit

NTP Server setting can be found via: **Advanced > Misc. Settings > NTP Server**



NTP Server	
Enable	□

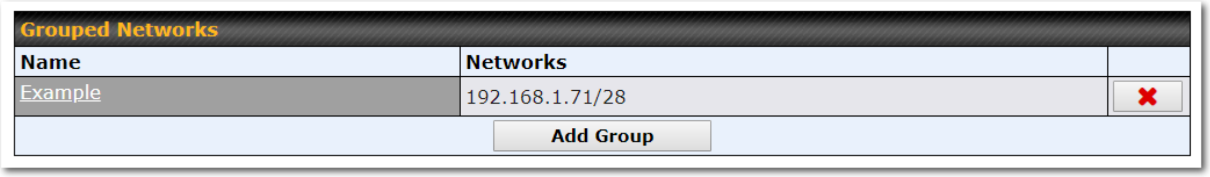
Time Settings can be found at **System > Time > Time Settings**



Time Settings	
Time Zone	(GMT) Casablanca □ Show all
Time Sync	Time Server
Time Server	0.peplink.pool.ntp.org

24.10 Grouped Networks

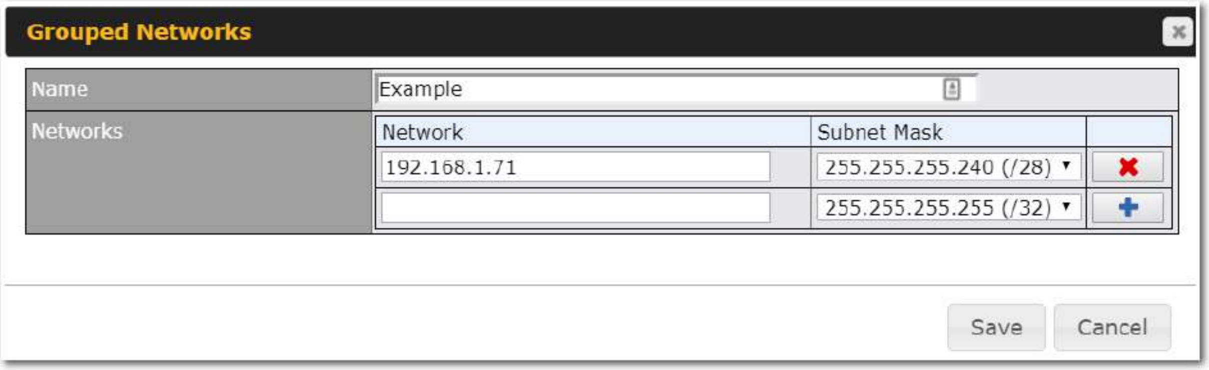
Advanced > Misc. Settings > Grouped Networks allows to configure destination networks in grouped format.



Grouped Networks

Name	Networks	
Example	192.168.1.71/28	✖

Select Add group to create a new group with single IPaddresses or subnets from different VLANs.



Grouped Networks

Name: Example

Networks:

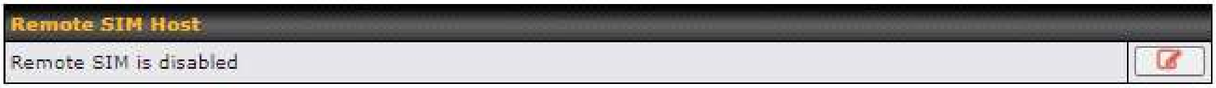
Network	Subnet Mask	
192.168.1.71	255.255.255.240 (/28)	✖
	255.255.255.255 (/32)	✚

The created network groups can be used in outbound policies, firewall rules.

24.11 Remote SIM Management

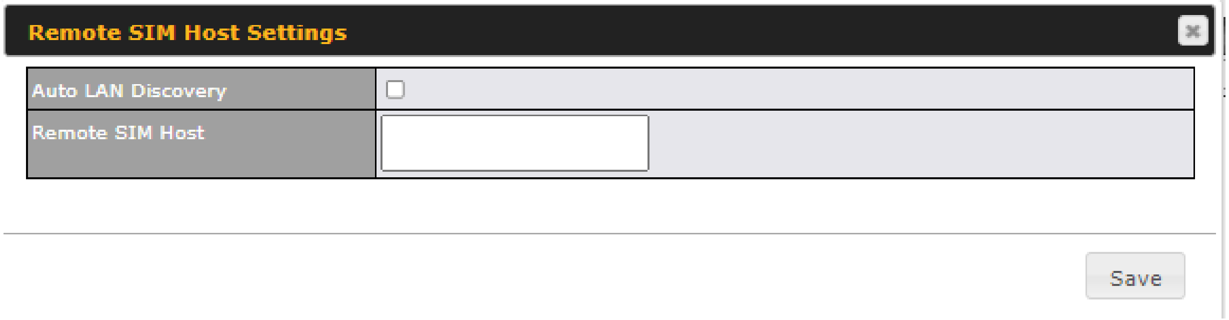
The Remote SIM management is accessible via **Advanced > Misc Settings > Remote SIM Management**. By default, this feature is disabled.

Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: https://www.peplink.com/products/sim-injector/ or Appendix B for more details on FusionSIM Manual.



Remote SIM Host	
Remote SIM is disabled	✎

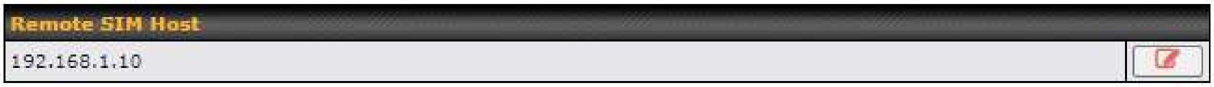
Remote SIM Host Settings



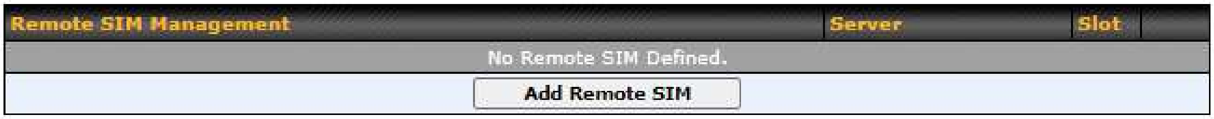
Remote SIM Host Settings ✖

Auto LAN Discovery	☐
Remote SIM Host	

Remote SIM Host Settings	
Active LAN Discovery	Check this box to enable Auto LAN discovery of the remote SIM server..
Remote SIM Host	Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the "**Auto LAN Discovery**" box above.

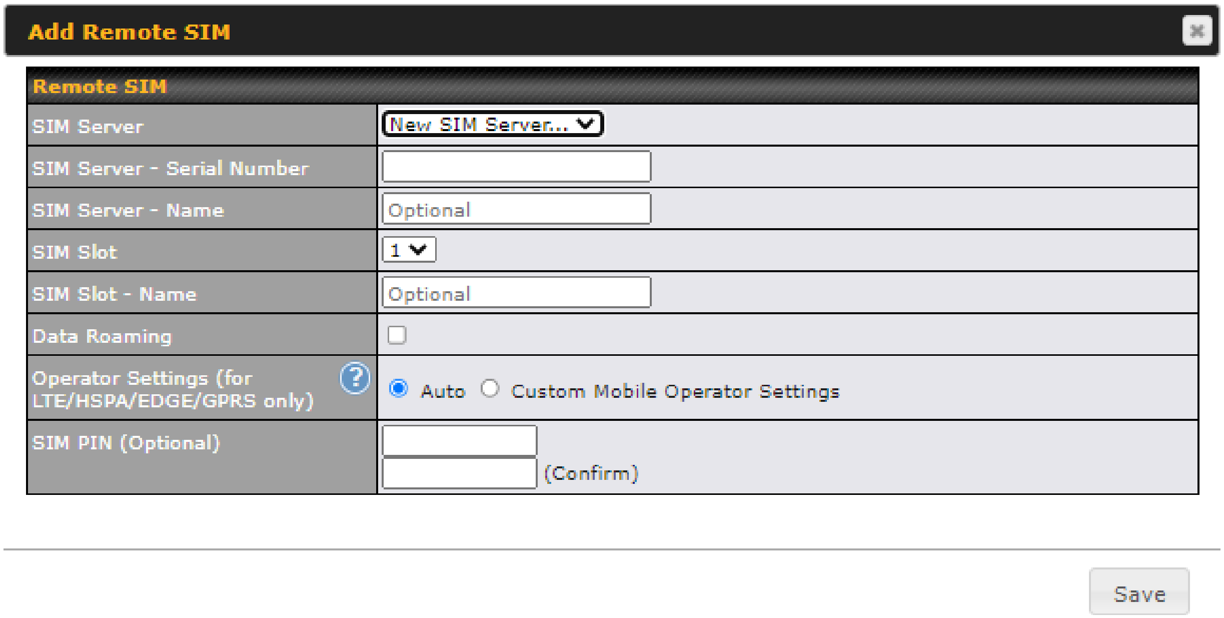


Remote SIM Host	
192.168.1.10	✎



Remote SIM Management	Server	Slot
No Remote SIM Defined.		

You may define the Remote SIM information by clicking the "**Add Remote SIM**". Here, you can enable **Data Roaming** and **custom APN** for your SIM cards.



Add Remote SIM

Remote SIM	
SIM Server	New SIM Server... ▾
SIM Server - Serial Number	
SIM Server - Name	Optional
SIM Slot	1 ▾
SIM Slot - Name	Optional
Data Roaming	□
Operator Settings (for LTE/HSPA/EDGE/GPRS only) ?	● Auto ○ Custom Mobile Operator Settings
SIM PIN (Optional)	 (Confirm)

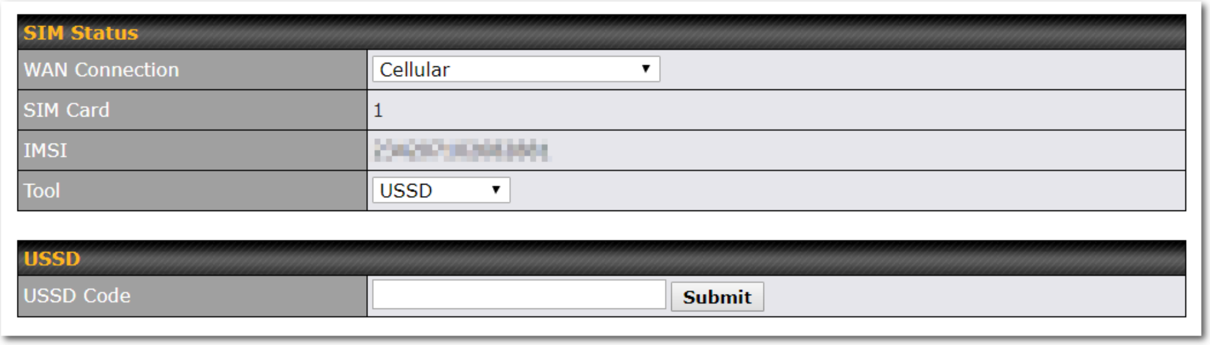
Add Remote SIM Settings	
SIM Server	Add a new SIM Server
SIM Server - Serial Number	Enter the serial number of SIM Server
SIM Server - Name	This optional field allows you define a name for the SIM Server
SIM Slot	Click the drop-down menu and choose which SIM slot you want to connect.
SIM Slot - Name	This optional field allows you define a name for the SIM slot.
Data Roaming	Enables data roaming on this particular SIM card.
Operator Settings (for LTE//HSPA/EDGE/GPRS Only)	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making a connection, you may select **Custom** to enter your carrier's APN, Username and Password settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto.

24.12 SIM Toolkit

The SIM Toolkit, accessible via **Advanced > Misc Settings > SIM Toolkit**, supports two functionalities, USSD and SMS.

USSD

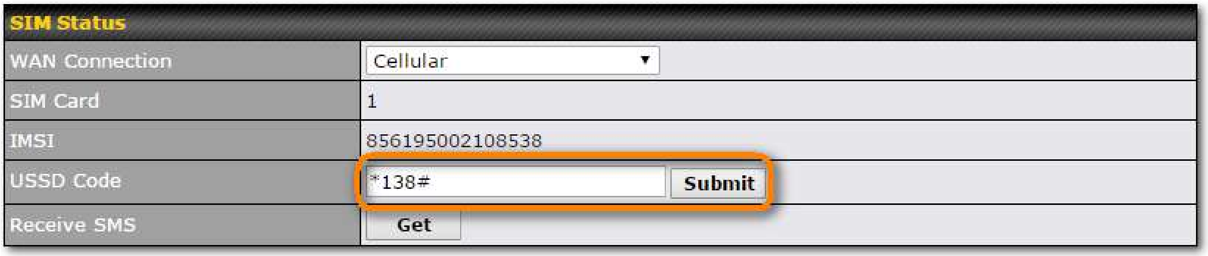
Unstructured Supplementary Service Data (USSD) is a protocol used by mobile phones to communicate with their service provider's computers. One of the most common uses is to query the available balance.



SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	[redacted]
Tool	USSD ▾

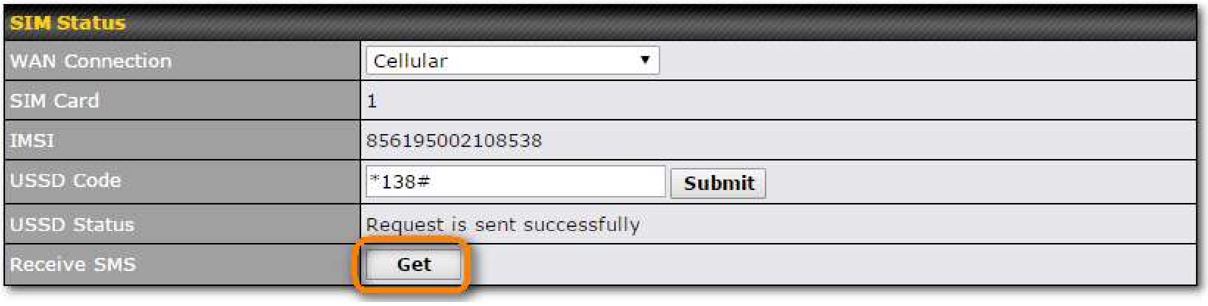
USSD	
USSD Code	Submit

Enter your USSD code under the **USSD Code** text field and click **Submit**.



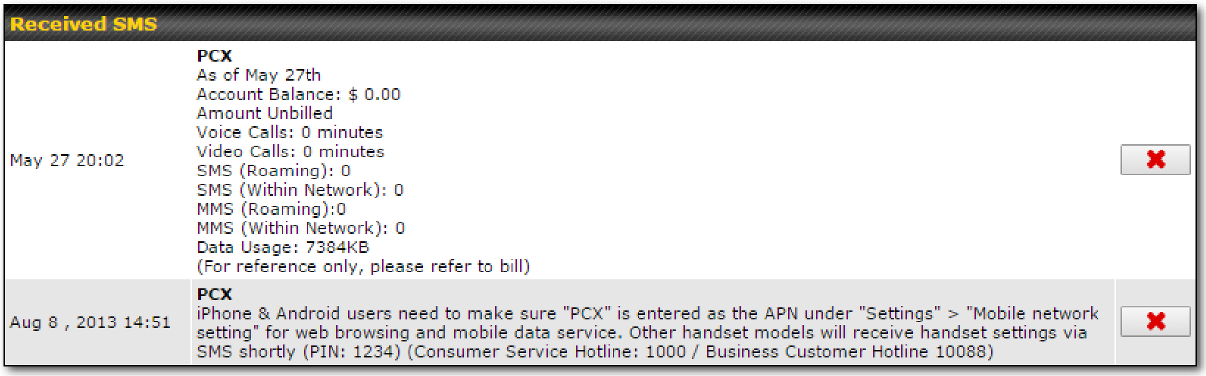
SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
Receive SMS	Get

You will receive a confirmation. To check the SMS response, click **Get**.



SIM Status	
WAN Connection	Cellular ▾
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
USSD Status	Request is sent successfully
Receive SMS	Get

After a few minutes you will receive a response to your USSD code

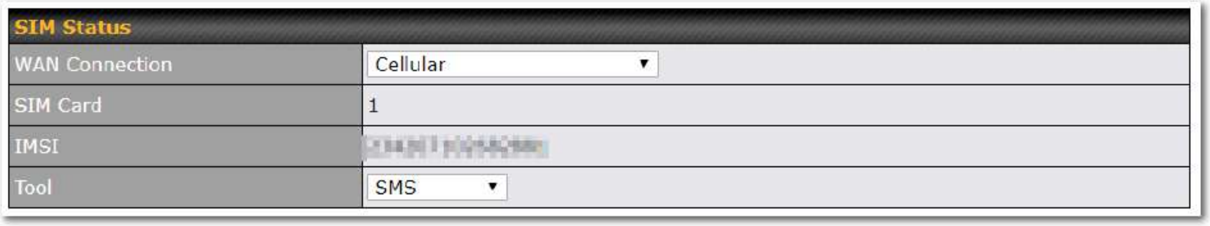


Received SMS

May 27 20:02	**PCX** As of May 27th Account Balance: $ 0.00 Amount Unbilled Voice Calls: 0 minutes Video Calls: 0 minutes SMS (Roaming): 0 SMS (Within Network): 0 MMS (Roaming):0 MMS (Within Network): 0 Data Usage: 7384KB (For reference only, please refer to bill)	✖
Aug 8 , 2013 14:51	**PCX** iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline 10088)	✖

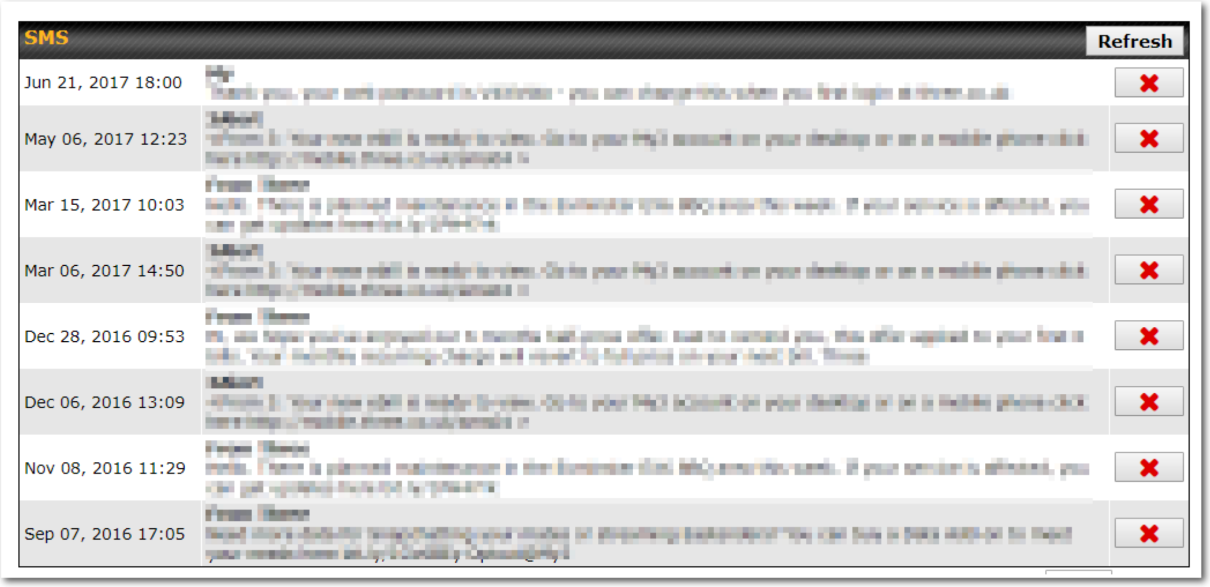
SMS

The SMS option allows you to read SMS (text) messages that have been sent to the SIM in your Pepwave router.



SIM Status

WAN Connection	Cellular ▾
SIM Card	1
IMSI	[redacted]
Tool	SMS ▾

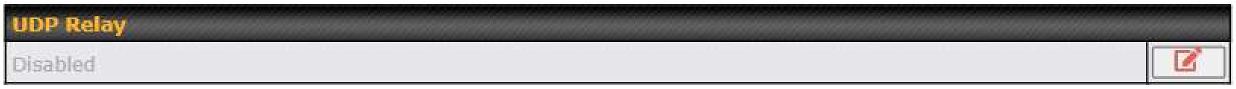


SMS Refresh

Jun 21, 2017 18:00	[redacted]	✖
May 06, 2017 12:23	[redacted]	✖
Mar 15, 2017 10:03	[redacted]	✖
Mar 06, 2017 14:50	[redacted]	✖
Dec 28, 2016 09:53	[redacted]	✖
Dec 06, 2016 13:09	[redacted]	✖
Nov 08, 2016 11:29	[redacted]	✖
Sep 07, 2016 17:05	[redacted]	✖

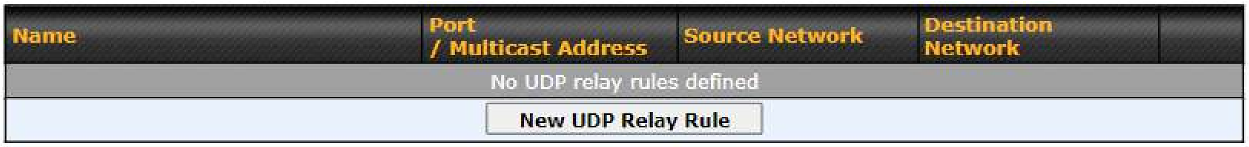
24.13 UDP Relay

You may define the UDP relay by clicking the **Advanced > Misc Settings > UDP Relay**. You can click ✎ to enable the UDP relay to relay UDP Broadcast or Multicast traffic for LAN/VLAN/SpeedFusion VPN.

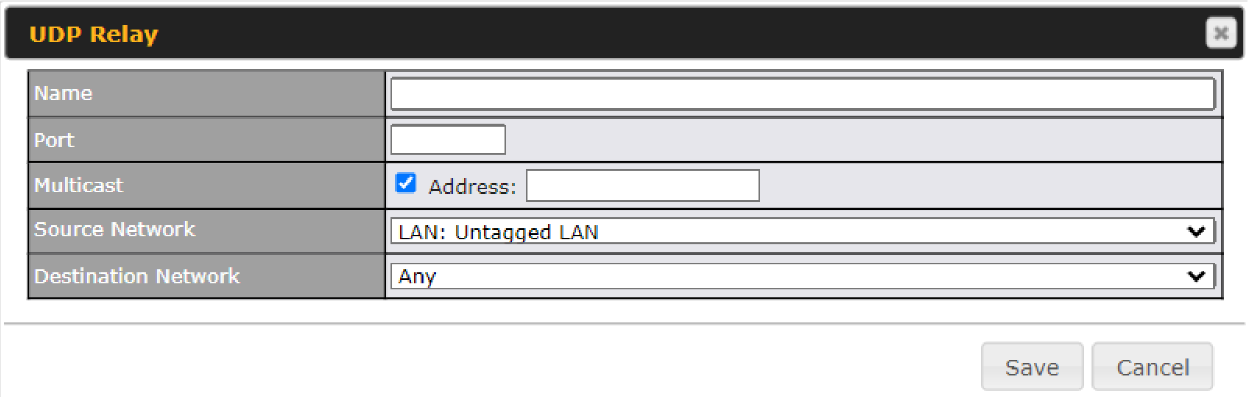


UDP Relay	
Disabled	✎

Click "*New UDP Relay Rule*" to define the relay rule.



Name	Port / Multicast Address	Source Network	Destination Network	
No UDP relay rules defined				



UDP Relay

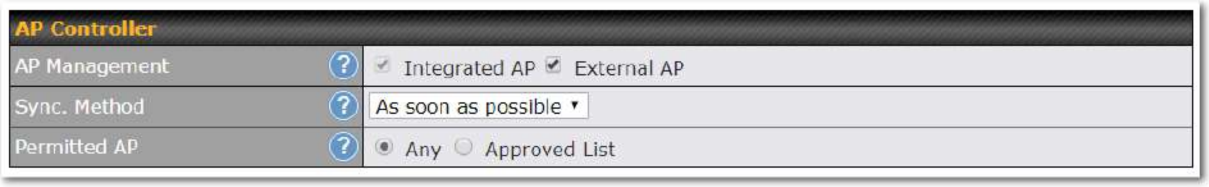
Name	
Port	
Multicast	☑ Address:
Source Network	LAN: Untagged LAN
Destination Network	Any

UDP Relay	
Name	This field is for specifying a name to represent this profile.
Port	This feid is to enter the specific port number for the UDP relay
Multicast	If Multicast is not selected, it will broadcast relay rule. If Multicast is selected, you may need to enter a valid multicast address.
Secure Network	Select the specific connection as a source network to where the device is to relay UDP Broadcast packets.
Destination Network	You may select the specific connection from the drop-down list or may custom combination network as a destination network that receives the UDP packet relays.

25 AP

25.1 AP Controller

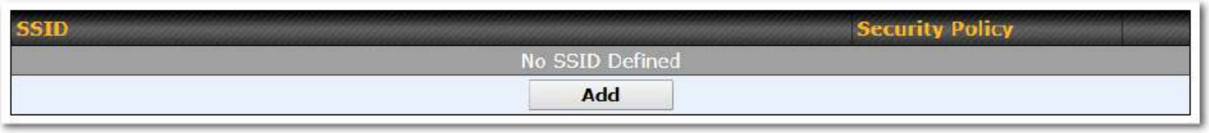
The AP controller acts as a centralized controller of Pepwave Access Points.
With this feature, users can customize and manage up to 1500 Access Points from a single Pepwave router interface.
To configure, navigate to the **AP** tab. and the following screen appears.



AP Controller	
AP Management	☑ Integrated AP ☑ External AP
Sync. Method	As soon as possible ▾
Permitted AP	● Any ○ Approved List

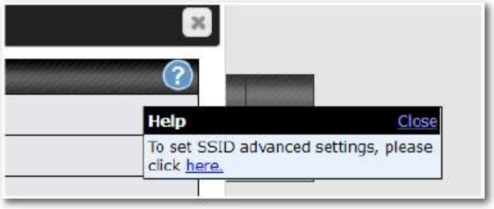
AP Controller	
AP Management	The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, **CAPWAP Access Controller addresses** (field 138), will be added to the DHCP server. A local DNS record, **AP Controller**, will be added to the local DNS proxy.
Sync Method	● As soon as possible ● Progressively ● One at a time
Permitted AP	Access points to manage can be specified here. If **Any** is selected, the AP controller will manage any AP that reports to it. If **Approved List** is selected, only APs with serial numbers listed in the provided text box will be managed.

25.2 Wireless SSID



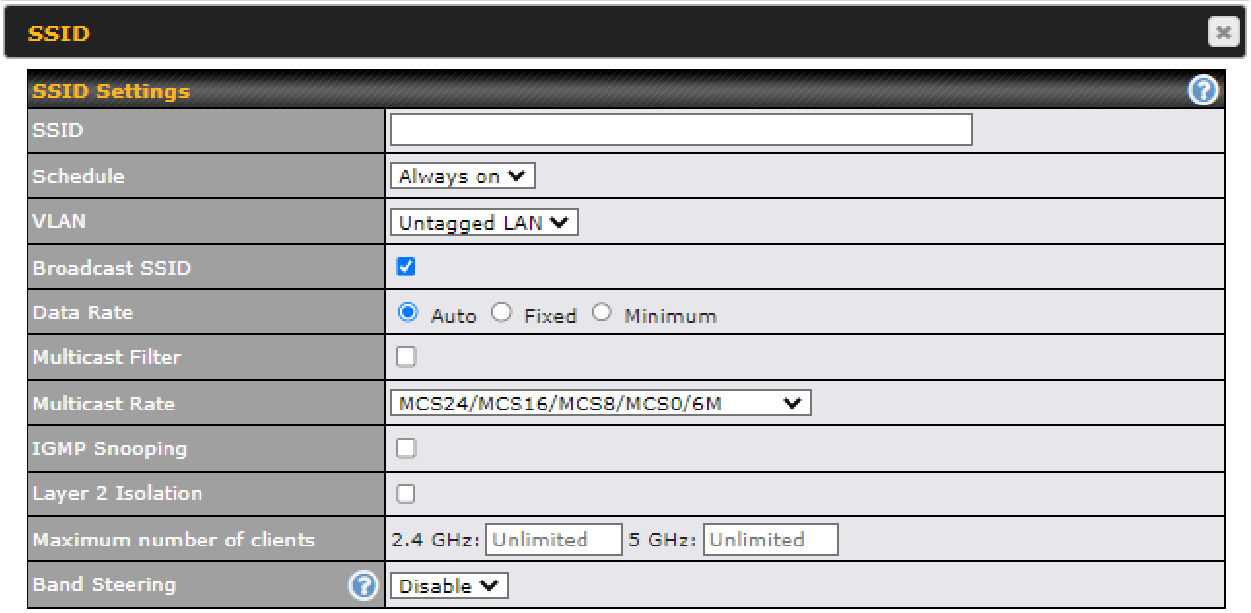
SSID	Security Policy
No SSID Defined	

Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model.
The below settings ishows a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



Help Close

To set SSID advanced settings, please click here.



SSID

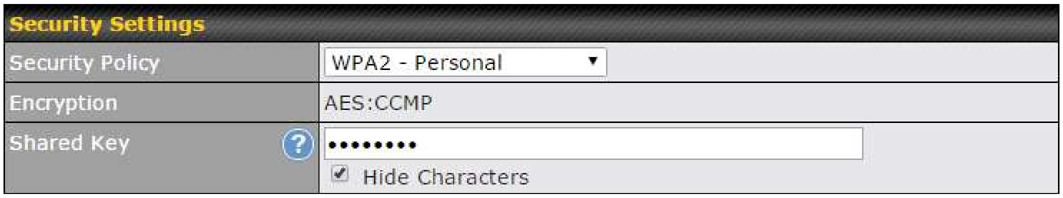
SSID Settings

SSID	
Schedule	Always on
VLAN	Untagged LAN
Broadcast SSID	☑
Data Rate	● Auto ○ Fixed ○ Minimum
Multicast Filter	□
Multicast Rate	MCS24/MCS16/MCS8/MCS0/6M
IGMP Snooping	□
Layer 2 Isolation	□
Maximum number of clients	2.4 GHz: Unlimited 5 GHz: Unlimited
Band Steering	Disable

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Schedule	Click the drop-down menu to apply a time schedule to this interface
VLAN	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is **0**, which means VLAN tagging is disabled (instead of tagged with zero).
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. **Broadcast SSID** is enabled by default.
Data Rate ^{A}	Select **Auto** to allow the Pepwave router to set the data rate automatically, or select **Fixed** and choose a rate from the displayed drop-down menu.
Multicast Filter^A	This setting enables the filtering of multicast network traffic to the wireless SSID.

Multicast Rate[A]	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected **Protocol** and **Channel Bonding** settings will affect the rate options and values available here.
IGMP Snooping [A]	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
Layer 2 Isolation [A]	**Layer 2** refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to the upper communication layer(s). By default, the setting is disabled.
Maximum Number of Clients [A]	Indicate the maximum number of clients that should be able to connect to each frequency.
Band Steering [A]	To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency. Choose between: **Force** - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. **Prefer** - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered. **Disable** - Default

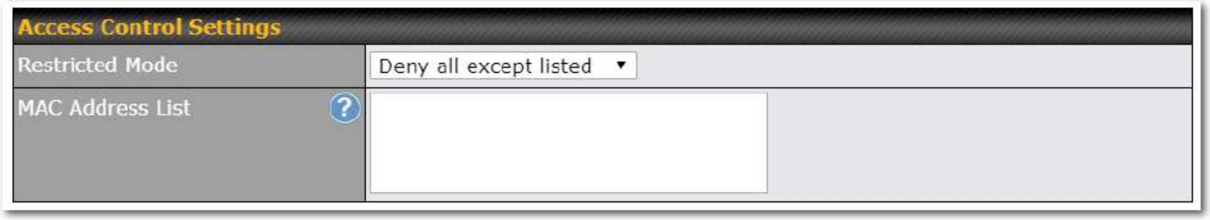
[A] - Advanced feature. Click the ? button on the top right-hand corner to activate.



Security Settings	
Security Policy	WPA2 - Personal ▾
Encryption	AES:CCMP
Shared Key ?	•••••••• ☑ Hide Characters

Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options : ● **Open (**No Encryption) ● **Enhanced Open** (OWE) ● **WPA3 -Personal** (AES:CCMP) ● **WPA3 -Enterprise** (AES:CCMP) ● **WPA2/WPA3 -Personal** (AES:CCMP) ● **WPA2 -Personal** (AES:CCMP) ● **WPA2 – Enterprise** ● **WPA/WPA2 - Personal** (TKIP/AES: CCMP)

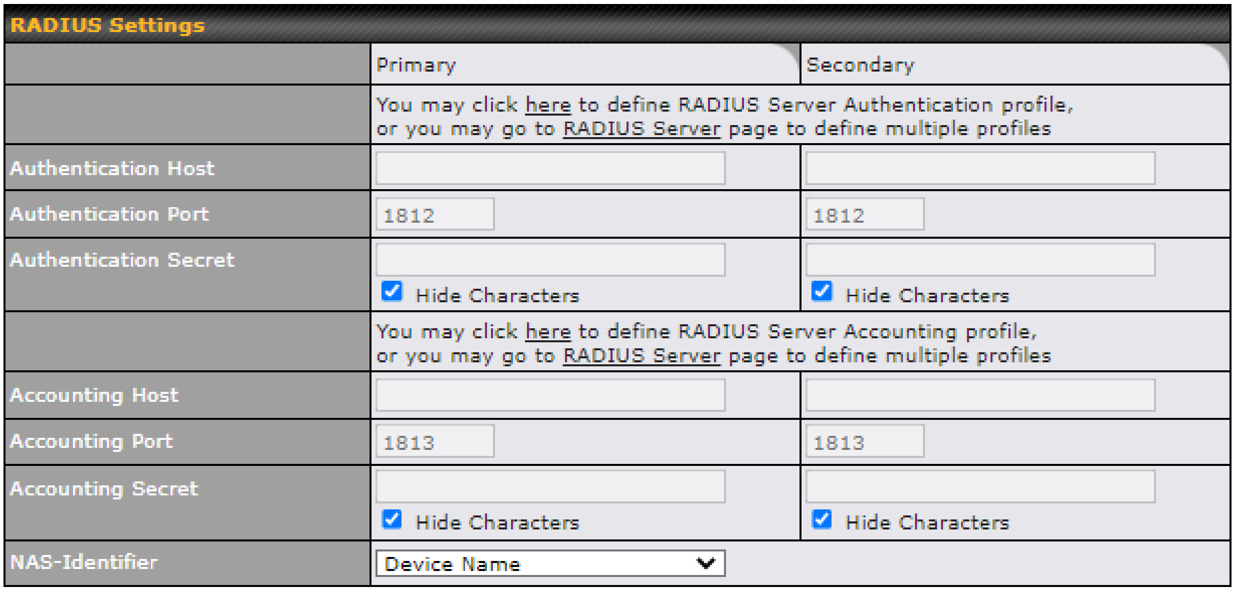
	● **WPA/WPA2 – Enterprise** When **WPA/WPA2 - Enterprise** is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the **Shared Key** option should be disabled. When using this method, select the appropriate version using the **V1/V2** controls. The security level of this method is known to be very high. When **WPA/WPA2- Personal** is configured, a shared key is used for data encryption and authentication. When using this configuration, the **Shared Key** option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high. **NOTE:** When **WPA2/WPA3- Personal** is configured, if a managed AP which is NOT WPA3 PSK capable, the AP Controller will not push those WPA3 and WPA2/WPA3 SSID to that AP.



Access Control Settings

Restricted Mode	Deny all except listed ▾
MAC Address List ?	

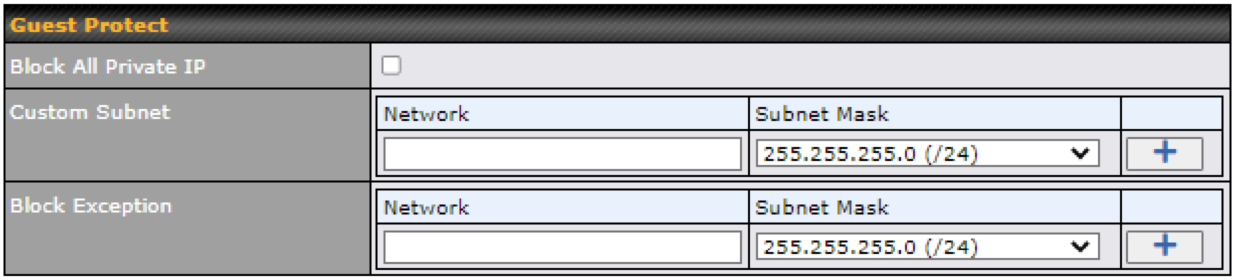
Access Control	
Restricted Mode	The settings allow the administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, **Accept all except listed** and **Radius MAC Authentication.**
MAC Address List	Connection coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field. If more than one MAC address needs to be entered, you can use a carriage return to separate them.



RADIUS Settings

	Primary	Secondary
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles	
Authentication Host		
Authentication Port	1812	1812
Authentication Secret	☑ Hide Characters	☑ Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles	
Accounting Host		
Accounting Port	1813	1813
Accounting Secret	☑ Hide Characters	☑ Hide Characters
NAS-Identifier	Device Name	

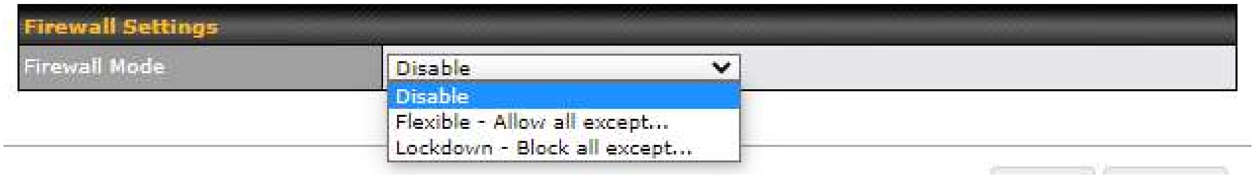
RADIUS Settings	
Authentication Host	This field is for specifying the IP address of the primary RADIUS server for Authentication and, if applicable, the secondary RADIUS server.
Authentication Port	In the field, the UDP authentication port(s) used by your RADIUS server(s) or click the **Default** is **1812**.
Authentication Secret	This settings is enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
Accounting Host	This field is for specifying the IP address of the primary RADIUS server for Accounting and, if applicable, the secondary RADIUS server.
Accounting Port	In the field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the **Default** is **1813**.
Accounting Secret	This settings is enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
NAS-Identifier	Choose between **Device Name**, **LAN MAC address**, **Device Serial Number** and **Custom Value**



Guest Protect

Block All Private IP	□
Custom Subnet	Network: □ Subnet Mask: 255.255.255.0 (/24) +
Block Exception	Network: □ Subnet Mask: 255.255.255.0 (/24) +

Guest Protect	
Block All Private IP	Check this box to deny all connection attempts by private IP addresses.
Custom Subnet	To create a custom subnet for guest access, enter the IP address and choose a subnet mask from the drop-down menu.
Block Exception	To block access from a particular subnet, enter the IP address and choose a subnet mask from the drop-down menu.



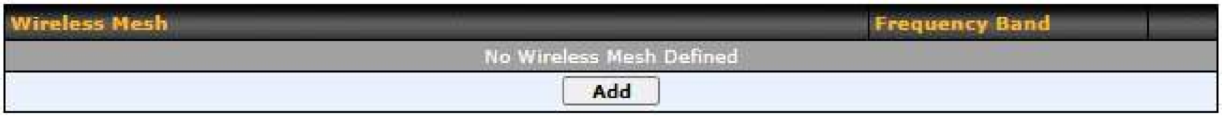
Firewall Settings

Firewall Mode: Disable

Disable
Flexible - Allow all except...
Lockdown - Block all except...

Firewall Settings	
Firewall Mode	The settings allow administrators to control access to the SSID based on Firewall Rules. Available options are **Disable, Lockdown - Block all except...** and **Flexible -Allow all except…**
Firewall Exceptions	Create Firewall Rules based on **Port, IP Network, MAC address** or **Domain Name**

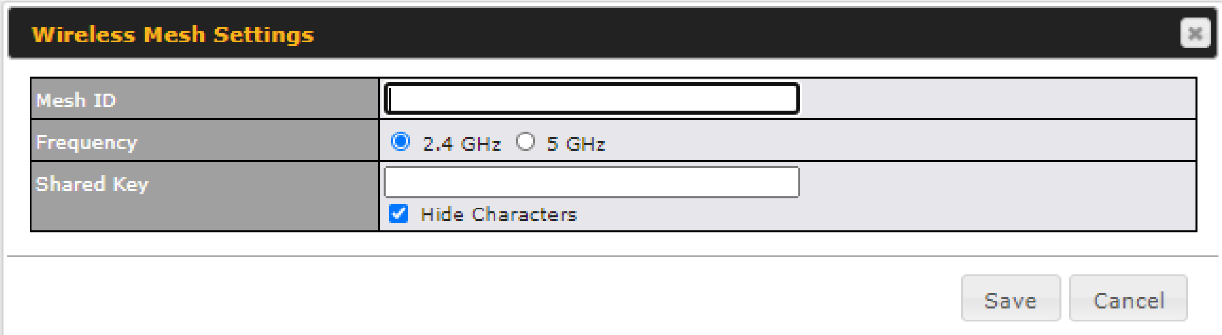
25.3 Wireless Mesh



Wireless Mesh	Frequency Band
No Wireless Mesh Defined	

Wireless Mesh Support is available on devices running 802.11ac (Wi-Fi 5) and above. Along with the AP Controller, mesh network extensions can be established, which can expand network coverage. Note that the Wireless Mesh settings need to match the Mesh ID and Shared Key of the other devices on the same selected frequency band.

To create a new Wireless Mesh profile, go to **AP** > **Wireless Mesh**, and click **Add**.



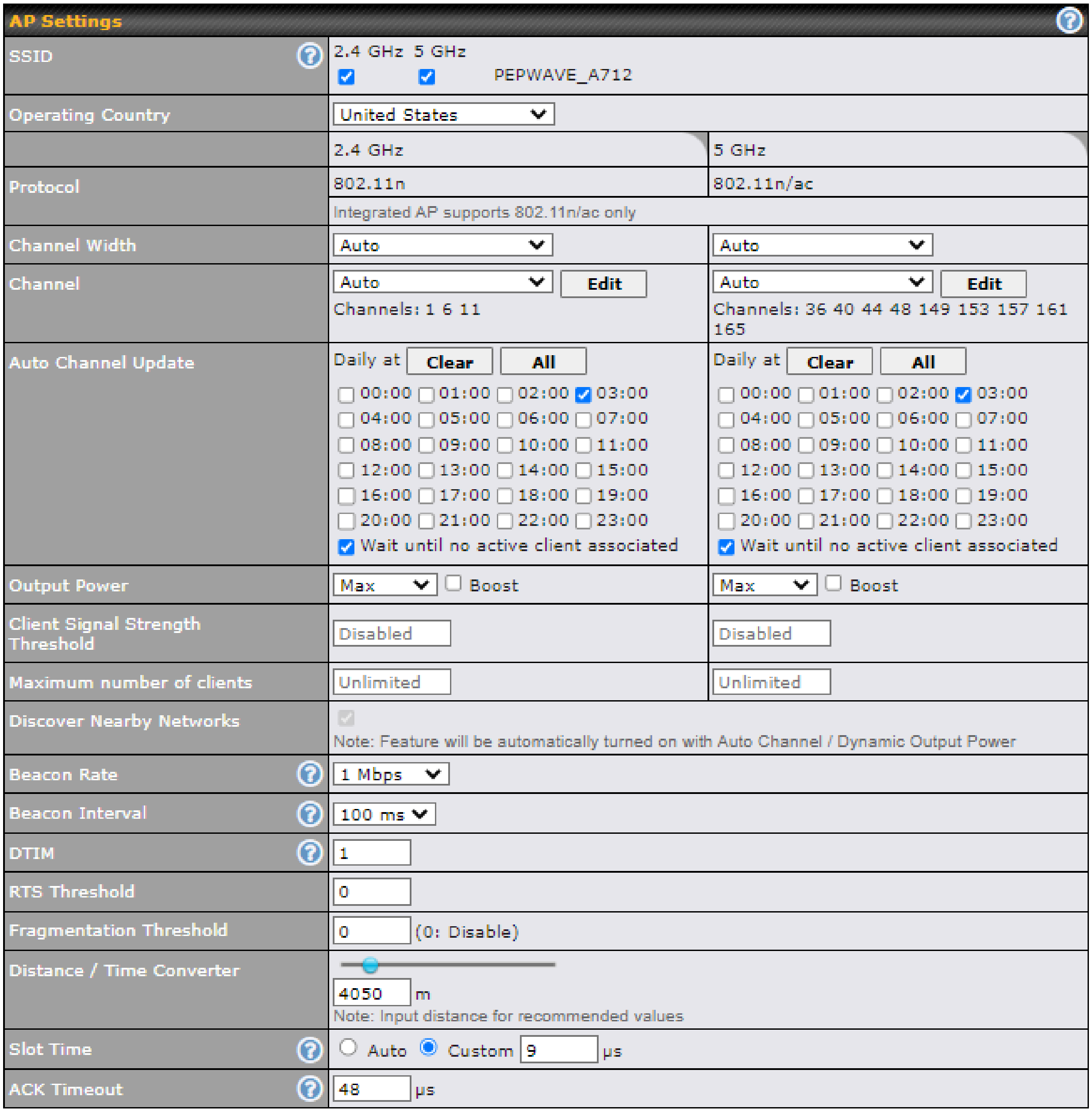
Wireless Mesh Settings

Mesh ID	
Frequency	● 2.4 GHz ○ 5 GHz
Shared Key	☑ Hide Characters

Wireless Mesh Settings	
Mesh ID	Enter a name to represent the Mesh profile.
Frequency	Select the 2.4GHz or 5GHz frequency to be used.
Shared Key	Enter the shared key in the text field. Please note that it needs to match the shared keys of the other APs in the Wireless Mesh settings. Click **Hide / Show Characters** to toggle visibility.

25.4 Settings

To configure the AP settings, navigating to **AP > Settings** :



AP Settings		
SSID	2.4 GHz 5 GHz ☑ ☑ PEPWAVE_A712	
Operating Country	United States	
	2.4 GHz	5 GHz
Protocol	802.11n	802.11n/ac
	Integrated AP supports 802.11n/ac only	
Channel Width	Auto	Auto
Channel	Auto Edit Channels: 1 6 11	Auto Edit Channels: 36 40 44 48 149 153 157 161 165
Auto Channel Update	Daily at Clear All □ 00:00 □ 01:00 □ 02:00 ☑ 03:00 □ 04:00 □ 05:00 □ 06:00 □ 07:00 □ 08:00 □ 09:00 □ 10:00 □ 11:00 □ 12:00 □ 13:00 □ 14:00 □ 15:00 □ 16:00 □ 17:00 □ 18:00 □ 19:00 □ 20:00 □ 21:00 □ 22:00 □ 23:00 ☑ Wait until no active client associated	Daily at Clear All □ 00:00 □ 01:00 □ 02:00 ☑ 03:00 □ 04:00 □ 05:00 □ 06:00 □ 07:00 □ 08:00 □ 09:00 □ 10:00 □ 11:00 □ 12:00 □ 13:00 □ 14:00 □ 15:00 □ 16:00 □ 17:00 □ 18:00 □ 19:00 □ 20:00 □ 21:00 □ 22:00 □ 23:00 ☑ Wait until no active client associated
Output Power	Max □ Boost	Max □ Boost
Client Signal Strength Threshold	Disabled	Disabled
Maximum number of clients	Unlimited	Unlimited
Discover Nearby Networks	☑ Note: Feature will be automatically turned on with Auto Channel / Dynamic Output Power	
Beacon Rate	1 Mbps	
Beacon Interval	100 ms	
DTIM	1	
RTS Threshold	0	
Fragmentation Threshold	0 (0: Disable)	
Distance / Time Converter	4050 m Note: Input distance for recommended values	
Slot Time	○ Auto ● Custom 9 μs	
ACK Timeout	48 μs	

AP Settings	
SSID	These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Pepwave MAX does not detect whether the AP is capable of transmitting at

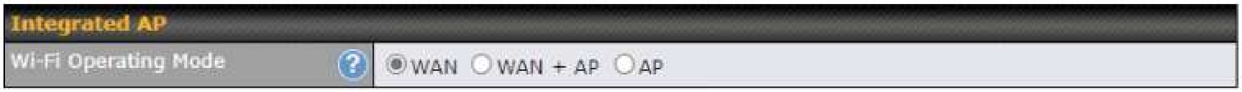
	both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
Operating Country	This drop-down menu specifies the national / regional regulations which the AP should follow. ● If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). ● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). Note: Users are required to choose an option suitable to local laws and regulations. Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.
Preferred Frequency	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected.
Channel Width	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
Channel	This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If **Auto** is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power	This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When **Dynamic** settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance. The **Dynamic: Auto** setting will set the AP to do this automatically. Otherwise, the **Dynamic: Manual** setting will set the AP to dynamically adjust only if instructed to do so. If you have set **Dynamic:Manual**, you can go to **AP>Toolbox>Auto Power Adj.** to give your AP further instructions. If you click the **Boost** checkbox, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference.

Client Signal Strength Threshold	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Max number of Clients	This field determines the maximum clients that can be connected to APs under this profile.
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is **0** by default, meaning that no VLAN tagging will be applied. Note: change this value with caution as alterations may result in loss of connection to the AP controller.
Discover Nearby Networks[A]	This option is to turn on and off to scan the nearby the AP. **Note**: Feature will be automatically turned on with Auto Channel / Dynamic Output Power
Beacon Rate[A]	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are **1Mbps**, **2Mbps**, **5.5Mbps**, **6Mbps**, and **11Mbps**.
Beacon Interval[A]	This drop-down menu provides the option to set the time between each beacon send. Available options are **100ms**, **250ms**, and **500ms**.
DTIM[A]	This field provides the option to set the frequency for beacon to include delivery traffic indication message (DTIM). The interval unit is measured in milliseconds.
RTS Threshold[A]	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting **0** disables this feature.
Fragmentation Threshold[A]	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
Distance/Time Converter[A]	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time[A]	This field provides the option to modify the unit wait time before it transmits. The default value is **9µs.**
ACK Timeout[A]	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is **48µs.**

[A] - Advanced feature. Click the ? button on the top right-hand corner to activate.

Important Note

Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.

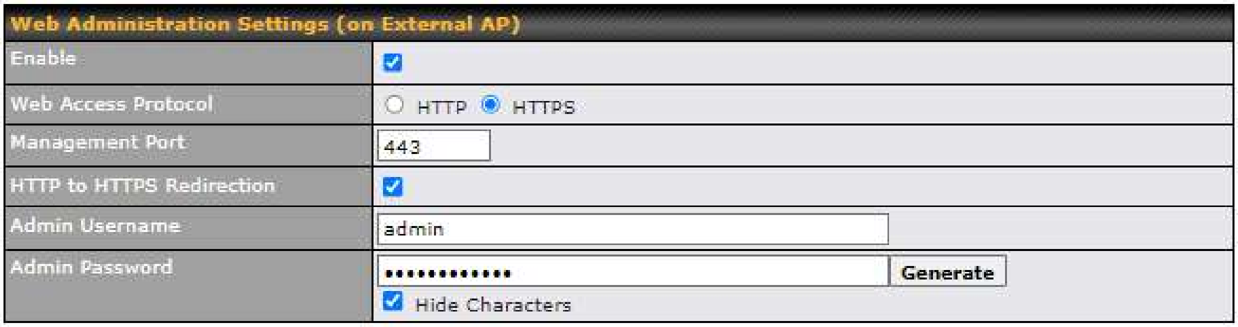


Integrated AP	
Wi-Fi Operating Mode	● WAN ○ WAN + AP ○ AP

The device with integrated AP can operate under the Wi-Fi Operating Mode, and the default setting is **WAN + AP** mode:

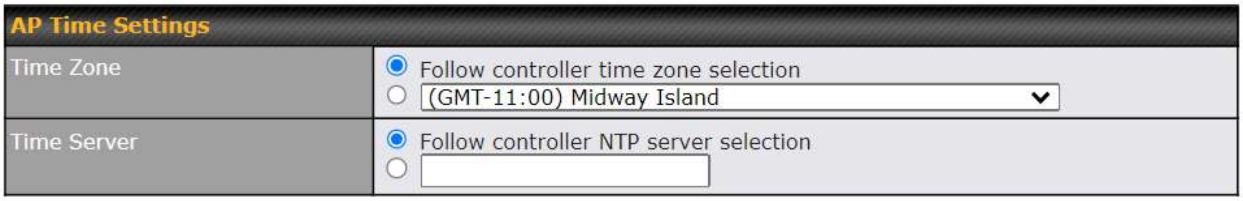
Note: This option is available for selected devices only (HD2/HD4 and HD2/HD4 MBX).

Integrated AP	
WAN	In this mode, all Wi-Fi will operate as Wi-Fi WAN and no integrated Wi-Fi AP will be operated on this device. If Wi-Fi Operating mode is choosing **WAN**, The status indicated by the front panel LED is as follows: - Wi-Fi 1 is Green if Wi-Fi WAN 1 is enabled. - Wi-Fi 2 is Green if Wi-Fi WAN 2 is enabled.
WAN + AP	In this mode, some Wi-Fi will operate as Wi-Fi WAN. Some other Wi-Fi WANs will be forced offline and their Wi-Fi resources will be reserved for integrated Wi-Fi AP operations. If Wi-Fi Operating mode is choosing **WAN + AP**, The status indicated by the front panel LED is as follows: - Wi-Fi 1 is Green if WI-FI WAN is enabled. - Wi-Fi 2 is Green if Wi-Fi AP is ON.
AP	In this mode, all Wi-Fi functions as integrated Wi-Fi AP. All Wi-Fi WANs will be forced to go offline. If Wi-Fi Operating mode is choosing **AP**, The status indicated by the front panel LED is as follows: - W-Fi 1 is Green, if there is any Wireless SSID is selected 2.4GHz. - W-Fi 2 is Green, if there is any Wireless SSID is selected 5GHz.



Web Administration Settings (on External AP)	
Enable	☑
Web Access Protocol	○ HTTP ● HTTPS
Management Port	443
HTTP to HTTPS Redirection	☑
Admin Username	admin
Admin Password	•••••••••••• Generate ☑ Hide Characters

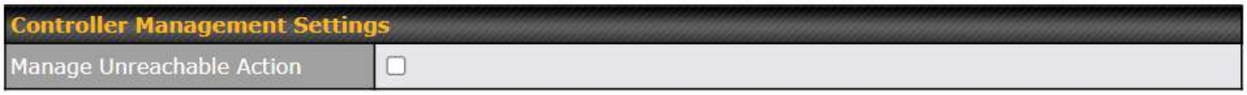
Web Administration Settings (on External AP)	
Enable	Check the box to allow the Pepwave router to manage the web admin access information of the AP.
Web Access Protocol	These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are **HTTP** and **HTTPS**.
Management Port	This field specifies the management port used for accessing the device.
HTTP to HTTPS Redirection	This option will be available if you have chosen **HTTPS** as the **Web Access Protocol**. With this enabled, any HTTP access to the web admin will redirect to HTTPS automatically.
Admin User Name	This field specifies the administrator username of the web admin. It is set as *admin* by default.
Admin Password	This field allows you to specify a new administrator password. You may also click the **Generate** button and let the system generate a random password automatically.



AP Time Settings	
Time Zone	● Follow controller time zone selection ○ (GMT-11:00) Midway Island
Time Server	● Follow controller NTP server selection ○

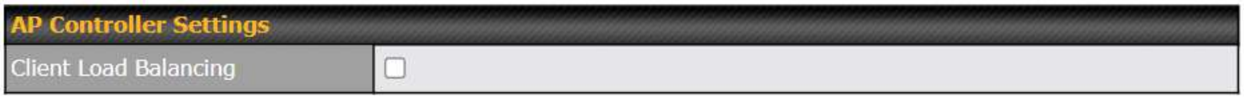
This allow user to configure AP Time Settings (both Timezone and NTP) in AP Controller.

AP Time Settings	
Time Zone	Ths field is to select the time zone for the AP controller.
Time Server	Ths field is to select the time server for the AP controller.



Controller Management Settings	
Manage Unreachable Action	□

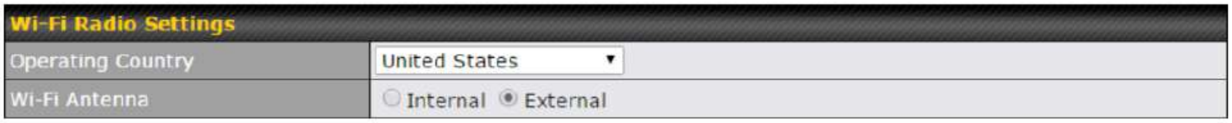
This settings is to allow user to manage external AP's controller unreachable action. When **Manage Unreachable Action** is checked, there will have 2 options which are "**None**" and "**Radio Off**".



AP Controller Settings	
Client Load Balancing	□

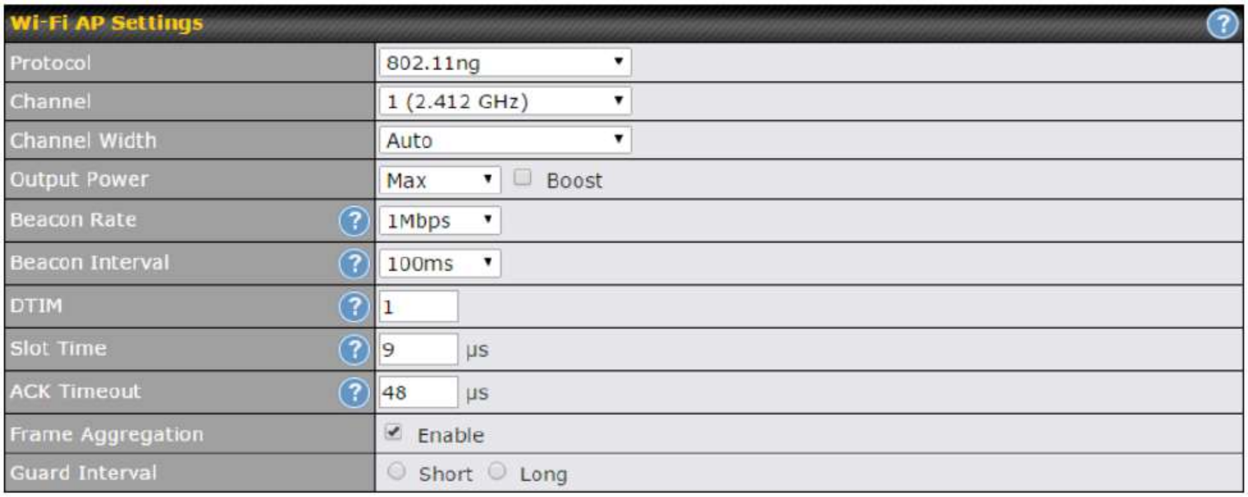
This is an option to enable client load balancing for AP Controller. When the option is enabled, it is trying to balance the station count on APs within the same profile.

Some Pepwave models displays a screen similar to the one shown below, navigating to **AP > Settings**:



Wi-Fi Radio Settings	
Operating Country	United States ▾
Wi-Fi Antenna	○ Internal ● External

Wi-Fi Radio Settings	
Operating Country	This option sets the country whose regulations the Pepwave router follows.
Wi-Fi Antenna	Wi-Fi Antenna Choose from the router's internal or optional external antennas, if so equipped.



Wi-Fi AP Settings	
Protocol	802.11ng ▾
Channel	1 (2.412 GHz) ▾
Channel Width	Auto ▾
Output Power	Max ▾ □ Boost
Beacon Rate	1Mbps ▾
Beacon Interval	100ms ▾
DTIM	1
Slot Time	9 μs
ACK Timeout	48 μs
Frame Aggregation	☑ Enable
Guard Interval	○ Short ○ Long

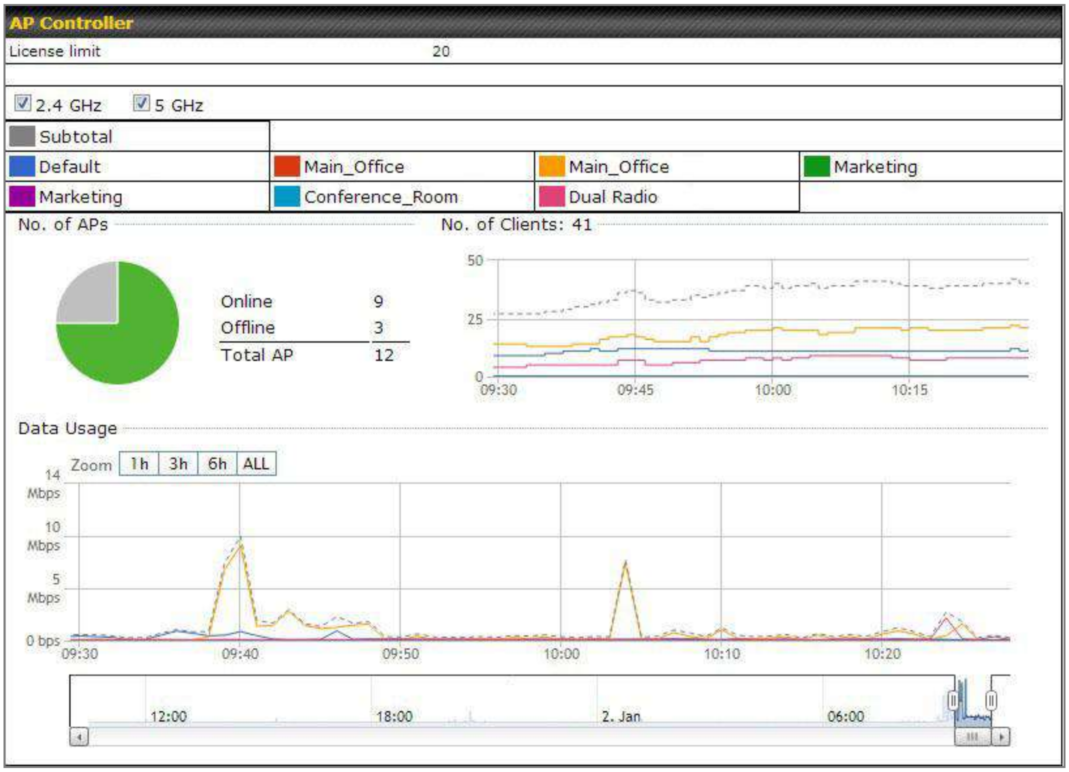
Wi-Fi AP Settings	
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, 802.11ng is selected.

Channel	This option allows you to select which 802.11 RF channel will be used. **Channel 1 (2.412 GHz)** is selected by default.
Channel Width	**Auto (20/40 MHz)** and **20 MH**z are available. The default setting is **Auto (20/40 MHz)**, which allows both widths to be used simultaneously.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country.
Beacon Rate[A]	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval[A]	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DITM[A]	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to **1 ms**.
Slot Time[A]	This field is for specifying the wait time before the Router transmits a packet. By default, this field is set to **9 µs**.
ACK Time[A]	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 µs**.
Frame Aggreagtion[A]	This option allows you to enable frame aggregation to increase transmission throughput.
Guard Interval[A]	This setting allows choosing a short or long guard period interval for your transmissions.

26 AP Controller Status

26.1 Info

A comprehensive overview of your AP can be accessed by navigating to **AP > Controller Status > Info**.



AP Controller

License limit	20

☑ 2.4 GHz ☑ 5 GHz

▨ Subtotal			
🟦 Default	🟥 Main_Office	🟧 Main_Office	🟩 Marketing
🟪 Marketing	🟦 Conference_Room	🟥 Dual Radio	

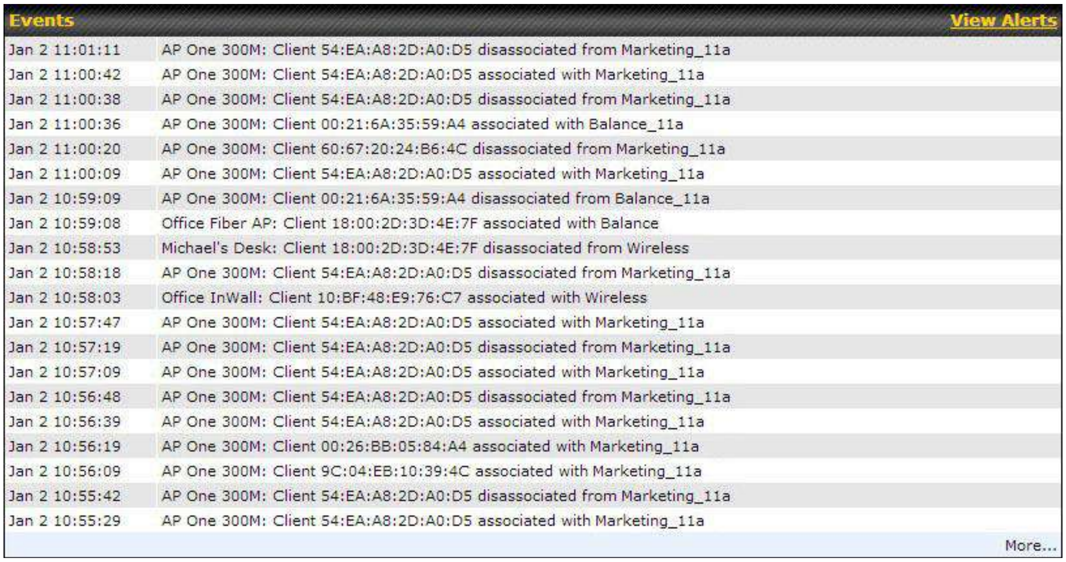
No. of APs

Online	9
Offline	3
Total AP	12

No. of Clients: 41

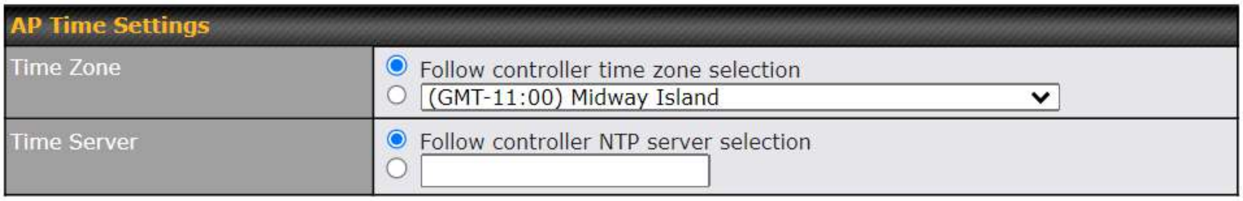
AP Controller	
License Limit	This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.
Frequency	Underneath, there are two check boxes labeled **2.4 Ghz** and **5 Ghz**. Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.
SSID	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No.of Clients	This graph displays the number of clients connected to each network at any

	given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.
Data Usage	This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to **Zoom** to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.



```
Events                                                                    View Alerts
Jan 2 11:01:11   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20   AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:00:09   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:59:09   AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:59:08   Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance
Jan 2 10:58:53   Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless
Jan 2 10:58:18   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:58:03   Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless
Jan 2 10:57:47   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:57:19   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:57:09   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:56:48   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:56:39   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:56:19   AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a
Jan 2 10:56:09   AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a
Jan 2 10:55:42   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:55:29   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
                                                                              More...
```

Events
This event log displays all activity on your AP network, down to the client level. Click **View Alerts** to see only alerts, and click the **More…** link for additional records.

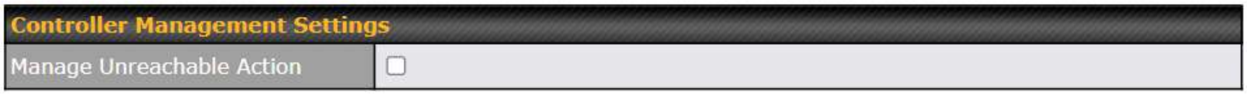


AP Time Settings

Time Zone	● Follow controller time zone selection ○ (GMT-11:00) Midway Island
Time Server	● Follow controller NTP server selection ○

This allow user to configure AP Time Settings (both Timezone and NTP) in AP Controller.

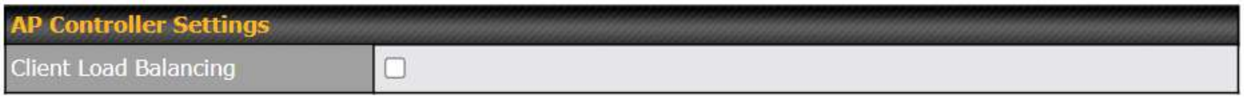
AP Time Settings	
Time Zone	Ths field is to select the time zone for the AP controller.
Time Server	Ths field is to select the time server for the AP controller.



Controller Management Settings

Manage Unreachable Action	□

This settings is to allow user to manage external AP's controller unreachable action. When **Manage Unreachable Action** is checked, there will have 2 options which are "**None**" and "**Radio Off**".



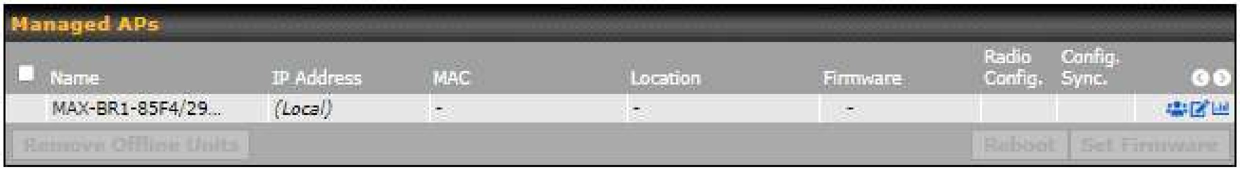
AP Controller Settings

Client Load Balancing	□

This is an option to enable client load balancing for AP Controller. When the option is enabled, it is trying to balance the station count on APs within the same profile.

26.2 Access Point

A detailed breakdown of data usage for each AP is available at **AP > Controller Status > Access Point**.

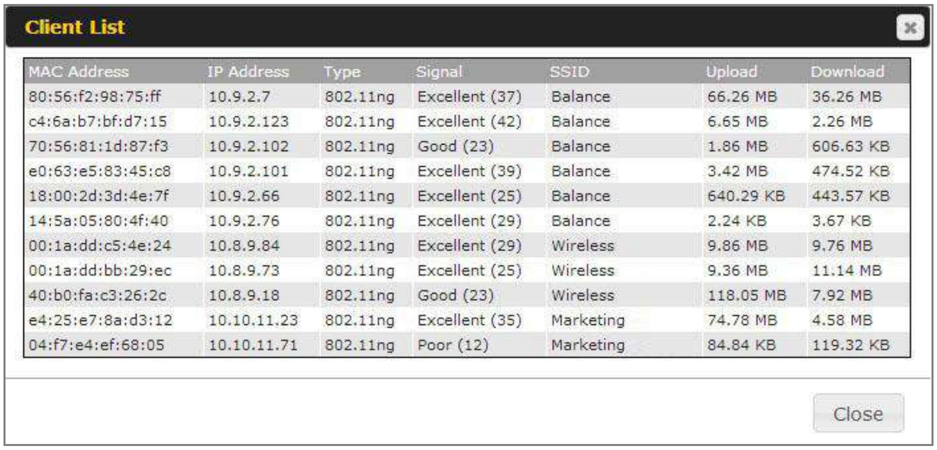


Managed APs

□	Name	IP Address	MAC	Location	Firmware	Radio Config.	Config. Sync.	
	MAX-BR1-85F4/29...	(Local)	-	-	-			

Remove Offline Units | Reboot | Set Firmware

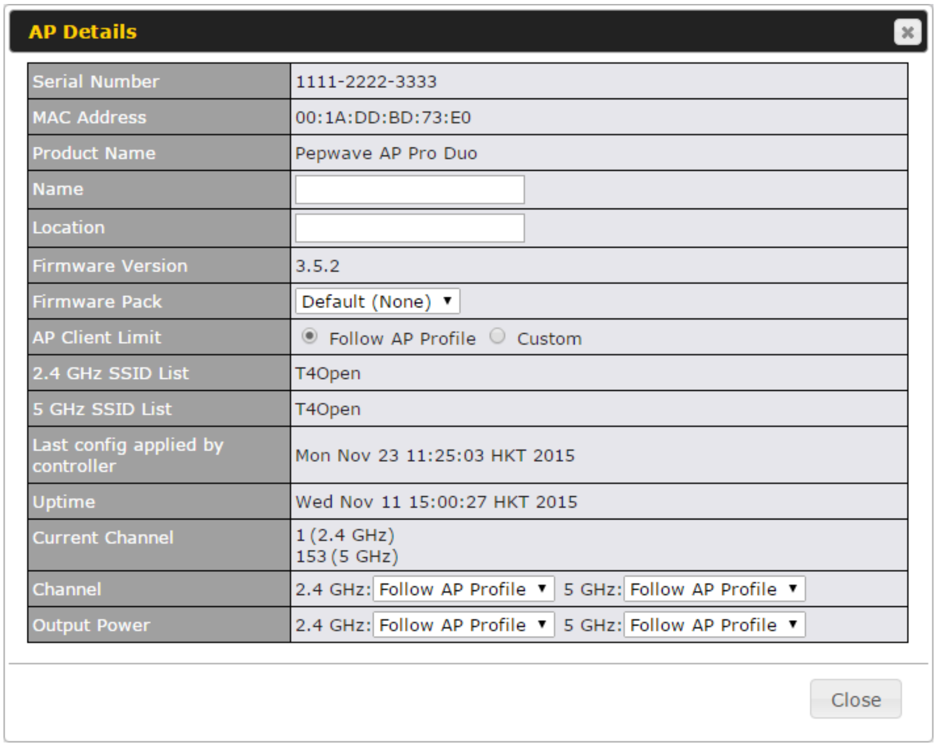
Managed APs	
Managed APs	This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group. On the right of the table, you will see the following icons: . Click the icon to see a usage table for each client:



Client List

MAC Address	IP Address	Type	Signal	SSID	Upload	Download
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB

Click the icon to configure each client

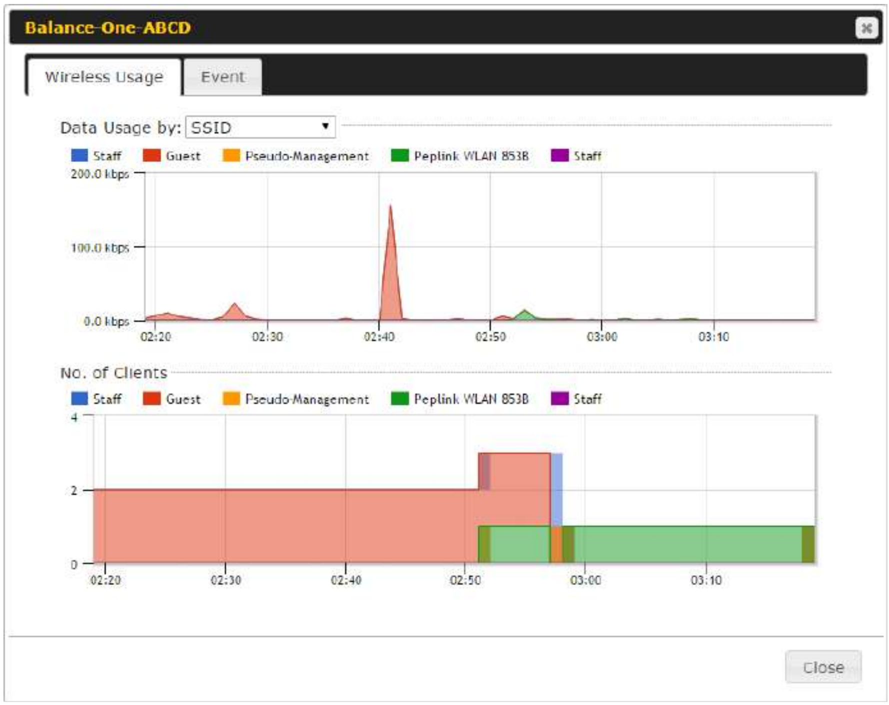


AP Details

Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
Product Name	Pepwave AP Pro Duo
Name	
Location	
Firmware Version	3.5.2
Firmware Pack	Default (None) ▾
AP Client Limit	● Follow AP Profile ○ Custom
2.4 GHz SSID List	T4Open
5 GHz SSID List	T4Open
Last config applied by controller	Mon Nov 23 11:25:03 HKT 2015
Uptime	Wed Nov 11 15:00:27 HKT 2015
Current Channel	1 (2.4 GHz) 153 (5 GHz)
Channel	2.4 GHz: Follow AP Profile ▾ 5 GHz: Follow AP Profile ▾
Output Power	2.4 GHz: Follow AP Profile ▾ 5 GHz: Follow AP Profile ▾

For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

Click the icon to see a graph displaying usage:

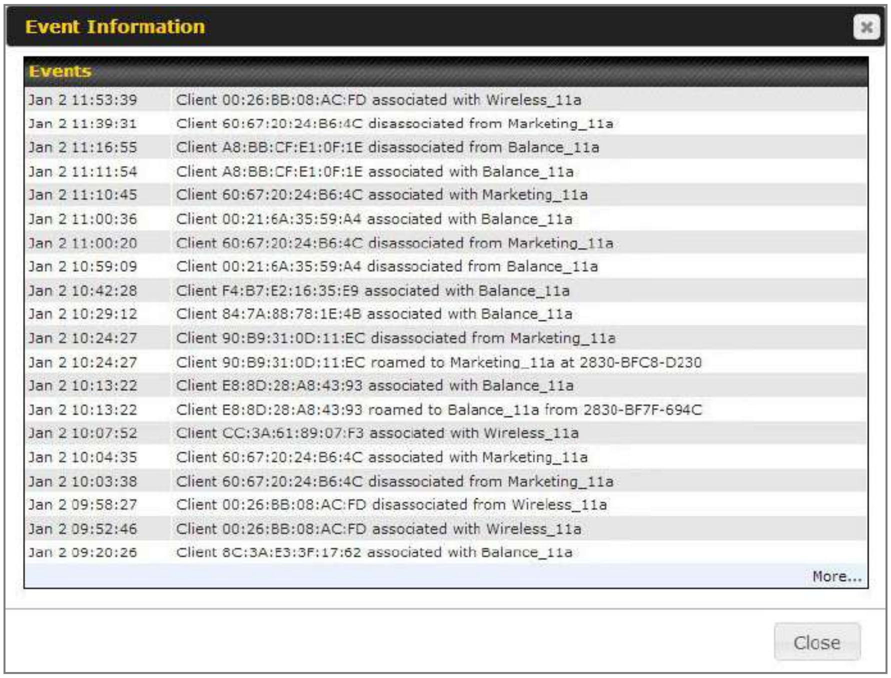


Balance-One-ABCD

Data Usage by: SSID

Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate.

Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:



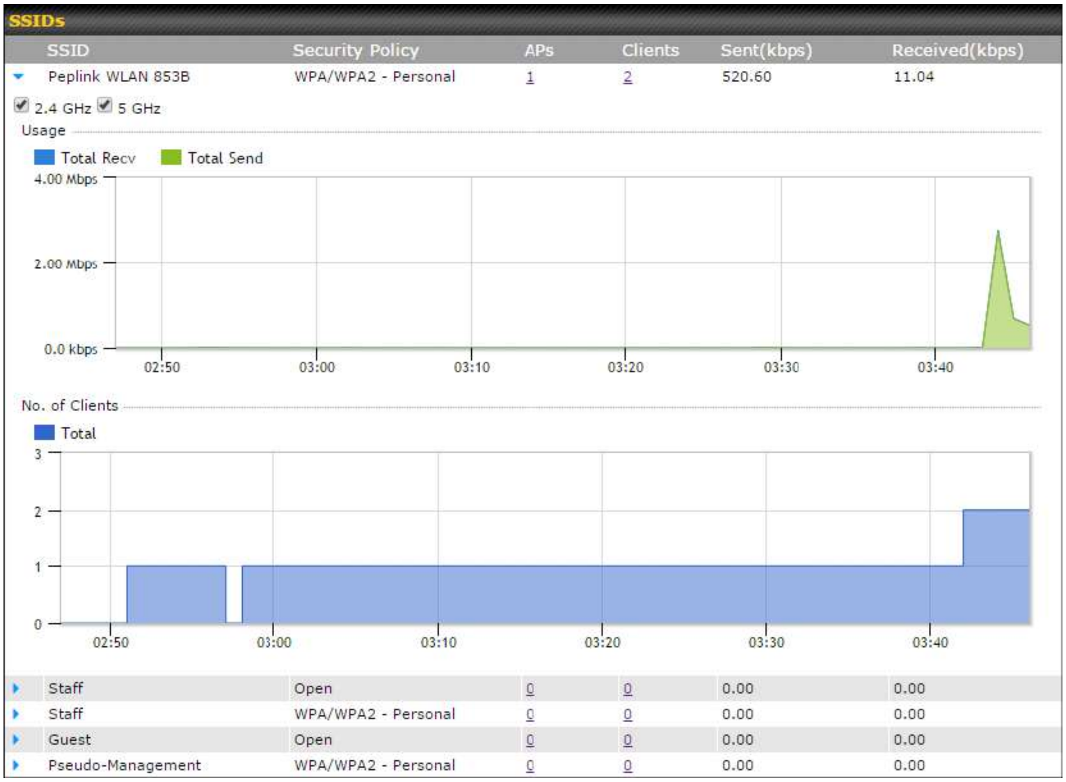
Event Information

Events

```
Jan 2 11:53:39    Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 11:39:31    Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:16:55    Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54    Client A8:BB:CF:E1:0F:1E associated with Balance_11a
Jan 2 11:10:45    Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 11:00:36    Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20    Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 10:59:09    Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:42:28    Client F4:B7:E2:16:35:E9 associated with Balance_11a
Jan 2 10:29:12    Client 84:7A:88:78:1E:4B associated with Balance_11a
Jan 2 10:24:27    Client 90:B9:31:0D:11:EC disassociated from Marketing_11a
Jan 2 10:24:27    Client 90:B9:31:0D:11:EC roamed to Marketing_11a at 2830-BFC8-D230
Jan 2 10:13:22    Client E8:8D:28:A8:43:93 associated with Balance_11a
Jan 2 10:13:22    Client E8:8D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-694C
Jan 2 10:07:52    Client CC:3A:61:89:07:F3 associated with Wireless_11a
Jan 2 10:04:35    Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 10:03:38    Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 09:58:27    Client 00:26:BB:08:AC:FD disassociated from Wireless_11a
Jan 2 09:52:46    Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 09:20:26    Client 8C:3A:E3:3F:17:62 associated with Balance_11a
```

26.3 Wireless SSID

In-depth SSID reports are available under **AP > Controller Status > Wireless SSID**.



SSIDs

	SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
▾	Peplink WLAN 853B	WPA/WPA2 - Personal	1	2	520.60	11.04

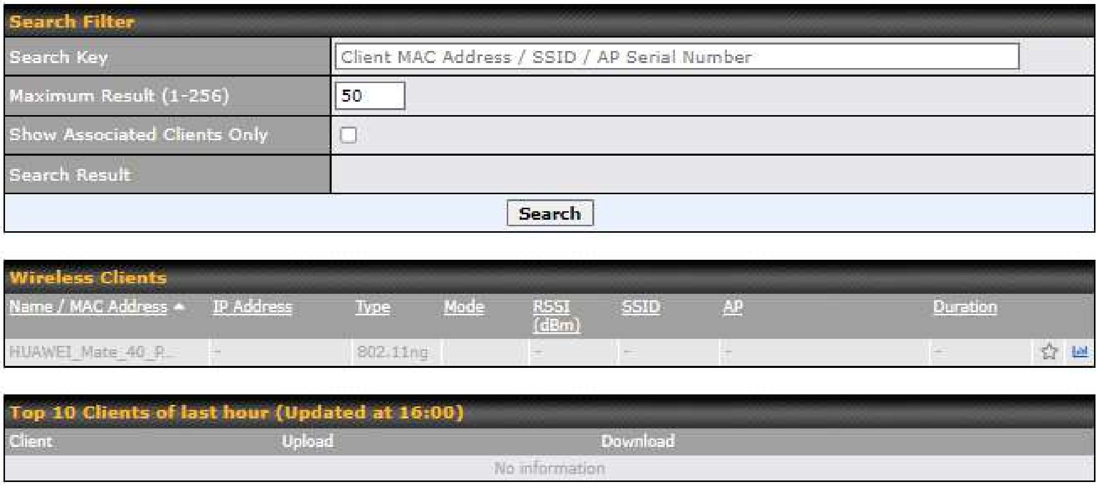
☑ 2.4 GHz ☑ 5 GHz

	SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
▸	Staff	Open	0	0	0.00	0.00
▸	Staff	WPA/WPA2 - Personal	0	0	0.00	0.00
▸	Guest	Open	0	0	0.00	0.00
▸	Pseudo-Management	WPA/WPA2 - Personal	0	0	0.00	0.00

Click the blue arrow on any SSID to obtain more detailed usage information on each SSID.

26.4 Wireless Client

You can search for specific Wi-Fi users by navigating to **AP > Controller Status > Wireless Client**.



Search Filter

Search Key	Client MAC Address / SSID / AP Serial Number
Maximum Result (1-256)	50
Show Associated Clients Only	□
Search Result	

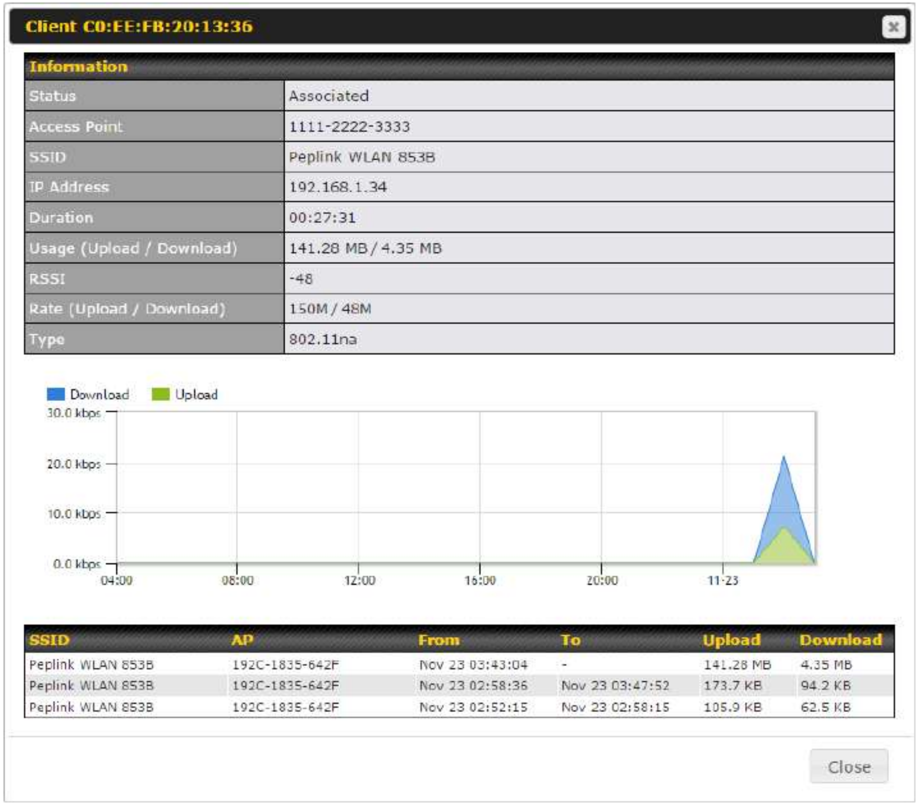
Wireless Clients

Name / MAC Address ▲	IP Address	Type	Mode	RSSI (dBm)	SSID	AP	Duration	
HUAWEI_Mate_40_P...	-	802.11ng		-	-	-	-	☆ 📊

Top 10 Clients of last hour (Updated at 16:00)

Client	Upload	Download
No information		

Here, you will be able to see your network's heaviest users as well as search for specific users. Click the ☆ icon to bookmark specific users, and click the 📊 icon for additional details about each user:



Client C0:EE:FB:20:13:36

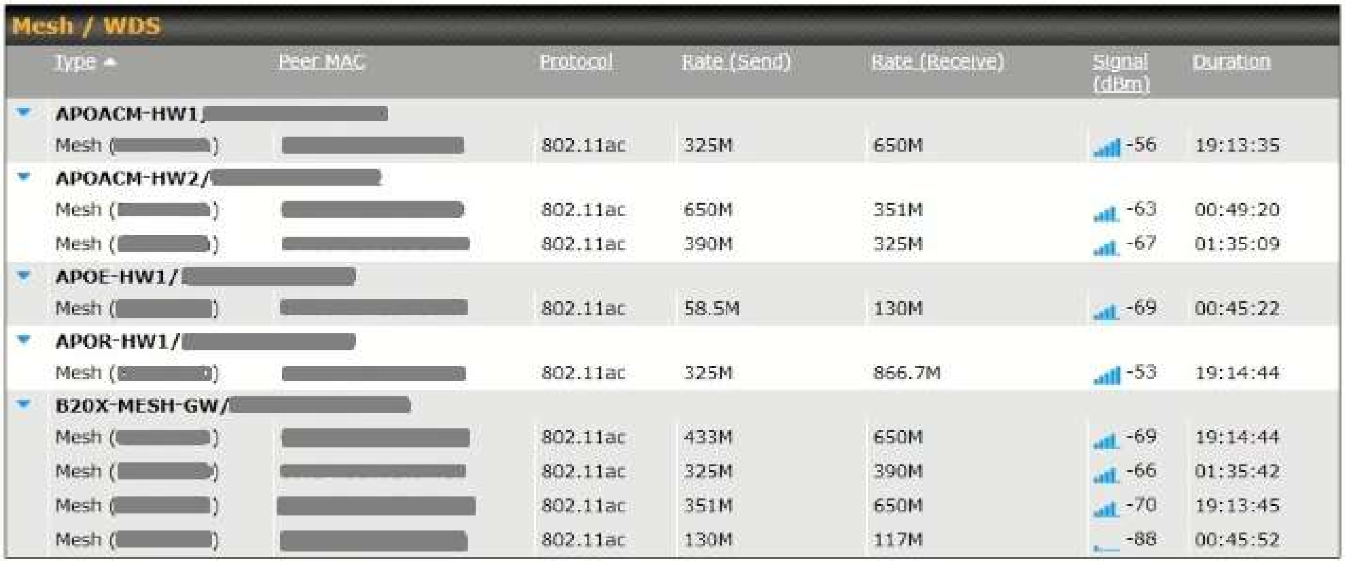
Information

Status	Associated
Access Point	1111-2222-3333
SSID	Peplink WLAN 853B
IP Address	192.168.1.34
Duration	00:27:31
Usage (Upload / Download)	141.28 MB / 4.35 MB
RSSI	-48
Rate (Upload / Download)	150M / 48M
Type	802.11na

SSID	AP	From	To	Upload	Download
Peplink WLAN 853B	192C-1835-642F	Nov 23 03:43:04	-	141.28 MB	4.35 MB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:58:36	Nov 23 03:47:52	173.7 KB	94.2 KB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:52:15	Nov 23 02:58:15	105.9 KB	62.5 KB

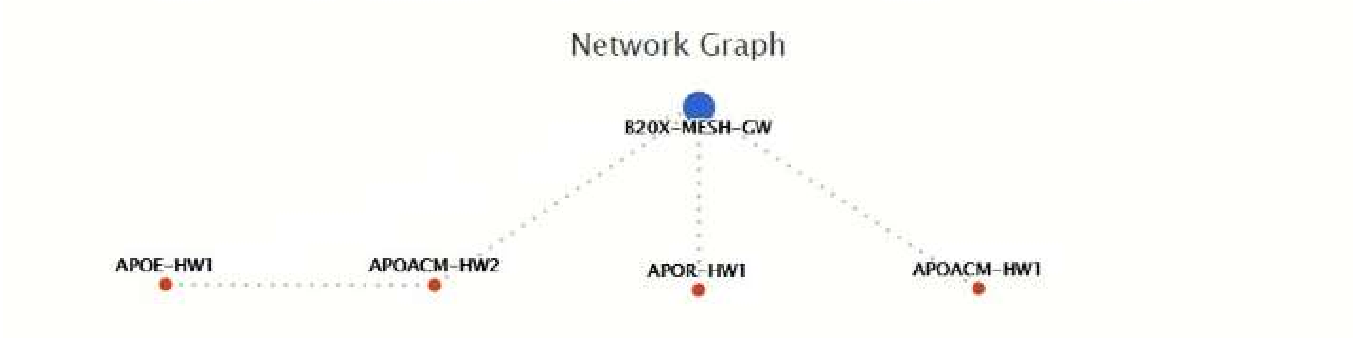
26.5 Mesh / WDS

Mesh / WDS allows you to monitor the status of your wireless distribution system (WDS) or Mesh, and track activity by MAC address by navigating to **AP > Controller Status > Mesh / WDS**. This table shows the detailed information of each AP, including protocol, transmit rate (sent / received), signal strength, and duration.



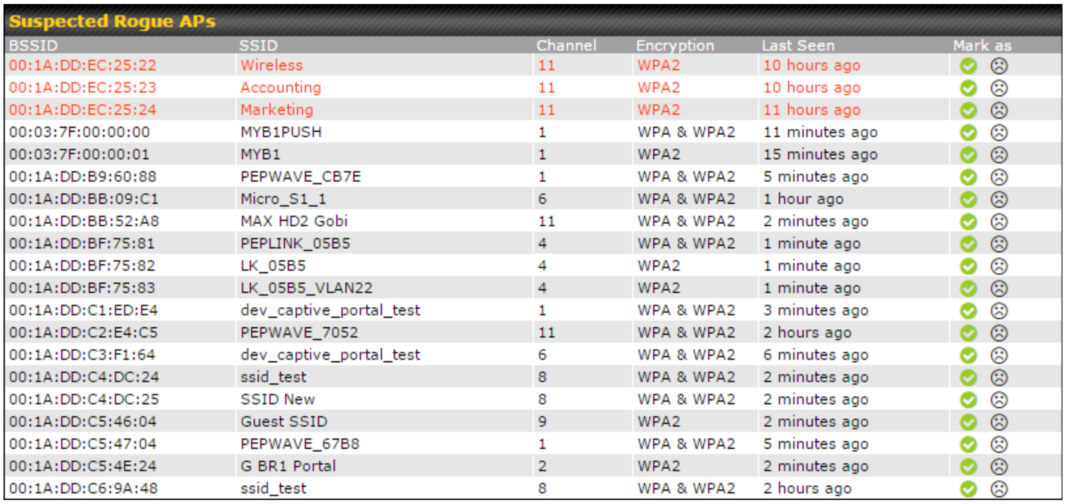
Mesh / WDS

	Type ▲	Peer MAC	Protocol	Rate (Send)	Rate (Receive)	Signal (dBm)	Duration
▼	APOACM-HW1/[redacted]						
	Mesh ([redacted])	[redacted]	802.11ac	325M	650M	-56	19:13:35
▼	APOACM-HW2/[redacted]						
	Mesh ([redacted])	[redacted]	802.11ac	650M	351M	-63	00:49:20
	Mesh ([redacted])	[redacted]	802.11ac	390M	325M	-67	01:35:09
▼	APOE-HW1/[redacted]						
	Mesh ([redacted])	[redacted]	802.11ac	58.5M	130M	-69	00:45:22
▼	APOR-HW1/[redacted]						
	Mesh ([redacted])	[redacted]	802.11ac	325M	866.7M	-53	19:14:44
▼	B20X-MESH-GW/[redacted]						
	Mesh ([redacted])	[redacted]	802.11ac	433M	650M	-69	19:14:44
	Mesh ([redacted])	[redacted]	802.11ac	325M	390M	-66	01:35:42
	Mesh ([redacted])	[redacted]	802.11ac	351M	650M	-70	19:13:45
	Mesh ([redacted])	[redacted]	802.11ac	130M	117M	-88	00:45:52



26.6 Nearby Device

A listing of near devices can be accessed by navigating to **AP > Controller Status > Nearby Device**.



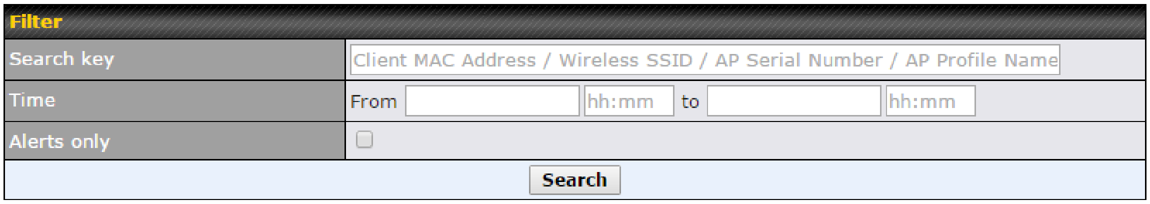
Suspected Rogue APs

BSSID	SSID	Channel	Encryption	Last Seen	Mark as
00:1A:DD:EC:25:22	Wireless	11	WPA2	10 hours ago	✓ ☹
00:1A:DD:EC:25:23	Accounting	11	WPA2	10 hours ago	✓ ☹
00:1A:DD:EC:25:24	Marketing	11	WPA2	11 hours ago	✓ ☹
00:03:7F:00:00:00	MYB1PUSH	1	WPA & WPA2	11 minutes ago	✓ ☹
00:03:7F:00:00:01	MYB1	1	WPA2	15 minutes ago	✓ ☹
00:1A:DD:B9:60:88	PEPWAVE_CB7E	1	WPA & WPA2	5 minutes ago	✓ ☹
00:1A:DD:BB:09:C1	Micro_S1_1	6	WPA & WPA2	1 hour ago	✓ ☹
00:1A:DD:BB:52:A8	MAX HD2 Gobi	11	WPA & WPA2	2 minutes ago	✓ ☹
00:1A:DD:BF:75:81	PEPLINK_05B5	4	WPA & WPA2	1 minute ago	✓ ☹
00:1A:DD:BF:75:82	LK_05B5	4	WPA2	1 minute ago	✓ ☹
00:1A:DD:BF:75:83	LK_05B5_VLAN22	4	WPA2	1 minute ago	✓ ☹
00:1A:DD:C1:ED:E4	dev_captive_portal_test	1	WPA & WPA2	3 minutes ago	✓ ☹
00:1A:DD:C2:E4:C5	PEPWAVE_7052	11	WPA & WPA2	2 hours ago	✓ ☹
00:1A:DD:C3:F1:64	dev_captive_portal_test	6	WPA & WPA2	6 minutes ago	✓ ☹
00:1A:DD:C4:DC:24	ssid_test	8	WPA & WPA2	2 minutes ago	✓ ☹
00:1A:DD:C4:DC:25	SSID New	8	WPA & WPA2	2 minutes ago	✓ ☹
00:1A:DD:C5:46:04	Guest SSID	9	WPA2	2 minutes ago	✓ ☹
00:1A:DD:C5:47:04	PEPWAVE_67B8	1	WPA & WPA2	5 minutes ago	✓ ☹
00:1A:DD:C5:4E:24	G BR1 Portal	2	WPA2	2 minutes ago	✓ ☹
00:1A:DD:C6:9A:48	ssid_test	8	WPA & WPA2	2 hours ago	✓ ☹

Suspected Rogue Devices
Hovering over the device MAC address will result in a popup with information on how this device was detected. Click the ✓ ☹ icons and the device will be moved to the bottom table of identified devices.

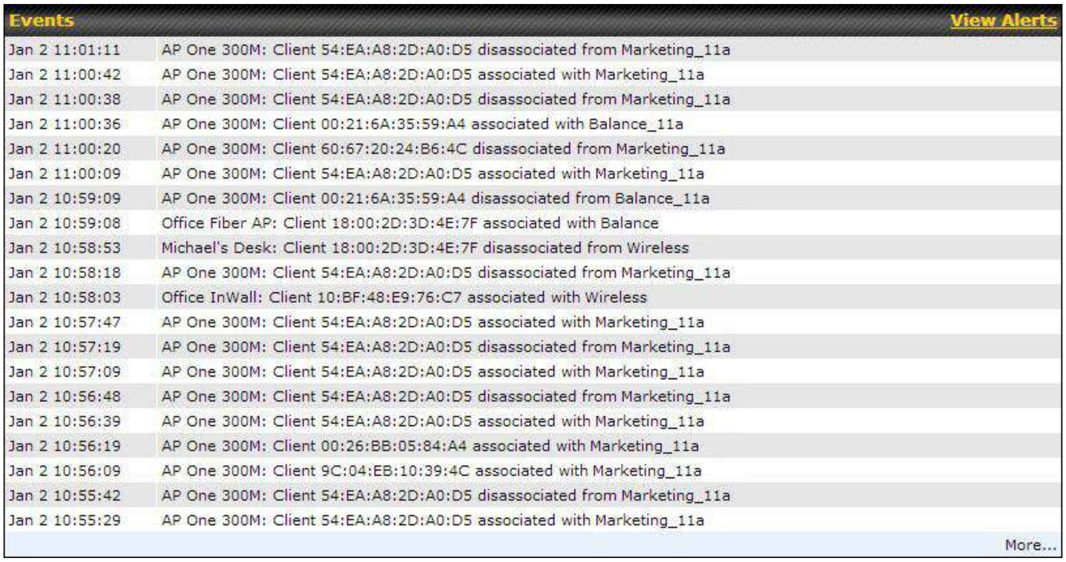
26.7 Event Log

You can access the AP Controller Event log by navigating to **AP > Controller Status > Event Log**.



Filter

Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From [ ] hh:mm to [ ] hh:mm
Alerts only	□

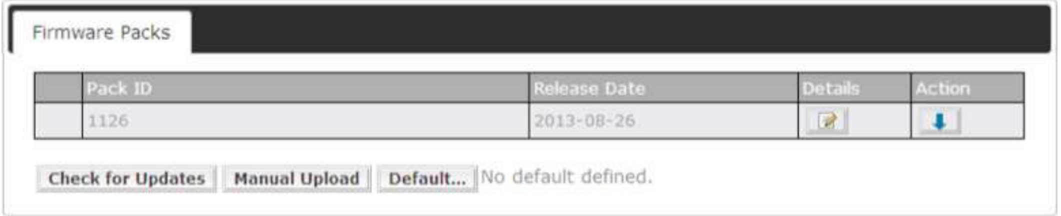


```
Jan 2 11:01:11   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20   AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:00:09   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:59:09   AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:59:08   Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance
Jan 2 10:58:53   Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless
Jan 2 10:58:18   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:58:03   Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless
Jan 2 10:57:47   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:57:19   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:57:09   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:56:48   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:56:39   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 10:56:19   AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a
Jan 2 10:56:09   AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a
Jan 2 10:55:42   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 10:55:29   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
```

Events
This event log displays all activity on your AP network, down to the client level. Use to filter box to search by MAC address, SSID, AP Serial Number, or AP Profile name. Click **View Alerts** to see only alerts, and click the **More…** link for additional records.

27 Toolbox

Tools for managing firmware packs can be found at **AP > Toolbox**.



	Pack ID	Release Date	Details	Action
	1126	2013-08-26	📝	⬇

No default defined.

Firmware Packs
Here, you can manage the firmware of your AP. Clicking on 📝 will result in information regarding each firmware pack. To receive new firmware packs, you can click **Check for Updates** to download new packs, or you can click **Manual Upload** to manually upload a firmware pack. Click **Default** to define which firmware pack is default.

28 System

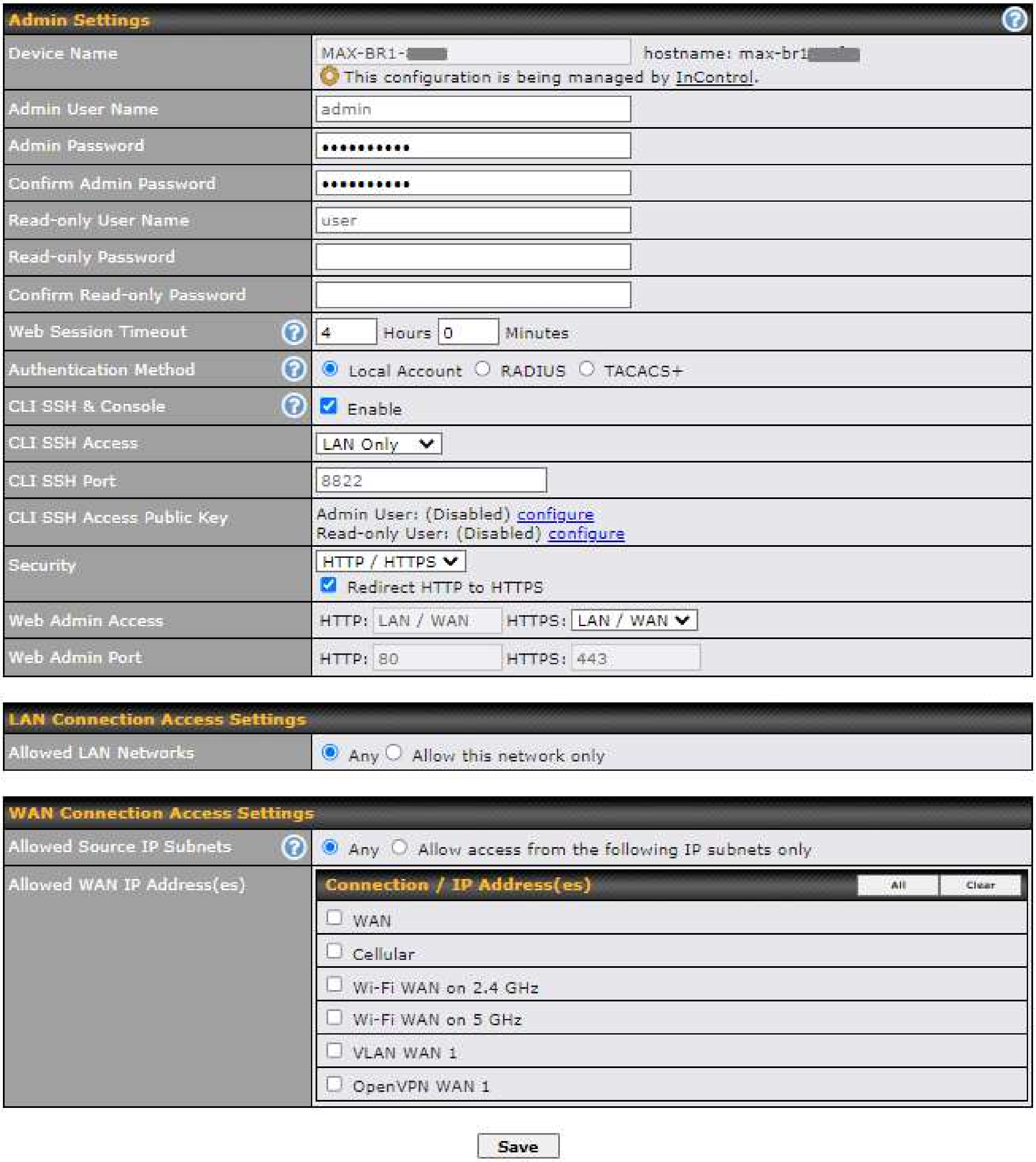
28.1 Admin Security

There are two types of user accounts available for accessing the web admin: *admin* and *user*. They represent two user levels: the admin level has full administrative access, while the user level is read-only. The user level can access only the device's status information; users cannot make any changes on the device.

A web login session will be logged out automatically when it has been idle longer than the **Web Session Timeout**. Before the session expires, you may click the **Logout** button in the web admin to exit the session.

0 hours 0 minutes signifies an unlimited session time. This setting should be used only in special situations, as it will lower the system security level if users do not log out before closing the browser. The **default** is 4 hours, 0 minutes.

For security reasons, after logging in to the web admin Interface for the first time, it is recommended to change the administrator password. Configuring the administration interface to be accessible only from the LAN can further improve system security. Administrative settings configuration is located at **System > Admin Security**.

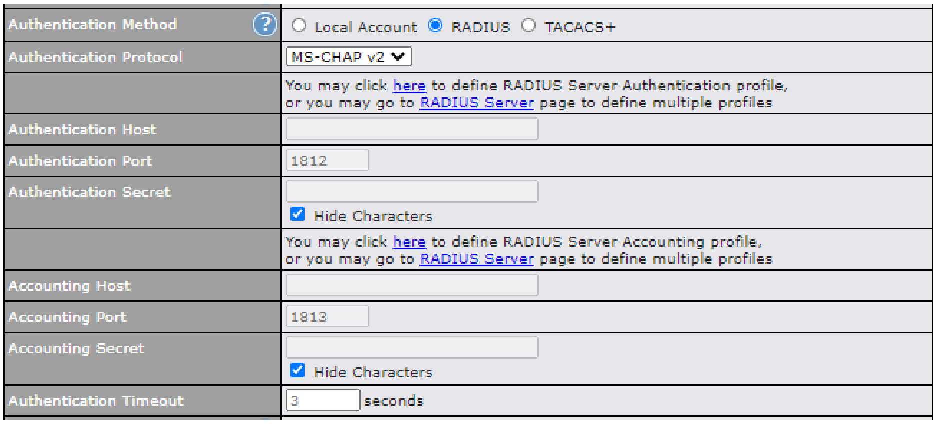


Admin Settings	
Device Name	MAX-BR1-[redacted] hostname: max-br1[redacted] This configuration is being managed by InControl.
Admin User Name	admin
Admin Password	••••••••••
Confirm Admin Password	••••••••••
Read-only User Name	user
Read-only Password	
Confirm Read-only Password	
Web Session Timeout	4 Hours 0 Minutes
Authentication Method	● Local Account ○ RADIUS ○ TACACS+
CLI SSH & Console	☑ Enable
CLI SSH Access	LAN Only
CLI SSH Port	8822
CLI SSH Access Public Key	Admin User: (Disabled) configure Read-only User: (Disabled) configure
Security	HTTP / HTTPS ☑ Redirect HTTP to HTTPS
Web Admin Access	HTTP: LAN / WAN HTTPS: LAN / WAN
Web Admin Port	HTTP: 80 HTTPS: 443

LAN Connection Access Settings	
Allowed LAN Networks	● Any ○ Allow this network only

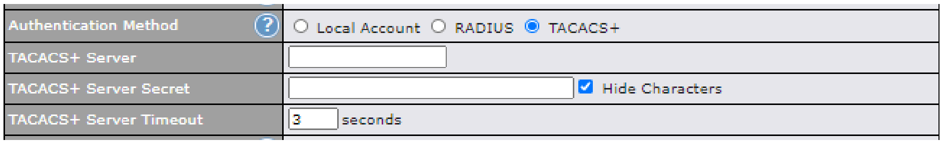
WAN Connection Access Settings	
Allowed Source IP Subnets	● Any ○ Allow access from the following IP subnets only
Allowed WAN IP Address(es)	Connection / IP Address(es) □ WAN □ Cellular □ Wi-Fi WAN on 2.4 GHz □ Wi-Fi WAN on 5 GHz □ VLAN WAN 1 □ OpenVPN WAN 1

Admin Settings	
Device Name	This field allows you to define a name for this Pepwave router. By default, **Device Name** is set as **MAX_XXXX**, where *XXXX* refers to the last 4 digits of

	the unit's serial number.
Admin User Name	**Admin User Name** is set as *admin* by default, but can be changed, if desired.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	**Read-only User Name** is set as *user* by default, but can be changed, if desired.
Read-only Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm Read-only Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to **4 hours**.
Authentication Method	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked. Available options: ● Local Account ● RADIUS  Authentication Method: ○ Local Account ● RADIUS ○ TACACS+ Authentication Protocol: MS-CHAP v2 You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles Authentication Host: Authentication Port: 1812 Authentication Secret: ☑ Hide Characters You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles Accounting Host: Accounting Port: 1813 Accounting Secret: ☑ Hide Characters Authentication Timeout: 3 seconds **Authentication** This specifies the authentication protocol used.

Protocol	Available options are **MS-CHAP v2** and **PAP**.
Authentication Host	This specifies the IP address or hostname of the RADIUS server host.
Authentication Port	This setting specifies the UDP destination port for authentication requests.
Authentication Secret	This field is for entering the secret key for accessing the RADIUS server.
Accounting Host	This specifies the IP address or hostname of the RADIUS server host.
Accounting Port	This setting specifies the UDP destination port for accounting requests.
Accounting Secret	This field is for entering the secret key for accessing the accounting server.
Authentication Timeout	This option specifies the time value for authentication timeout

- TACACS+

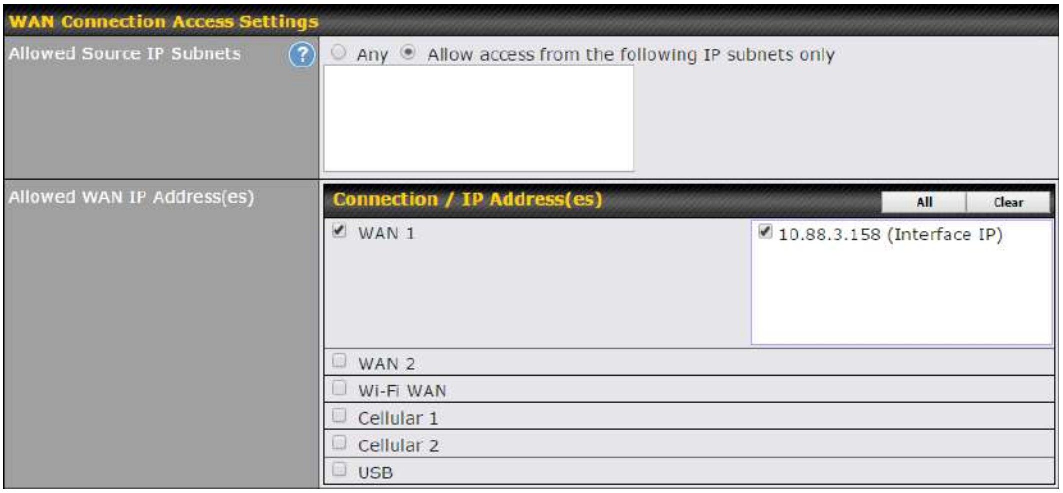


Authentication Method	○ Local Account ○ RADIUS ● TACACS+
TACACS+ Server	
TACACS+ Server Secret	☑ Hide Characters
TACACS+ Server Timeout	3 seconds

TACACS+ Server	This specifies the access address of the external TACACS+ server.
TACACS+ Server Secret	This field is for entering the secret key for accessing the RADIUS server.
TACACS+ Server Timeout	This option specifies the time value for TACACS+ timeout

CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to **Section 30.5.**
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.

CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access Public Key	This field is for entering the Public Key for Admin Users and Read-only Users to access CLI SSH.
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: ● HTTP ● HTTPS ● HTTP/HTTPS HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.
Web Admin Access	This option is for specifying the network interfaces through which the web admin interface can be accessed: ● LAN only ● LAN/WAN If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed.
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.



WAN Connection Access Settings

Allowed Source IP Subnets ? ○ Any ● Allow access from the following IP subnets only

Allowed WAN IP Address(es)

Connection / IP Address(es)	All Clear
☑ WAN 1	☑ 10.88.3.158 (Interface IP)
□ WAN 2	
□ Wi-Fi WAN	
□ Cellular 1	
□ Cellular 2	
□ USB	

WAN Connection Access Settings	
Allowed Source IP Subnets	This field allows you to restrict web admin access only from defined IP subnets. ● **Any** - Allow web admin accesses to be from anywhere, without IP address restriction. ● **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:

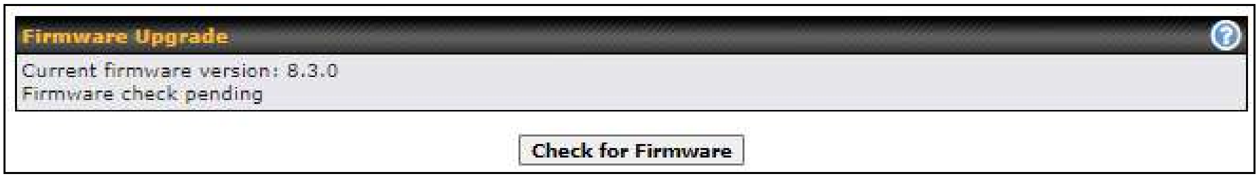
	The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., *192.168.0.0*), and *m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, *192.168.0.0/24*). To define multiple subnets, separate each IP subnet one in a line. For example: ● 192.168.0.0/24 ● 10.8.0.0/16
Allowed WAN IP Address(es)	This is to choose which WAN IP address(es) the web server should listen on.

28.2 Firmware

Web admin interface : automatically check for updates

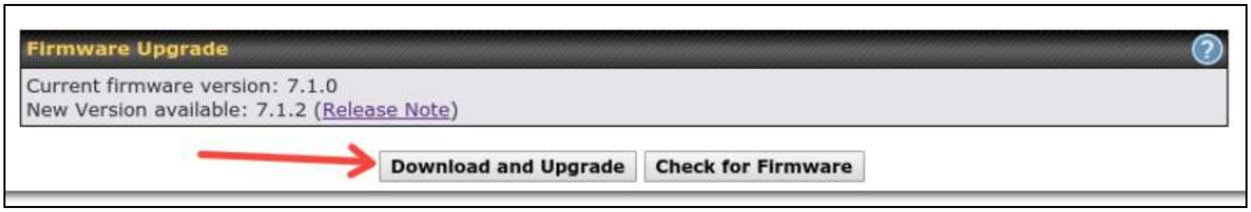
Upgrading firmware can be done in one of three ways.
Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

The automatic upgrade can be done from **System** > **Firmware**.



Current firmware version: 8.3.0
Firmware check pending

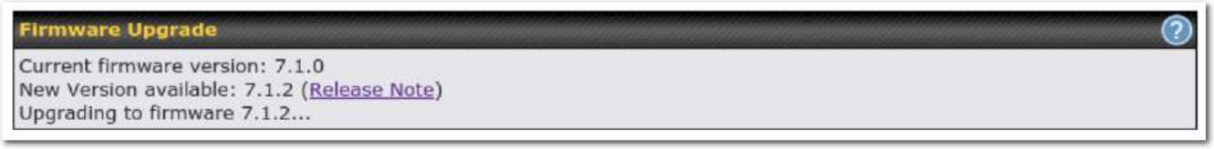
If an update is found the buttons will change to allow you to **Download and Update** the firmware.



Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)

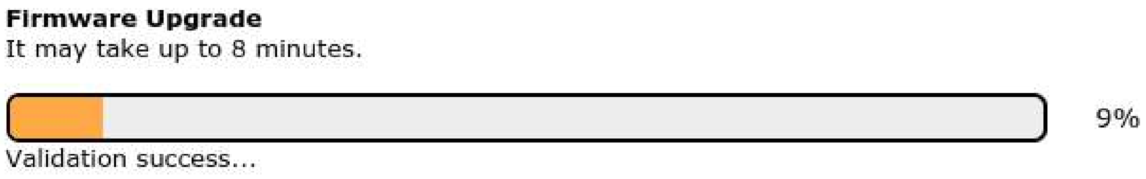
Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

The router will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)
Upgrading to firmware 7.1.2...

The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will also depend on the router that's being upgraded.



Firmware Upgrade
It may take up to 8 minutes.

9%

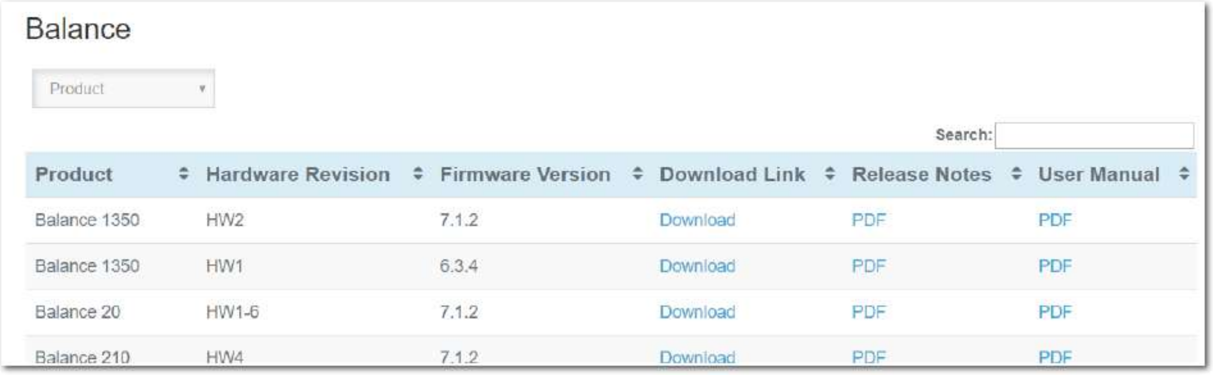
Validation success...

**Upgrading the firmware will cause the router to reboot.*

Web admin interface : install updates manually

In some cases, a special build may be provided via a ticket or it may be found in the forum. Upgrading to the special build can be done using this method, or using IC2 if you are using that to manage your firmware upgrades. A manual upgrade using the GA firmware posted on the site may also be recommended or required for a couple of reasons.

All of the Peplink/Pepwave GA firmware can be found here Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.



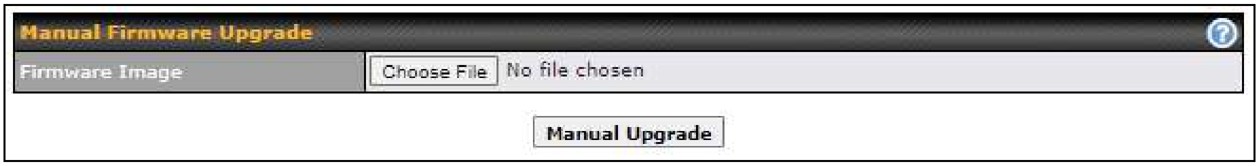
Balance

Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual
Balance 1350	HW2	7.1.2	Download	PDF	PDF
Balance 1350	HW1	6.3.4	Download	PDF	PDF
Balance 20	HW1-6	7.1.2	Download	PDF	PDF
Balance 210	HW4	7.1.2	Download	PDF	PDF

If the device has more than one firmware version the current hardware revision will be required to know what firmware to download.

Navigate to System > Firmware and click the Choose File button under the Manual Firmware Upgrade section. Navigate to the location that the firmware was downloaded to select the ".img" file and click the Open button.

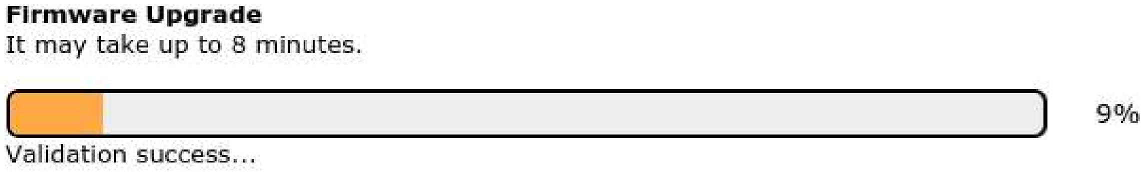
Click on the Manual Upgrade button to start the upgrade process.



Manual Firmware Upgrade	
Firmware Image	Choose File No file chosen

Manual Upgrade

A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the Ok button to start the upgrade process. The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will depend on the router that's being upgraded.



Firmware Upgrade
It may take up to 8 minutes.

9%

Validation success...

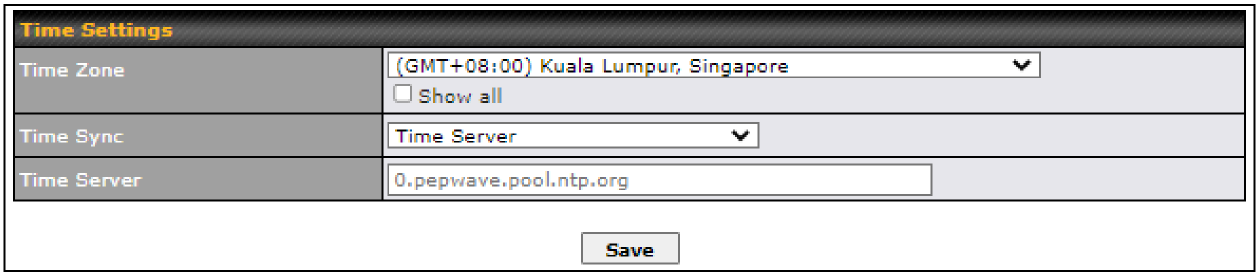
**Upgrading the firmware will cause the router to reboot.*

The InControl method

Described in this knowledgebase article on our forum.

28.3 Time

Time Settings enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System > Time**.



Time Settings	
Time Zone	(GMT+08:00) Kuala Lumpur, Singapore □ Show all
Time Sync	Time Server
Time Server	0.pepwave.pool.ntp.org

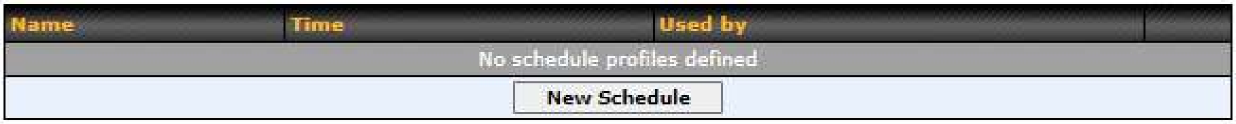
Save

Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The **Time Zone** value affects the time stamps in the Pepwave router's event log and e-mail notifications. Check **Show all** to show all time zone options.

Time Sync	This field allows to select your time sync mode, the available options are: ● Time Server ● GPS ● GPS with Time Server as fallback
Time Server	This setting specifies the NTP network time server to be utilized by the Pepwave router.

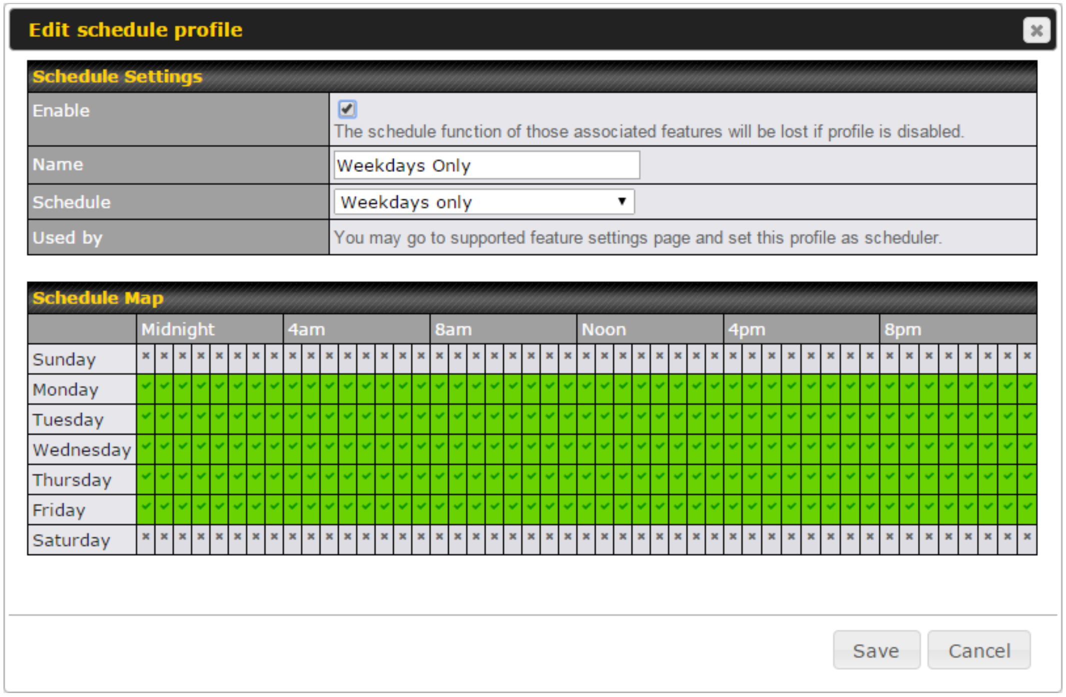
28.4 Schedule

Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**



Name	Time	Used by	
No schedule profiles defined			

Enable scheduling, and then click on your schedule name or on the **New Schedule** button to begin.



Edit schedule profile

Schedule Settings

Enable	☑ The schedule function of those associated features will be lost if profile is disabled.
Name	Weekdays Only
Schedule	Weekdays only ▾
Used by	You may go to supported feature settings page and set this profile as scheduler.

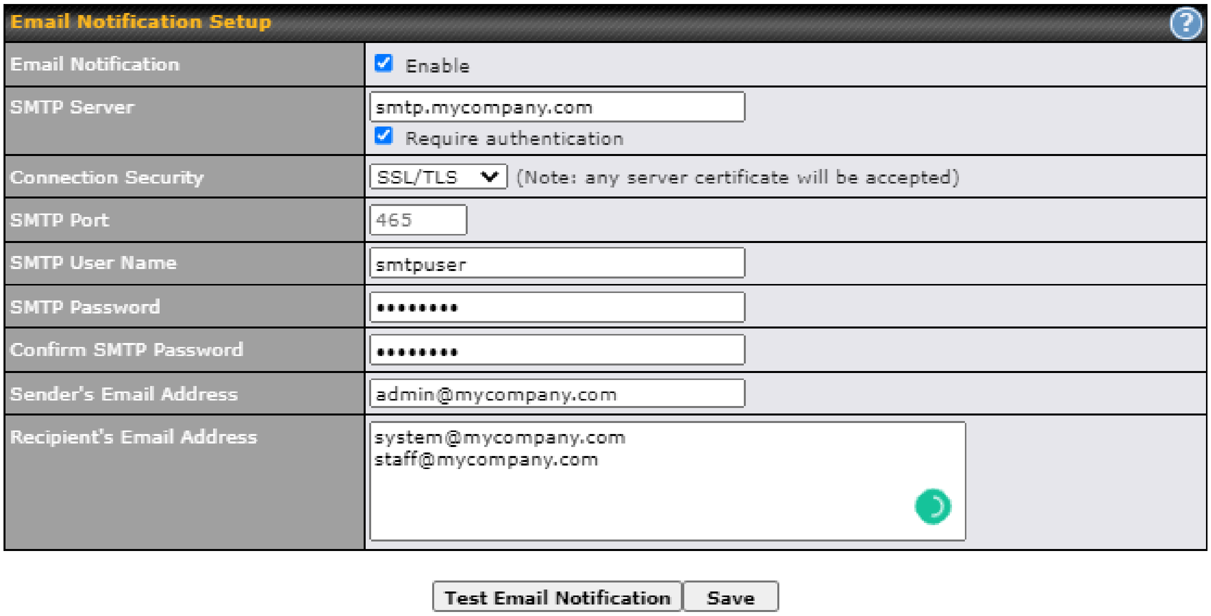
Schedule Map

	Midnight								4am								8am								Noon								4pm								8pm							
Sunday	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Monday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Saturday	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

Edit Schedule Profile	
Enabling	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
Name	Enter your desired name for this particular schedule profile.
Schedule	Click the drop-down menu to choose pre-defined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.
Schedule Map	Click on the desired times to enable features at that time period. You can hold your mouse for faster entry.

28.5 Email Notification

Email notification functionality provides a system administrator with up-to-date information on network status. The settings for configuring email notifications are found at **System>Email Notification**.

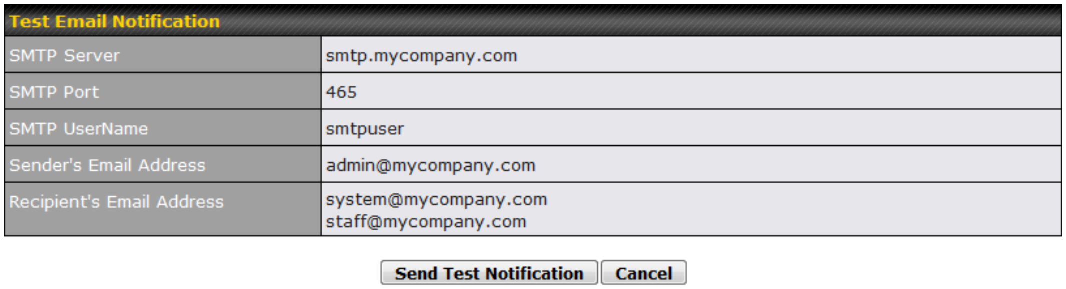


Email Notification Setup	
Email Notification	☑ Enable
SMTP Server	smtp.mycompany.com ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	smtpuser
SMTP Password	••••••••
Confirm SMTP Password	••••••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If **Enable** is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If **Enable** is not checked, email notification is disabled and the Pepwave router will not send email messages.

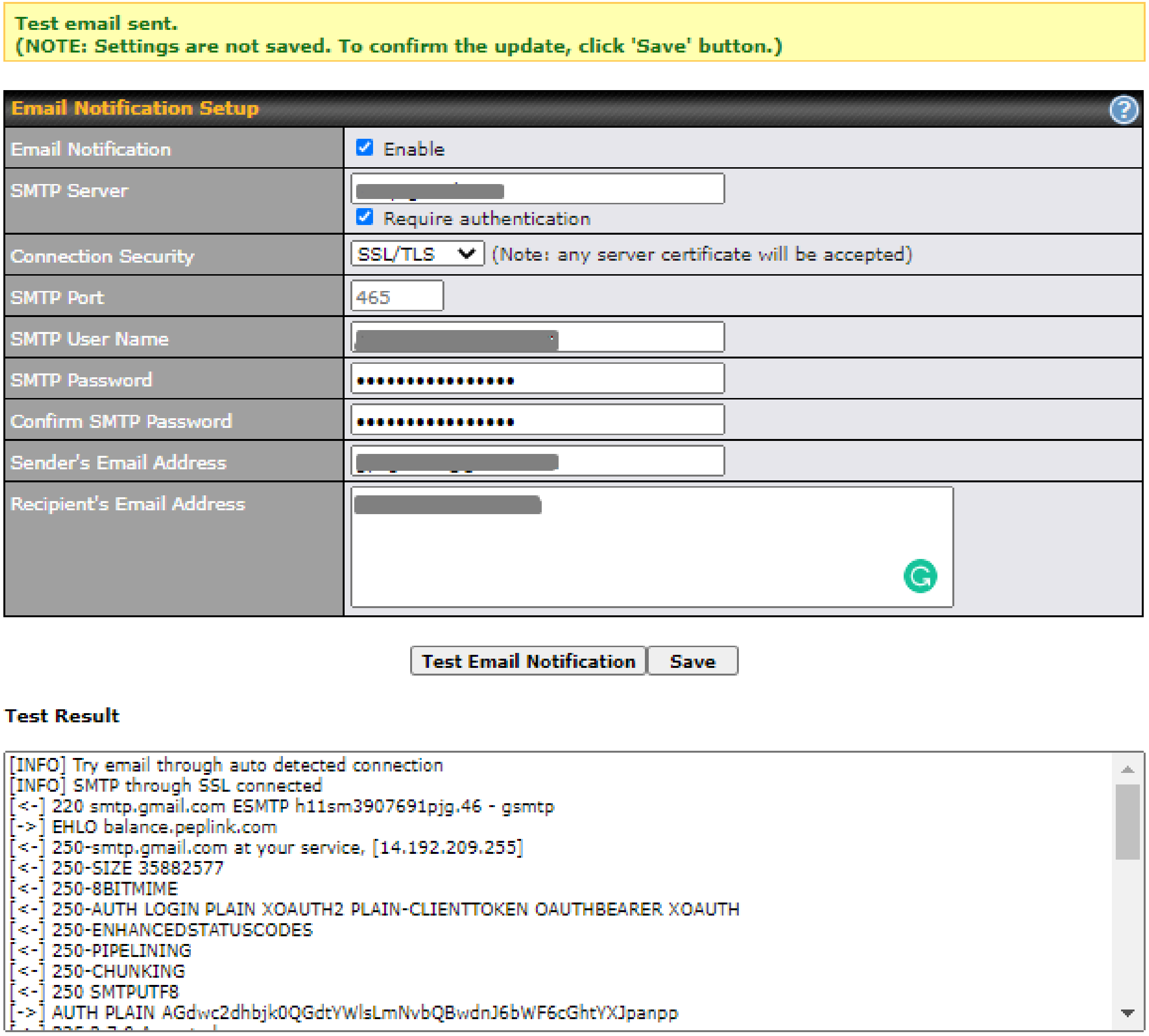
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check **Require authentication**.
Connection Security	This setting specifies via a drop-down menu one of the following valid Connection Security: ● None ● STARTTLS ● SSL/TLS
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to **25**. If Connection Security is selected "**STARTTLS**", the default port number will be set to **587**. If Connection Security is selected "**SSL/TLS**", the default port number will be set to **465**. You may customize the port number by editing this field.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if **Require authentication** is checked in the **SMTP Server** setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address the Pepwave router will use to send reports.
Recipient's Email Address	This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.

After you have finished setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is clicked, you will see this screen to confirm the settings:



Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Click **Send Test Notification** to confirm. In a few seconds, you will see a message with detailed test results.



Test email sent.
(NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

Email Notification Setup

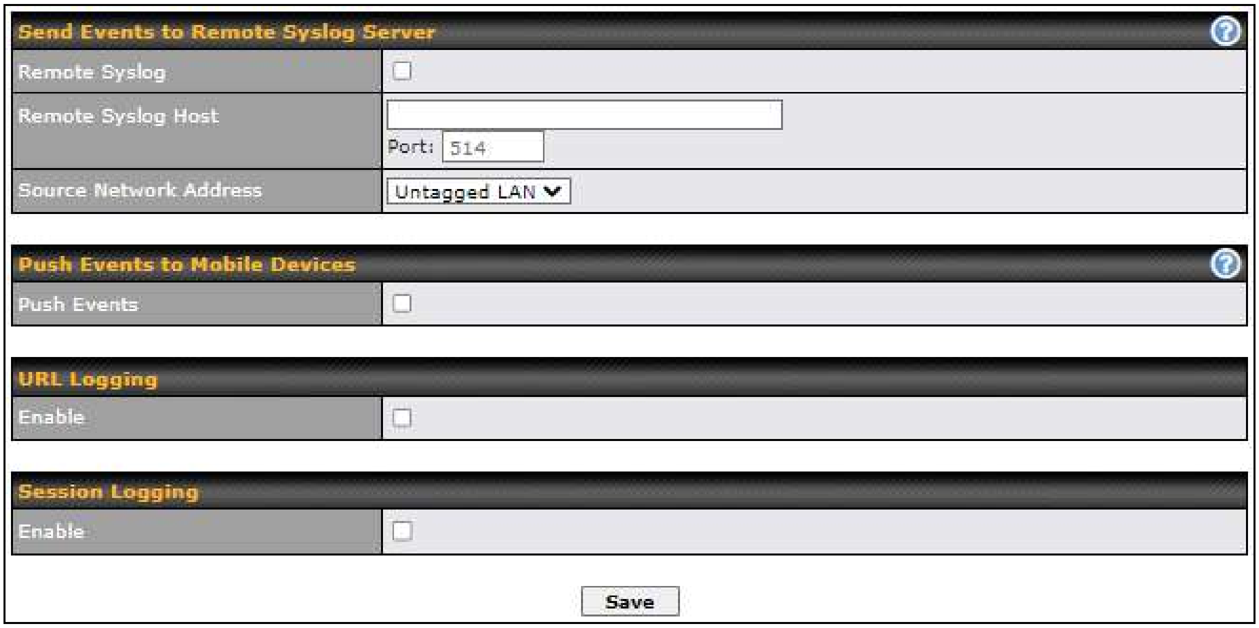
Email Notification	☑ Enable
SMTP Server	[redacted] ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	[redacted]
SMTP Password	••••••••••••••••
Confirm SMTP Password	••••••••••••••••
Sender's Email Address	[redacted]
Recipient's Email Address	[redacted]

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
[<-] 220 smtp.gmail.com ESMTP h11sm3907691pjg.46 - gsmtp
[->] EHLO balance.peplink.com
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]
[<-] 250-SIZE 35882577
[<-] 250-8BITMIME
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
[<-] 250-ENHANCEDSTATUSCODES
[<-] 250-PIPELINING
[<-] 250-CHUNKING
[<-] 250 SMTPUTF8
[->] AUTH PLAIN AGdwc2dhbjk0QGdtYWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

28.6 Event Log

Event log functionality enables event logging at a specified remote syslog server. The settings for configuring the remote system log can be found at **System > Event Log**.



Send Events to Remote Syslog Server

Remote Syslog	□
Remote Syslog Host	Port: 514
Source Network Address	Untagged LAN

Push Events to Mobile Devices

Push Events	□

URL Logging

Enable	□

Session Logging

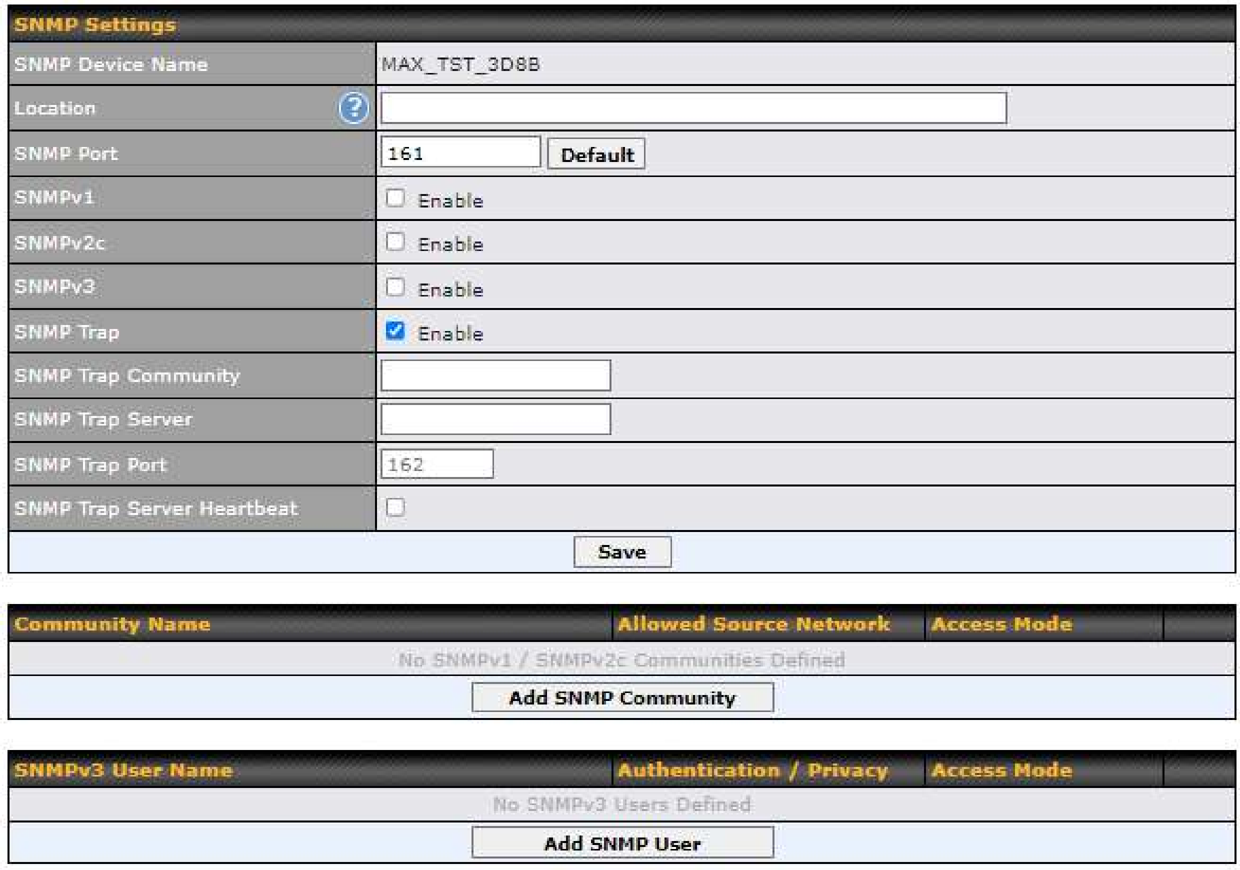
Enable	□

Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Source Network Address	Via drop-down list, you may choose the LAN interface for Event Log, URL Logging, Sessions Logging and RADIUS.
Push Events	The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.

Session Logging	This setting is to enable event logging at the specified log server.
Session Logging Host	This setting specifies the IP address or hostname of the Session log server.
peplink PEPWAVE	For more information on the Router Utility, go to: www.peplink.com/products/router-utility

28.7 SNMP

SNMP or simple network management protocol is an open standard that can be used to collect information about the Pepwave router. SNMP configuration is located at **System > SNMP**.



SNMP Settings	
SNMP Device Name	MAX_TST_3D8B
Location ?	
SNMP Port	161 Default
SNMPv1	□ Enable
SNMPv2c	□ Enable
SNMPv3	□ Enable
SNMP Trap	☑ Enable
SNMP Trap Community	
SNMP Trap Server	
SNMP Trap Port	162
SNMP Trap Server Heartbeat	□
Save	

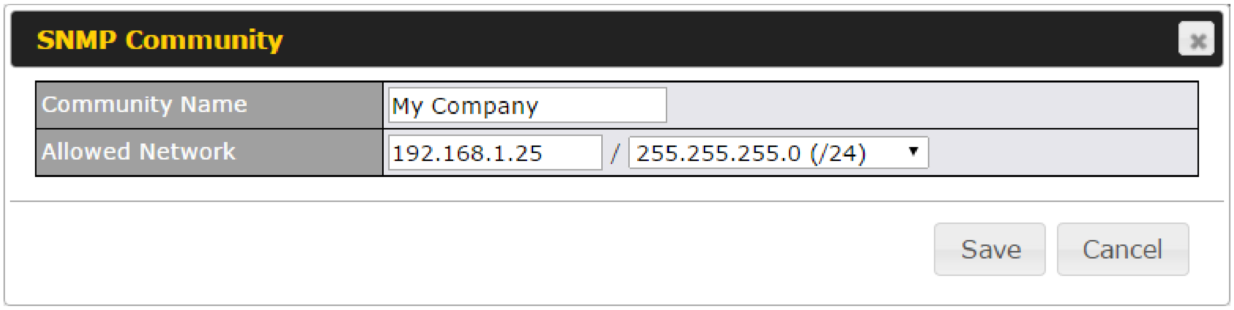
Community Name	Allowed Source Network	Access Mode	
No SNMPv1 / SNMPv2c Communities Defined			
Add SNMP Community			

SNMPv3 User Name	Authentication / Privacy	Access Mode	
No SNMPv3 Users Defined			
Add SNMP User			

SNMP Settings	
SNMP Device	This field shows the router name defined at **System > Admin Security**.

Name	
SNMP Port	This option specifies the port which SNMP will use. The default port is **161**.
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.
SNMP Trap	This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear.
SNMP Trap Community	This setting specifies the SNMP Trap community name.
SNMP Trap Server	Enter the IP address of the SNMP Trap server.
SNMP Trap Port	This option specifies the port which the SNMP Trap server will use. The default port is **162**.
SNMP Trap Server Heartbeat	This option allows you to enable and configure the heartbeat interval for the SNMP Trap server.

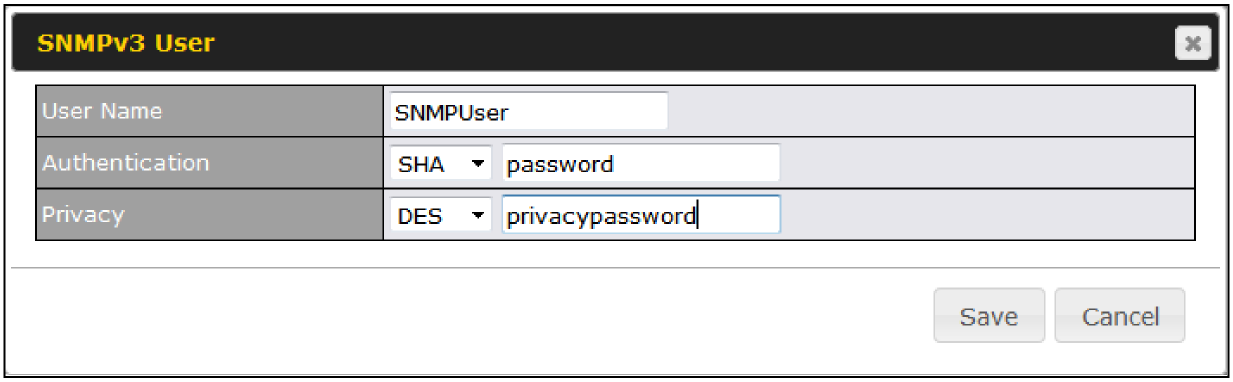
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:


SNMP Community

Community Name	My Company
Allowed Network	192.168.1.25 / 255.255.255.0 (/24)

SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.
Allowed Source Subnet Address	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., *192.168.1.0*) and select the appropriate subnet mask.

To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:



SNMPv3 User

User Name	SNMPUser
Authentication	SHA ▾ password
Privacy	DES ▾ privacypassword

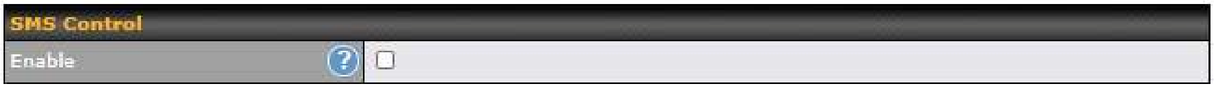
SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: ● NONE ● MD5 ● SHA When MD5 or SHA is selected, an entry field will appear for the password.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: ● NONE ● DES When DES is selected, an entry field will appear for the password.

28.8 SMS Control

SMS Control allows the user to control the device using SMS even if the modem does not have a data connection. The settings for configuring the SMS Control can be found at **System > SMS Control**.

Supported Models

- **Balance/MAX**: *-LTE-E, *-LTEA-W, *-LTEA-P, *-LTE-MX
- **EPX**: *-LW*, *-LP*



SMS Control

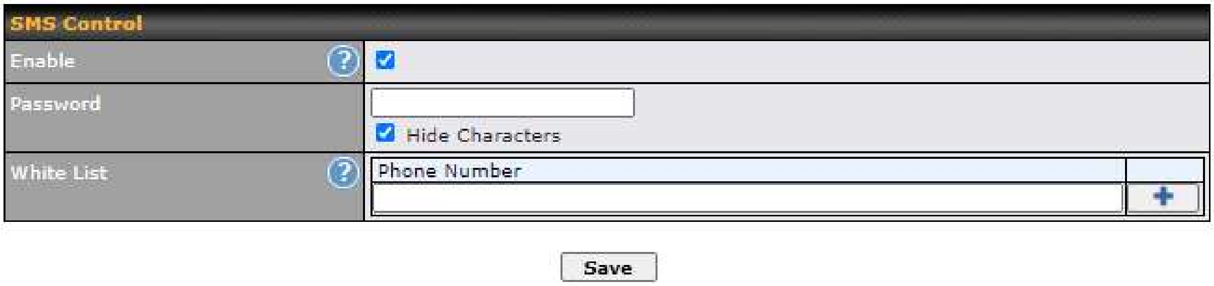
Enable	□

When this box is checked, the device will be allowed to take actions according to received commands via SMS.

Make sure your mobile plan supports SMS, and note that some plans may incur additional charges for this.

SMS Control can reboot devices and configure cellular settings over signalling channels, even if the modem does not have a data connection.

For details of supported SMS command sets, please refer to our knowledge base.

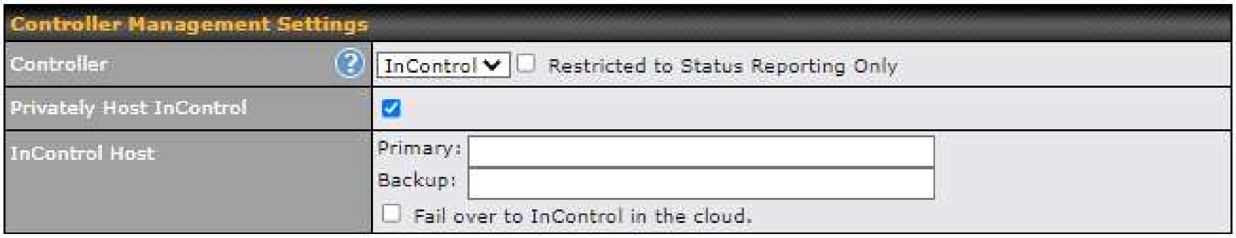


SMS Control

Enable	☑
Password	☑ Hide Characters
White List	Phone Number

SMS Control Settings	
Enable	Click the checkbox to enable the SMS Control.
Password	This setting sets the password for authentication - maximum of 32 characters, which cannot include semicolon (;).
White List	Optionally, you can add phone number(s) to the whitelist. Only matching phone numbers are allowed to issue SMS commands. Phone numbers must be in the E.164 International Phone Numbers format.

28.9 InControl



Controller Management Settings

Controller	InControl □ Restricted to Status Reporting Only
Privately Host InControl	☑
InControl Host	Primary: Backup: □ Fail over to InControl in the cloud.

InControl is a cloud-based service which allows you to manage all of your Peplink and Pepwave devices with one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

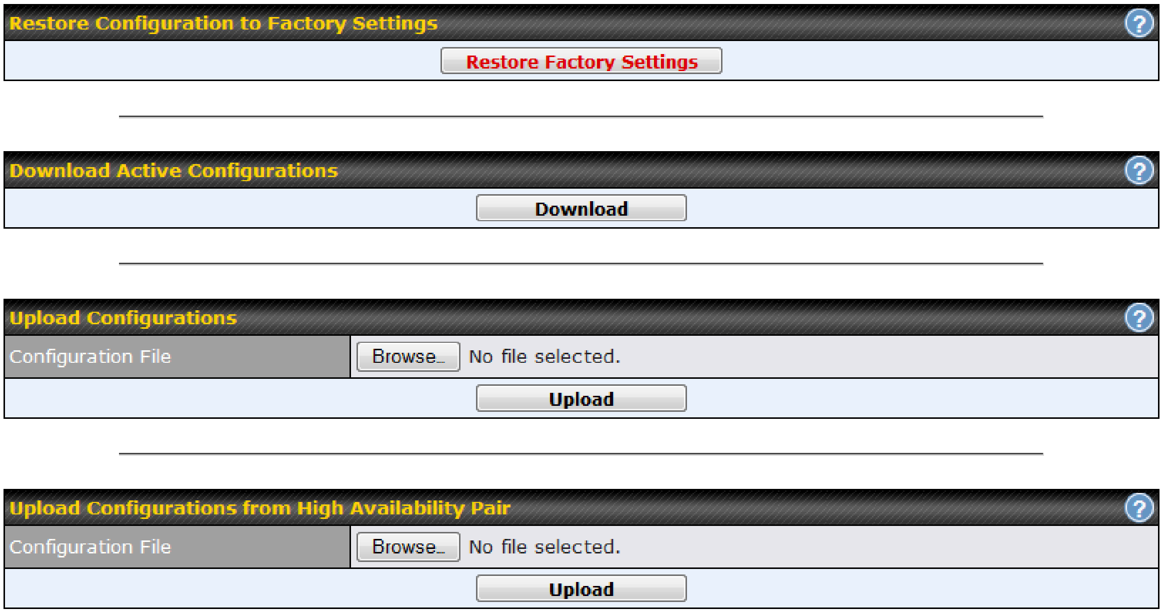
When this check box is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

Alternatively, you can also privately host InControl. Simply check the “Privately Host InControl” box and enter the IP Address of your InControl Host. If you have multiple hosts, you may enter the primary and backup IP addresses for the InControl Host and tick the “Fail over to InControl in the cloud” box. The device will connect to either the primary InControl Host or the secondary/backup ICA/IC2.

You can sign up for an InControl account at https://incontrol2.peplink.com/. You can register your devices under the account, monitor their status, see their usage reports, and receive offline notifications.

28.10 Configuration

Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System > Configuration**. Note that available options vary by model.


Restore Configuration to Factory Settings
Restore Factory Settings
Download Active Configurations
Download
Upload Configurations
Upload
Upload Configurations from High Availability Pair
Upload

Configuration File: Browse... No file selected.

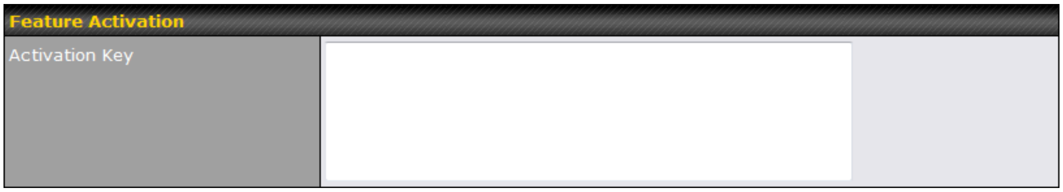
Configuration File: Browse... No file selected.

Configuration	
Restore Configuration to	The **Restore Factory Settings** button is to reset the configuration to factory default settings. After clicking the button, you will need to click the **Apply**

Factory Settings	**Changes** button on the top right corner to make the settings effective.
Download Active Configurations	Click **Download** to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click **Choose File** to locate the configuration file on the local computer, and then click **Upload**. The new settings can then be applied by clicking the **Apply Changes** button on the page header, or you can cancel the procedure by pressing **discard** on the main page of the web admin interface.
Upload Configurations from High Availability Pair	In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the **Upload** button. After loading the settings, configure the LAN IP address of the Pepwave router so that it is different from the HA counterpart.

28.11 Feature Add-ons

Some Pepwave routers have features that can be activated upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**, and then click **Apply Changes**.

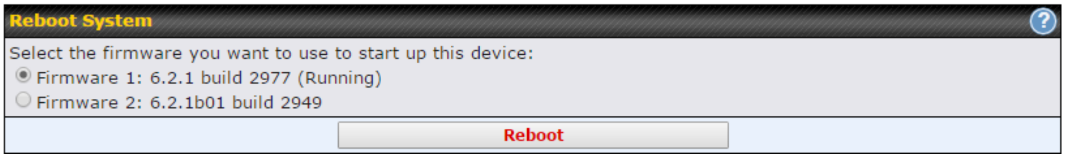

Feature Activation

Activation Key	

28.12 Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Pepwave router can equip with two copies of firmware. Each copy can be a different version. You can select the firmware version you would like to reboot the device with. The firmware marked with **(Running)** is the current system boot up firmware.

Please note that a firmware upgrade will always replace the inactive firmware partition.


Reboot System

Select the firmware you want to use to start up this device:

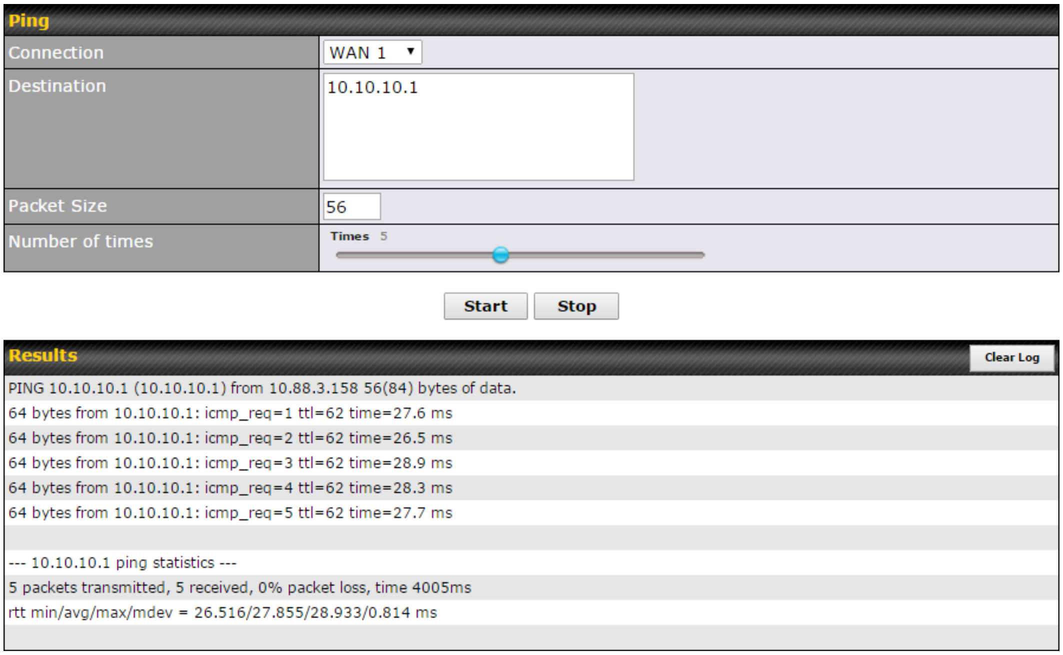
● Firmware 1: 6.2.1 build 2977 (Running)

○ Firmware 2: 6.2.1b01 build 2949

29 Tools

29.1 Ping

The ping test tool sends pings through a specific Ethernet interface or a SpeedFusion^{TM} VPN connection. You can specify the number of pings in the field **Number of times**, to a maximum number of 10 times. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System > Tools > Ping,** illustrated below:



Ping

Connection	WAN 1
Destination	10.10.10.1
Packet Size	56
Number of times	Times 5

Results

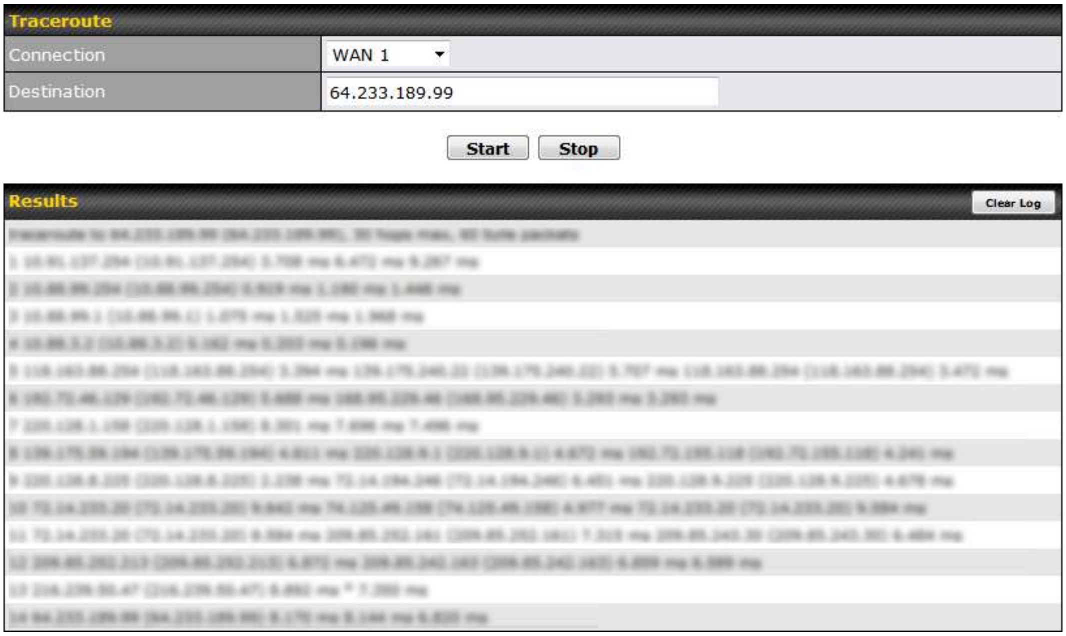
```
PING 10.10.10.1 (10.10.10.1) from 10.88.3.158 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_req=1 ttl=62 time=27.6 ms
64 bytes from 10.10.10.1: icmp_req=2 ttl=62 time=26.5 ms
64 bytes from 10.10.10.1: icmp_req=3 ttl=62 time=28.9 ms
64 bytes from 10.10.10.1: icmp_req=4 ttl=62 time=28.3 ms
64 bytes from 10.10.10.1: icmp_req=5 ttl=62 time=27.7 ms

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 26.516/27.855/28.933/0.814 ms
```

Tip

A system administrator can use the ping utility to manually check the connectivity of a particular LAN/WAN connection.

29.2 Traceroute Test

The traceroute test tool traces the routing path to the destination through a particular Ethernet interface or a SpeedFusion^{TM} connection. The traceroute test utility is located at **System > Tools > Traceroute**.



Traceroute

Connection	WAN 1 ▾
Destination	64.233.189.99

Results

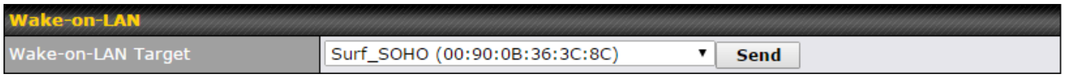
```
[illegible]
1 [illegible]
2 [illegible]
3 [illegible]
4 [illegible]
5 [illegible]
6 [illegible]
7 [illegible]
8 [illegible]
9 [illegible]
10 [illegible]
11 [illegible]
12 [illegible]
13 [illegible]
14 [illegible]
```

Tip

A system administrator can use the traceroute utility to analyze the connection path of a LAN/WAN connection.

29.3 Wake-on-LAN

Pepwane routers can send special "magic packets" to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**



Wake-on-LAN

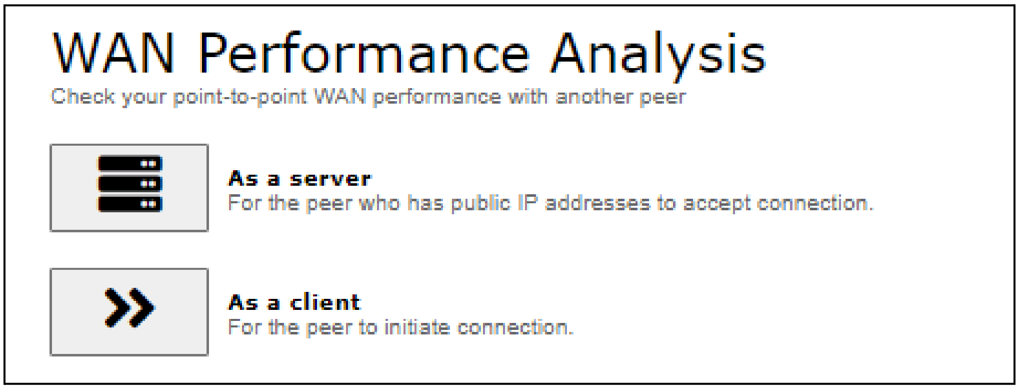
Wake-on-LAN Target	Surf_SOHO (00:90:0B:36:3C:8C) ▾

Select a client from the drop-down list and click **Send** to send a "magic packet"

29.4 WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speed test between 2 Peplink devices .

You can set a device up as a **Server** or a **Client**. One device must be set up as a server to run the speed tests and the server must have a public IP address.



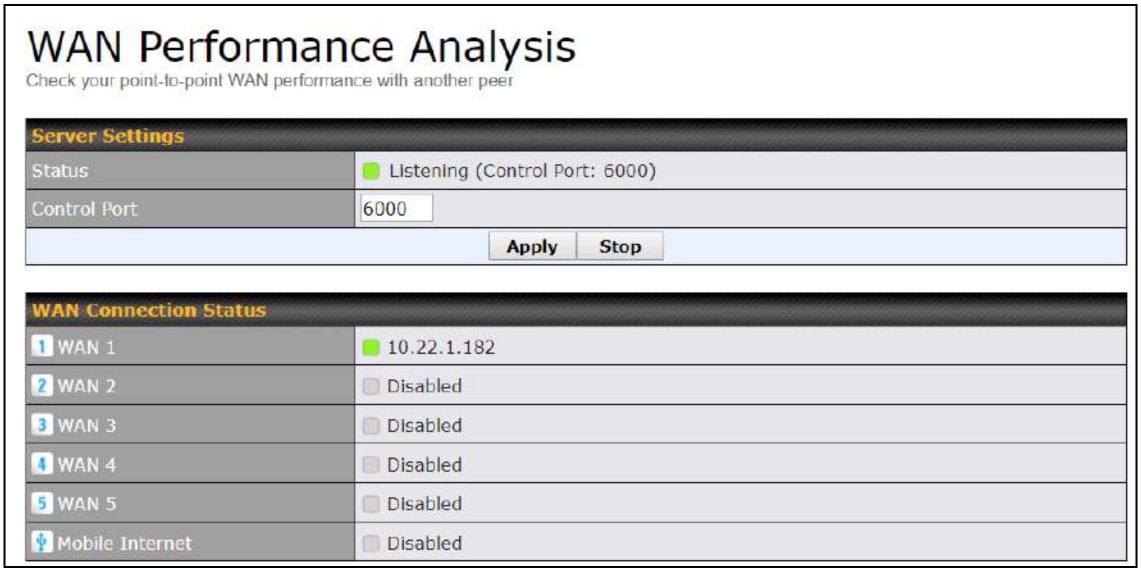
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

As a server
For the peer who has public IP addresses to accept connection.

As a client
For the peer to initiate connection.

The default port is 6000 and can be changed if required. The IP address of the WAN interface will be shown in the **WAN Connection Status** section.



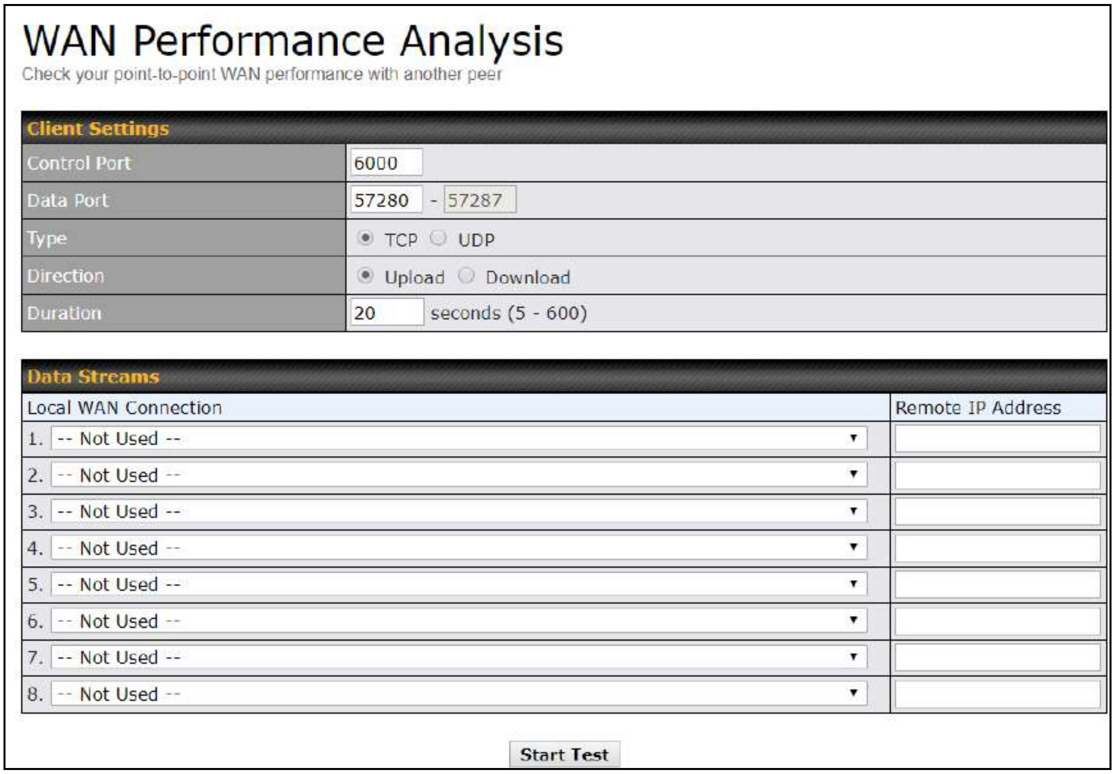
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

Server Settings	
Status	🟩 Listening (Control Port: 6000)
Control Port	6000

WAN Connection Status	
1 WAN 1	🟩 10.22.1.182
2 WAN 2	□ Disabled
3 WAN 3	□ Disabled
4 WAN 4	□ Disabled
5 WAN 5	□ Disabled
Mobile Internet	□ Disabled

The client side has a few more settings that can be changed. Make sure that the **Control Port** matches what's been entered on the server side. Select the WAN(s) that will be used for testing and enter the Servers WAN IP address. Once all of the options have been set, click the **Start Test** button.



WAN Performance Analysis

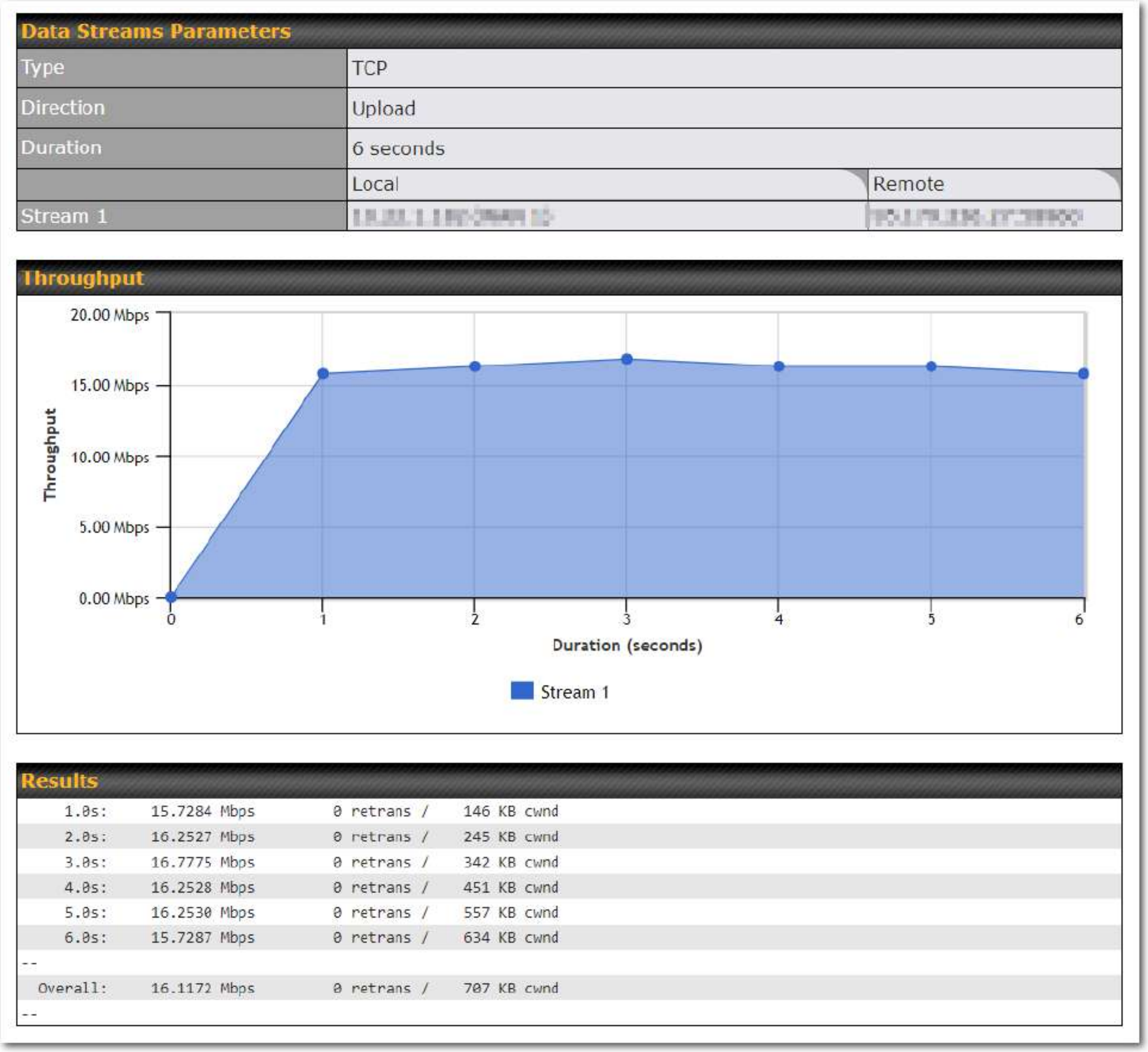
Check your point-to-point WAN performance with another peer

Client Settings	
Control Port	6000
Data Port	57280 - 57287
Type	● TCP ○ UDP
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

Data Streams

Local WAN Connection	Remote IP Address
1. -- Not Used --	
2. -- Not Used --	
3. -- Not Used --	
4. -- Not Used --	
5. -- Not Used --	
6. -- Not Used --	
7. -- Not Used --	
8. -- Not Used --	

The test output will show the **Data Streams Parameters**, the **Throughput** as a graph, and the **Results**.



Data Streams Parameters

Type	TCP	
Direction	Upload	
Duration	6 seconds	
	Local	Remote
Stream 1	[redacted]	[redacted]

Throughput

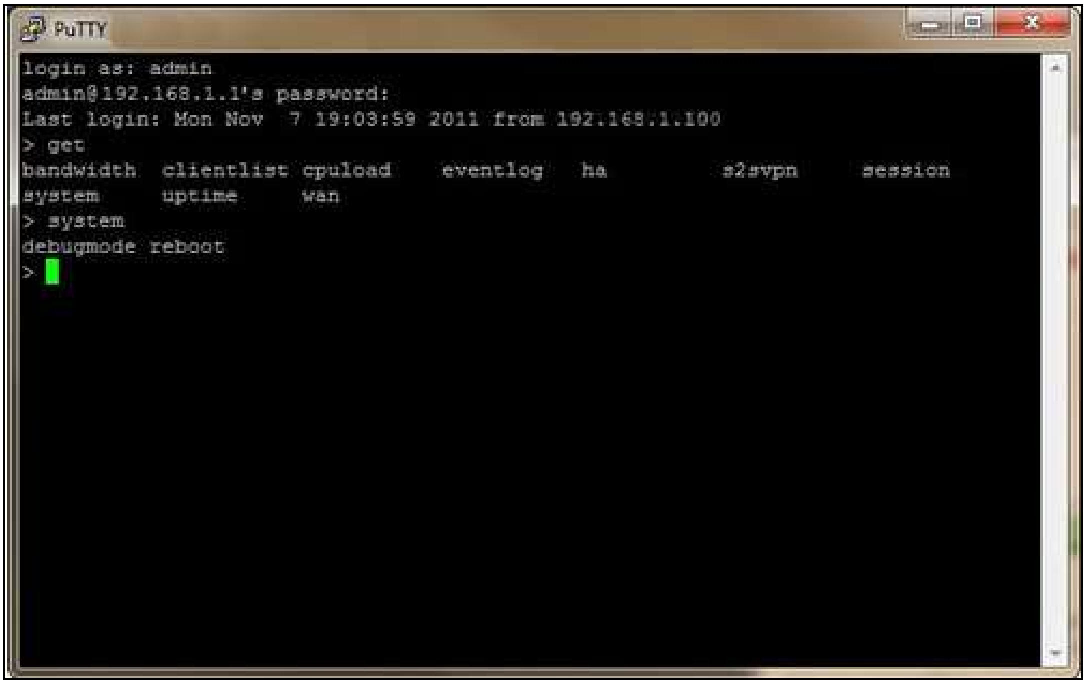
Results

```
     1.0s:    15.7284 Mbps        0 retrans /    146 KB cwnd
     2.0s:    16.2527 Mbps        0 retrans /    245 KB cwnd
     3.0s:    16.7775 Mbps        0 retrans /    342 KB cwnd
     4.0s:    16.2528 Mbps        0 retrans /    451 KB cwnd
     5.0s:    16.2530 Mbps        0 retrans /    557 KB cwnd
     6.0s:    15.7287 Mbps        0 retrans /    634 KB cwnd
--
  Overall:    16.1172 Mbps        0 retrans /    707 KB cwnd
--
```

The test can be run again once it's complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

29.5 CLI (Command Line Interface Support)

The CLI (command line interface) can be accessed via SSH. This field enables CLI support. The below settings specify which TCP port and which interface(s) should accept remote SSH CLI access. The user name and password used for remote SSH CLI access are the same as those used for web admin access.

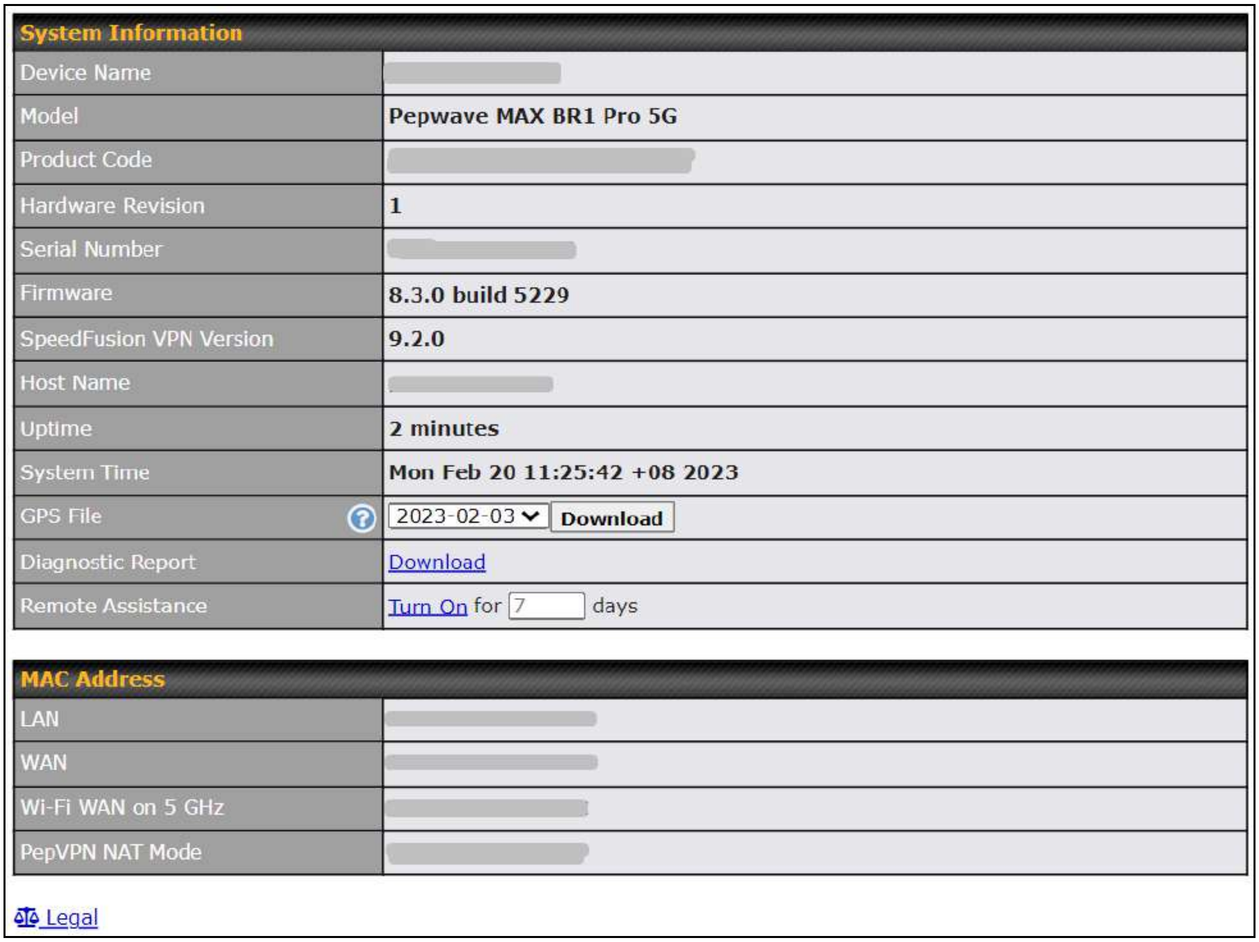


```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist cpuload    eventlog   ha         s2svpn     session
system     uptime     wan
> system
debugmode reboot
> 
```

30 Status

30.1 Device

System information is located at **Status > Device**.



System Information	
Device Name	[redacted]
Model	Pepwave MAX BR1 Pro 5G
Product Code	[redacted]
Hardware Revision	1
Serial Number	[redacted]
Firmware	8.3.0 build 5229
SpeedFusion VPN Version	9.2.0
Host Name	[redacted]
Uptime	2 minutes
System Time	Mon Feb 20 11:25:42 +08 2023
GPS File ?	2023-02-03 ▾ Download
Diagnostic Report	Download
Remote Assistance	Turn On for 7 days

MAC Address	
LAN	[redacted]
WAN	[redacted]
Wi-Fi WAN on 5 GHz	[redacted]
PepVPN NAT Mode	[redacted]

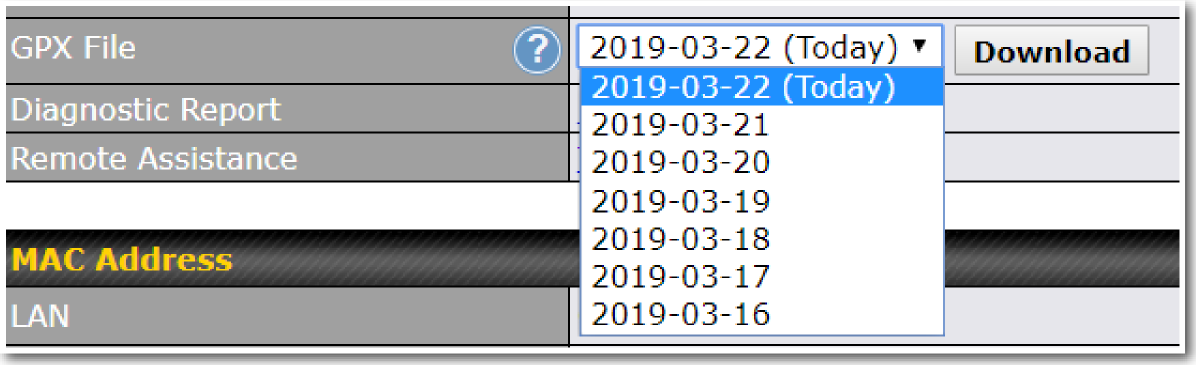
⚖ Legal

System Information	
Device Name	This is the name specified in the **Device Name** field located at **System > Admin Security**.
Model	This shows the model name and number of this device.
Product Code	If your model uses a product code, it will appear here.
Hardware Revision	This shows the hardware version of this device.

Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
SpeedFusion VPN Version	This shows the current SpeedFusion VPN version.
Modem Support Version	This shows the modem support version. For a list of supported modems, click **Modem Support List**.
InControl Managed Configuration	InControl Managed Configurations (firmware, VLAN, Captive Portal, etcetera)
Host Name	The host name assigned to the Pepwave router appears here.
Uptime	This shows the length of time since the device has been rebooted.
System Time	This shows the current system time.
OpenVPN Client Profile	Link to download OpenVpn Client profile when this is enabled in Remote User Access
Diagnostic Report	The **Download** link is for exporting a diagnostic report file required for system investigation.
Remote Assistance	This option is to **Turn on** remote assistance with the time duration.

The second table shows the MAC address of each LAN/WAN interface connected. To view your device's End User License Agreement (EULA), click ⚖ Legal.

30.2 GPS Data



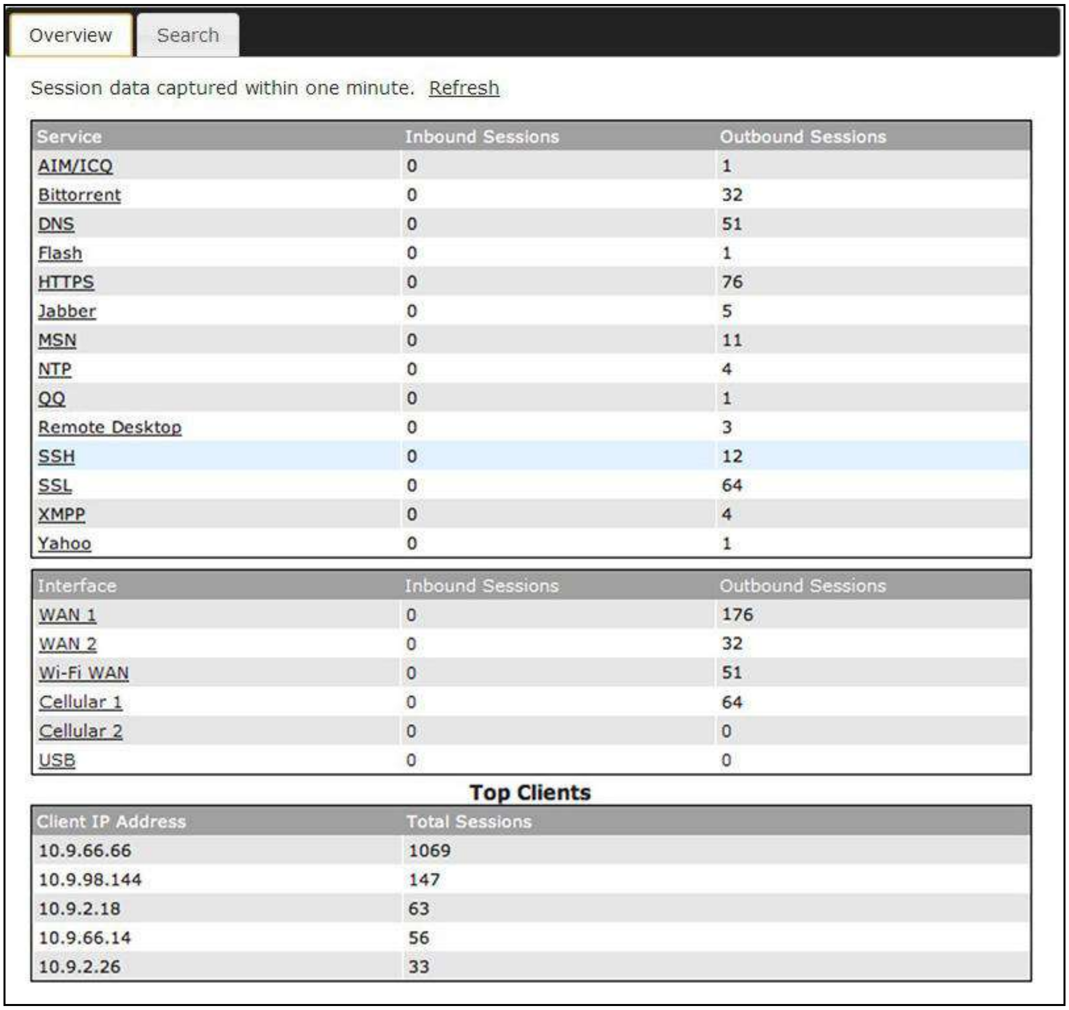
GPX File: 2019-03-22 (Today)

GPS enabled models automatically store up to seven days of GPS location data in GPS eXchange format (GPX). To review this data using third-party applications, click **Status > Device** and then download your GPX file.

The Pepwave GPS enabled devices export real-time location data in NMEA format through the LAN IP address at TCP port 60660. It is accessible from the LAN or over a SpeedFusion connection. To access the data via a virtual serial port, install a virtual serial port driver. Visit http://www.peplink.com/index.php?view=faq&id=294 to download the driver.

30.3 Active Sessions

Information on active sessions can be found at **Status > Active Sessions > Overview.**



Session data captured within one minute. Refresh

Service	Inbound Sessions	Outbound Sessions
AIM/ICQ	0	1
Bittorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1

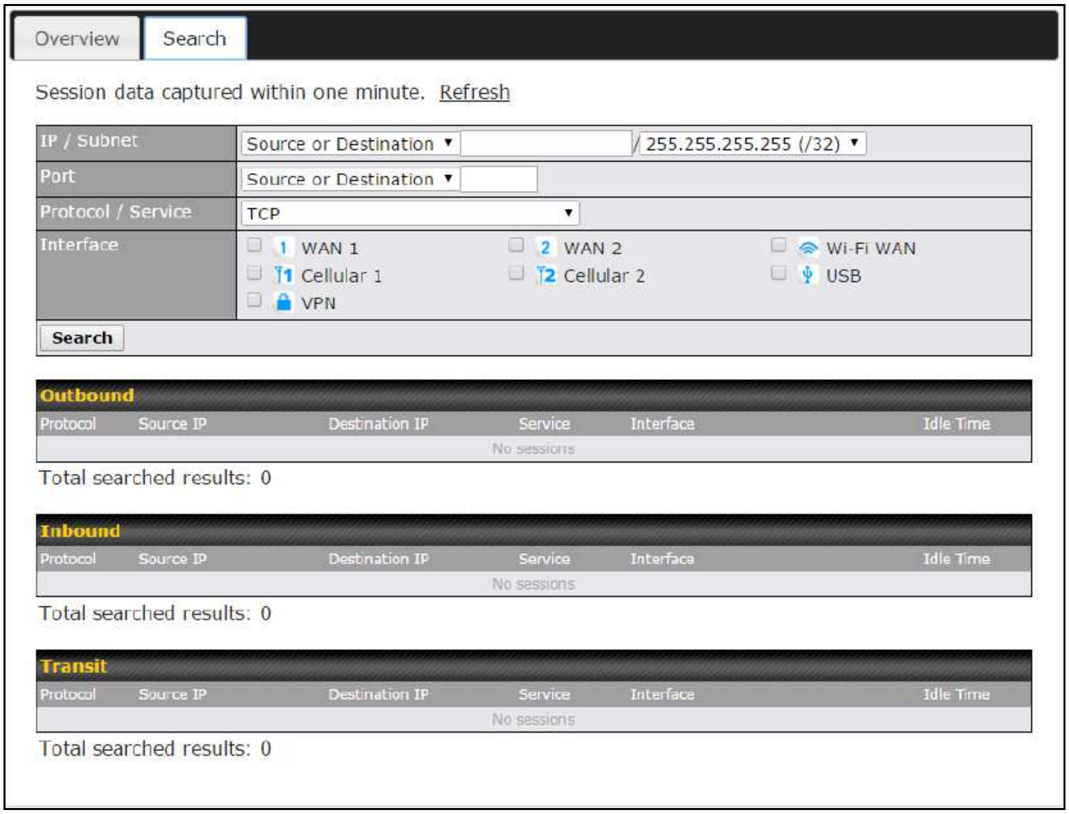
Interface	Inbound Sessions	Outbound Sessions
WAN 1	0	176
WAN 2	0	32
Wi-Fi WAN	0	51
Cellular 1	0	64
Cellular 2	0	0
USB	0	0

Top Clients

Client IP Address	Total Sessions
10.9.66.66	1069
10.9.98.144	147
10.9.2.18	63
10.9.66.14	56
10.9.2.26	33

This screen displays the number of sessions initiated by each application. Click on each service listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. In addition, you can see which clients are initiating the most sessions.

You can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to **Status > Active Sessions > Search**.



Overview | Search

Session data captured within one minute. Refresh

IP / Subnet	Source or Destination ▾ / 255.255.255.255 (/32) ▾
Port	Source or Destination ▾
Protocol / Service	TCP ▾
Interface	□ 1 WAN 1 □ 2 WAN 2 □ Wi-Fi WAN □ Cellular 1 □ Cellular 2 □ USB □ VPN

Search

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
		No sessions			

Total searched results: 0

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
		No sessions			

Total searched results: 0

Transit

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
		No sessions			

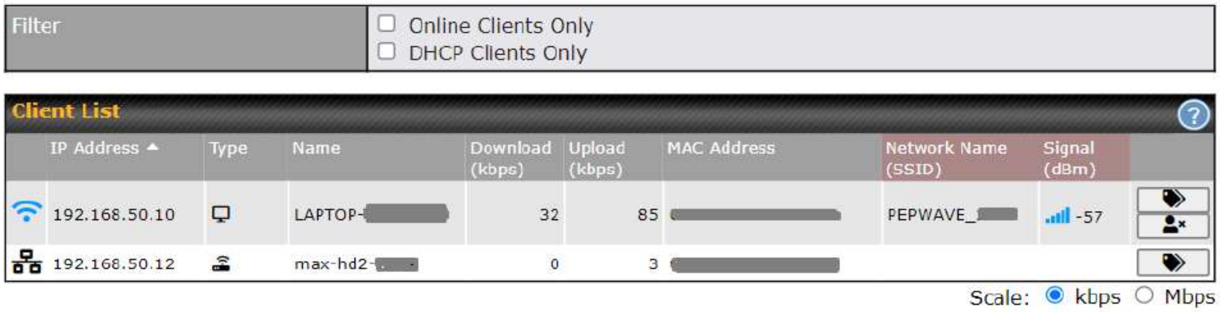
Total searched results: 0

This **Active Sessions** section displays the active inbound/outbound sessions of each WAN connection on the Pepwave router. A filter is available to sort active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

30.4 Client List

The client list table is located at **Status > Client List**. It lists DHCP and online client IP addresses**,** names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address.

Clients can be imported into the DHCP reservation table by clicking the button on the right. You can update the record after import by going to **Network > LAN**.



Filter	☐ Online Clients Only ☐ DHCP Clients Only

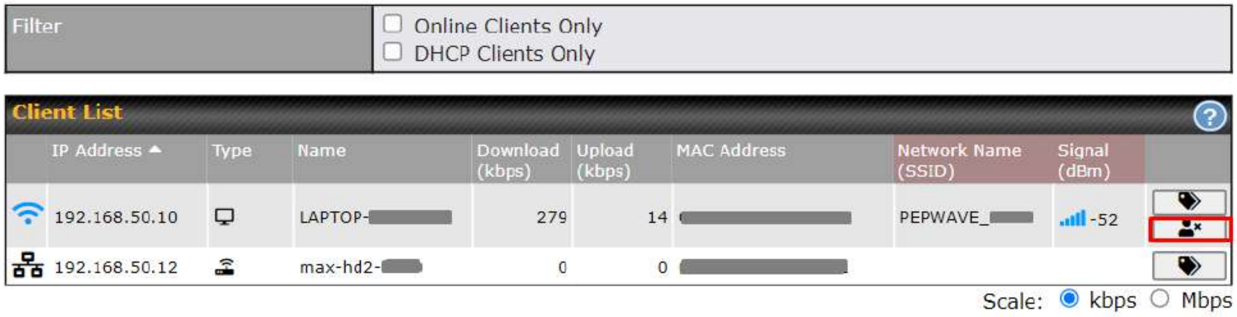
Client List

IP Address ▲	Type	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)
192.168.50.10		LAPTOP-[redacted]	32	85	[redacted]	PEPWAVE_[redacted]	-57
192.168.50.12		max-hd2-[redacted]	0	3	[redacted]		

Scale: ● kbps ○ Mbps

If the PPTP server (see **Section 19.2),** SpeedFusion^{TM} (see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

In the client list table, there is a "Ban Client" feature which is used to disconnect the Wi-Fi and Remote User Access clients by clicking the button on the right.



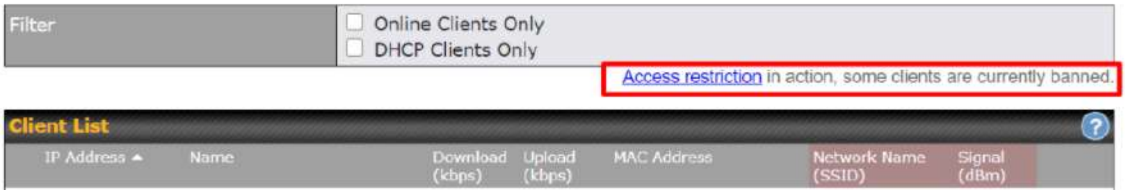
Filter	☐ Online Clients Only ☐ DHCP Clients Only

Client List

IP Address ▲	Type	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)
192.168.50.10		LAPTOP-[redacted]	279	14	[redacted]	PEPWAVE_[redacted]	-52
192.168.50.12		max-hd2-[redacted]	0	0	[redacted]		

Scale: ● kbps ○ Mbps

There is a blocklist on the same page after you banned the Wi-Fi or Remote User Access clients.



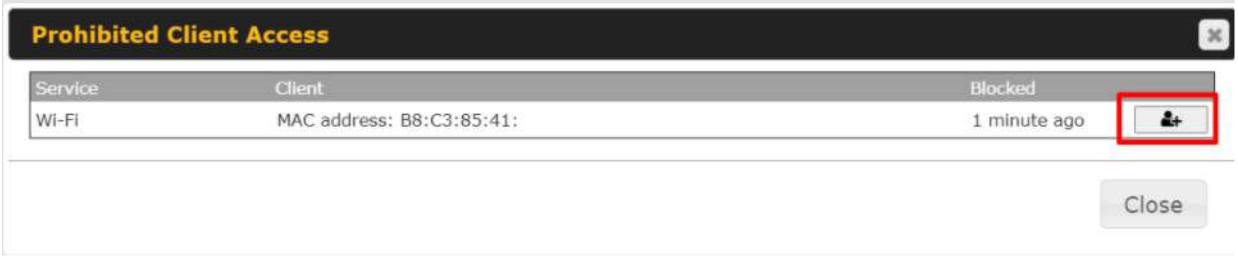
Filter	☐ Online Clients Only ☐ DHCP Clients Only

Access restriction in action, some clients are currently banned.

Client List

IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)

You may also unblock the Wi-Fi or Remote User Access clients when the client devices need to reconnect the network by clicking 👤+ the button on the right.

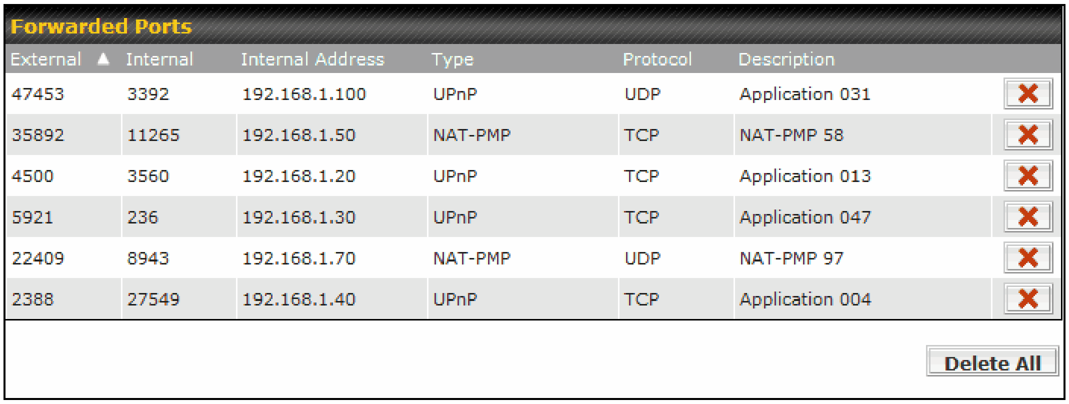


Prohibited Client Access

Service	Client	Blocked	
Wi-Fi	MAC address: B8:C3:85:41:	1 minute ago	👤+

30.5 UPnP / NAT-PMP

The table that shows the forwarded ports under UPnP and NAT-PMP protocols is located at **Status > UPnP/NAT-PMP**. This section appears only if you have enabled UPnP / NAT-PMP as mentioned in **Section 16.1.1**.



Forwarded Ports

External ▲	Internal	Internal Address	Type	Protocol	Description	
47453	3392	192.168.1.100	UPnP	UDP	Application 031	✖
35892	11265	192.168.1.50	NAT-PMP	TCP	NAT-PMP 58	✖
4500	3560	192.168.1.20	UPnP	TCP	Application 013	✖
5921	236	192.168.1.30	UPnP	TCP	Application 047	✖
22409	8943	192.168.1.70	NAT-PMP	UDP	NAT-PMP 97	✖
2388	27549	192.168.1.40	UPnP	TCP	Application 004	✖

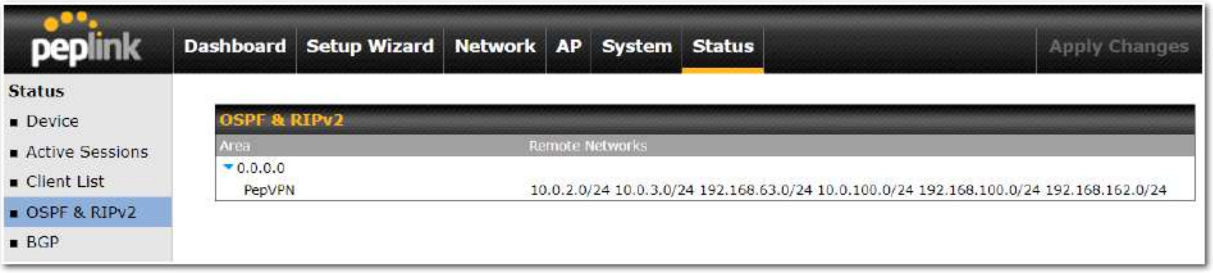
Click ✖ to delete a single UPnP / NAT-PMP record in its corresponding row. To delete all records, click **Delete All** on the right-hand side below the table.

Important Note

UPnP / NAT-PMP records will be deleted immediately after clicking the button ✖ or **Delete All,** without the need to click **Save** or **Confirm**.

30.6 OSPF & RIPv2

The table shows status of OSPF and RIPv2.

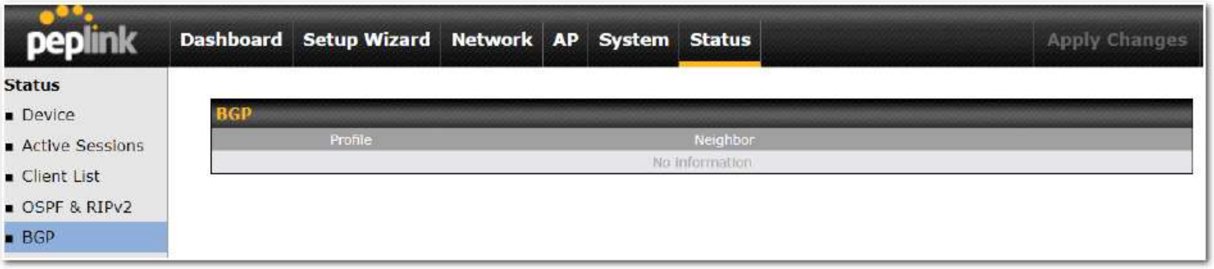


OSPF & RIPv2

Area	Remote Networks
0.0.0.0	
PepVPN	10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24

30.7 BGP

The table shows status of BGP

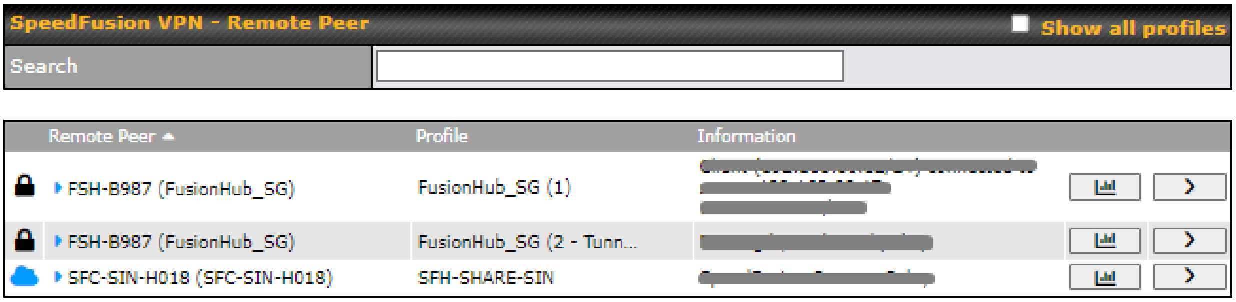


BGP

Profile	Neighbor
No information	

30.8 SpeedFusion VPN

Current SpeedFusion VPN status information is located at **Status > SpeedFusion VPN**. Details about SpeedFusion VPN connection peers appears as below:

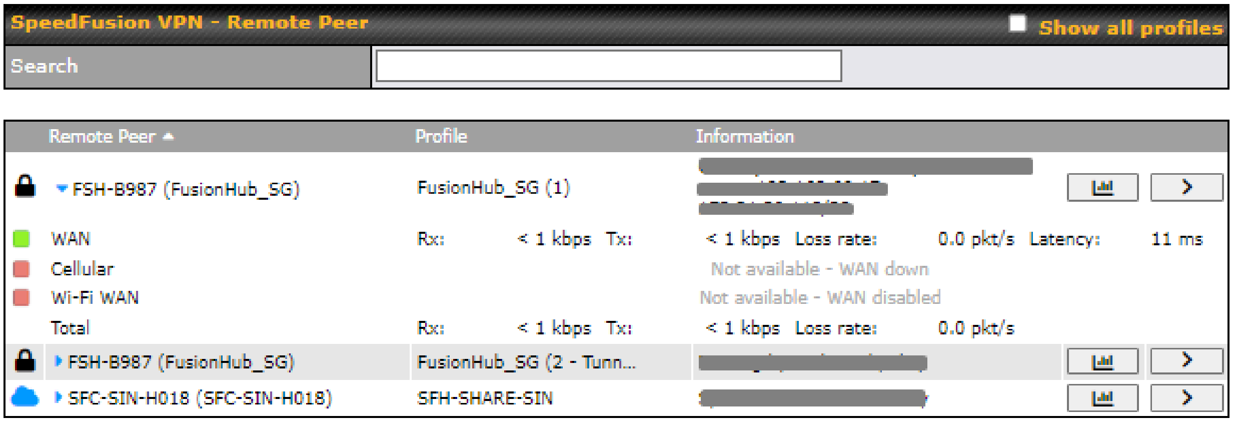


SpeedFusion VPN - Remote Peer

Search

Remote Peer ▲	Profile	Information
FSH-B987 (FusionHub_SG)	FusionHub_SG (1)	[redacted]
FSH-B987 (FusionHub_SG)	FusionHub_SG (2 - Tunn...	[redacted]
SFC-SIN-H018 (SFC-SIN-H018)	SFH-SHARE-SIN	[redacted]

Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

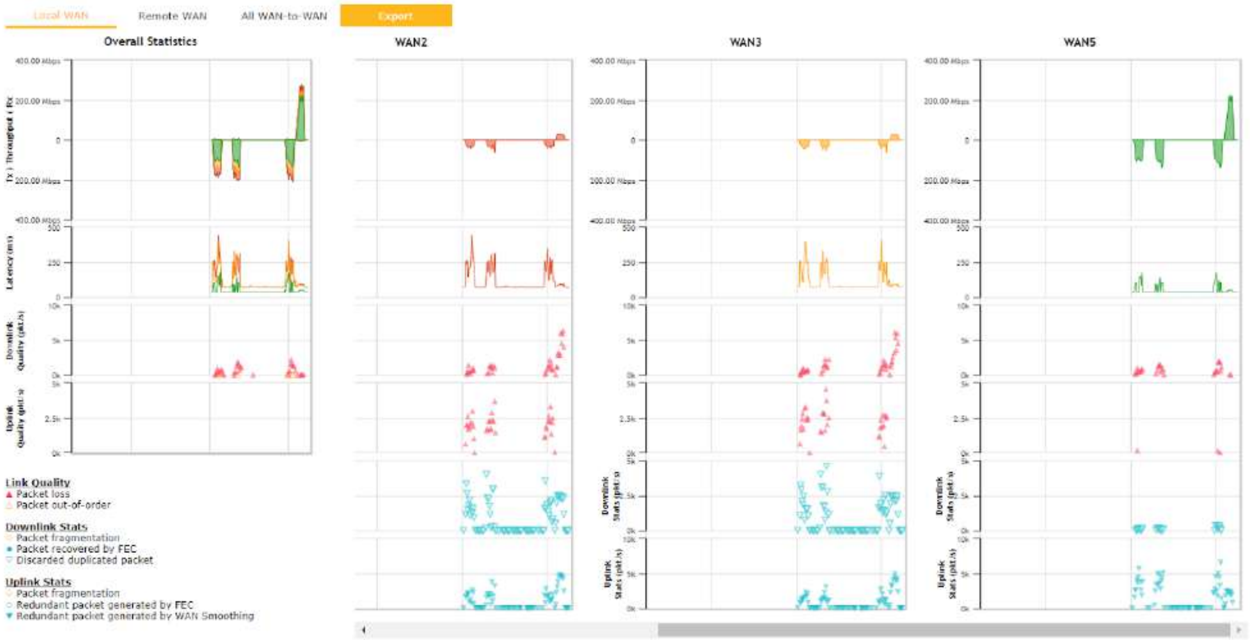


SpeedFusion VPN - Remote Peer ☐ Show all profiles

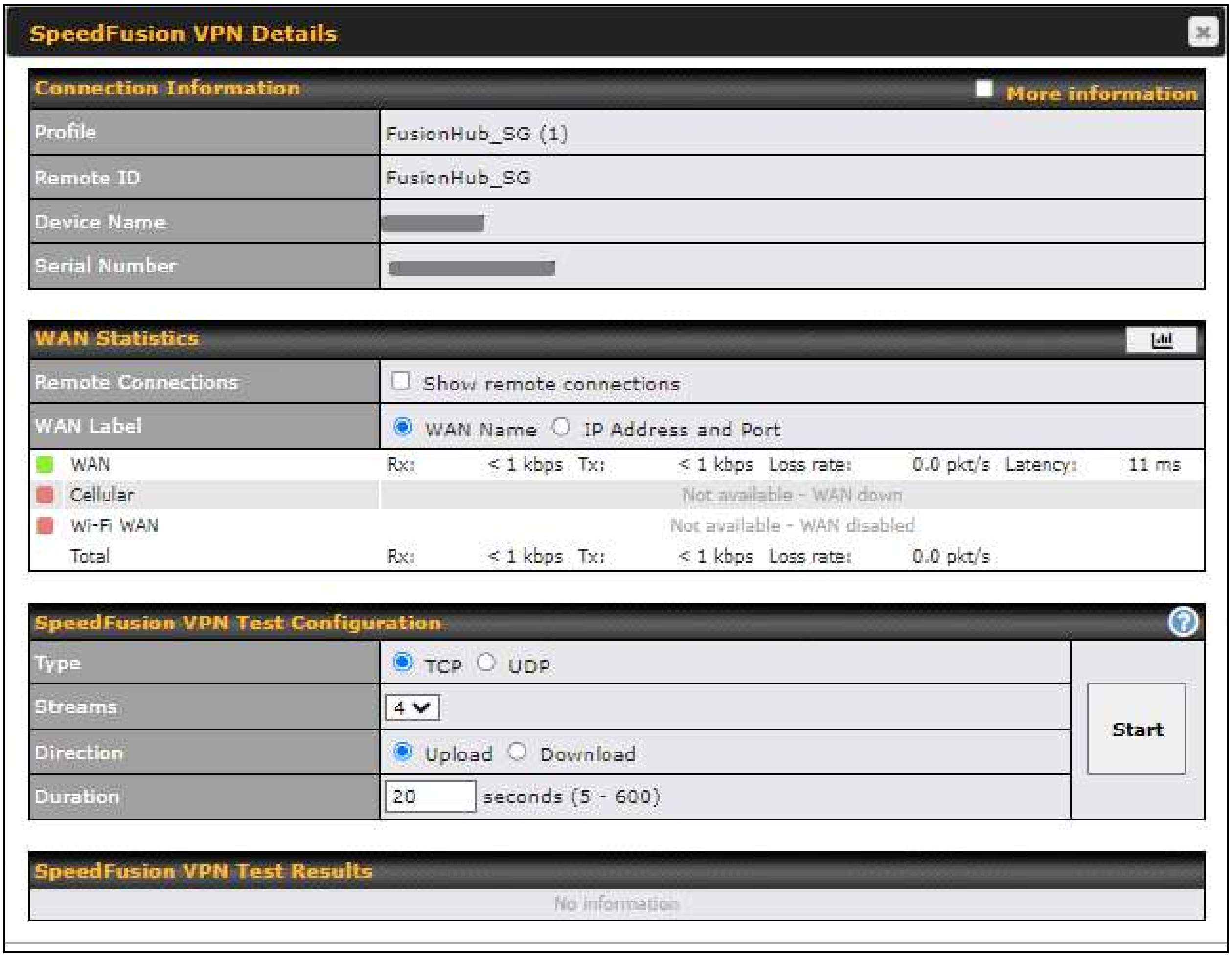
Search:

Remote Peer ▲	Profile	Information
🔒 ▼ FSH-B987 (FusionHub_SG)	FusionHub_SG (1)	[redacted]
🟩 WAN	Rx: < 1 kbps Tx:	< 1 kbps Loss rate: 0.0 pkt/s Latency: 11 ms
🟥 Cellular		Not available - WAN down
🟥 Wi-Fi WAN		Not available - WAN disabled
Total	Rx: < 1 kbps Tx:	< 1 kbps Loss rate: 0.0 pkt/s
🔒 ▶ FSH-B987 (FusionHub_SG)	FusionHub_SG (2 - Tunn...	[redacted]
☁ ▶ SFC-SIN-H018 (SFC-SIN-H018)	SFH-SHARE-SIN	[redacted]

Click the 📊 button for a SpeedFusion chart displaying real-time throughput, latency, and drop-rate information for each WAN connection.



When pressing the > button, the following menu will appear:



SpeedFusion VPN Details

Connection Information	☐ More information
Profile	FusionHub_SG (1)
Remote ID	FusionHub_SG
Device Name	[redacted]
Serial Number	[redacted]

WAN Statistics									
Remote Connections	☐ Show remote connections								
WAN Label	● WAN Name ○ IP Address and Port								
🟩 WAN	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s	Latency:	11 ms
🟥 Cellular	Not available - WAN down							
🟥 Wi-Fi WAN	Not available - WAN disabled							
Total	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s		

SpeedFusion VPN Test Configuration		
Type	● TCP ○ UDP	Start
Streams	4	
Direction	● Upload ○ Download	
Duration	20 seconds (5 - 600)	

SpeedFusion VPN Test Results
No information

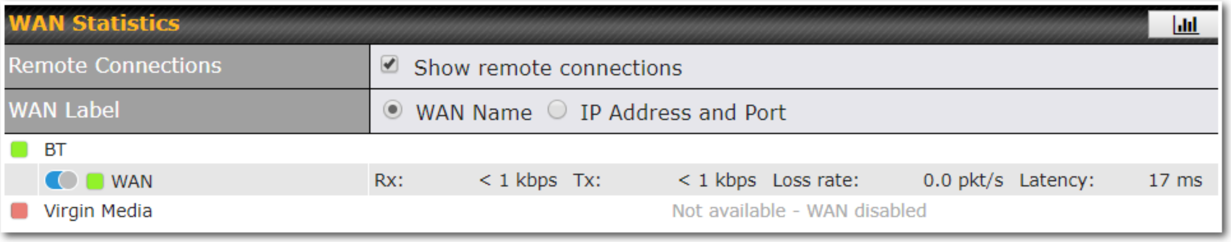
The **connection information** shows the details of the selected SpeedFusion VPN profile, consisting of the Profile name, **Router ID**, **Router Nam**e and **Serial Number** of the remote router
Advanced features for the SpeedFusion VPN profile will also be shown when the **More Information** checkbox is selected.

The **WAN statistics** show information about the local and remote WAN connections (when **show Remote connections**) is selected.
The available details are **WAN Name, IP address** and **port** used for the Speedfusion connection. **Rx and Tx rates, Loss rate and Latency**.

Connections can be temporarily disabled by sliding the switch button next to a WAN connection to the left.
The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15

minutes without any action.

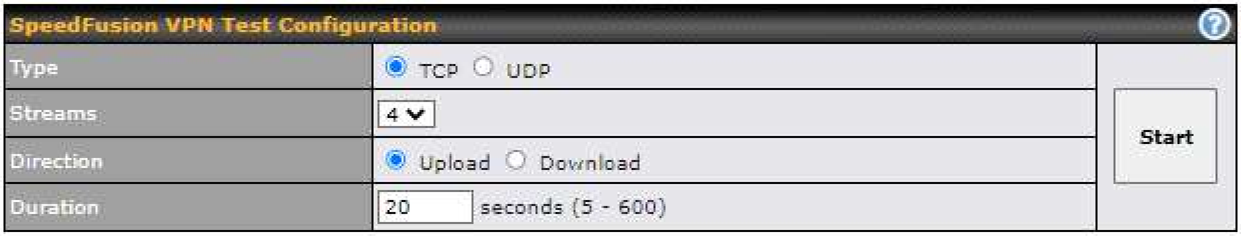
This can be used when testing the SpeedFusion VPN's speed between two locations to see if there is interference or network congestion between certain WAN connections.



WAN Statistics

Remote Connections	☑ Show remote connections							
WAN Label	● WAN Name ○ IP Address and Port							
🟩 BT								
🟩 WAN	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s	Latency:	17 ms
🟥 Virgin Media	Not available - WAN disabled							

The SpeedFusion VPN test configuration allows us to configure and perform thorough tests. This is usually done after the initial installation of the routers and in case there are problems with aggregation.



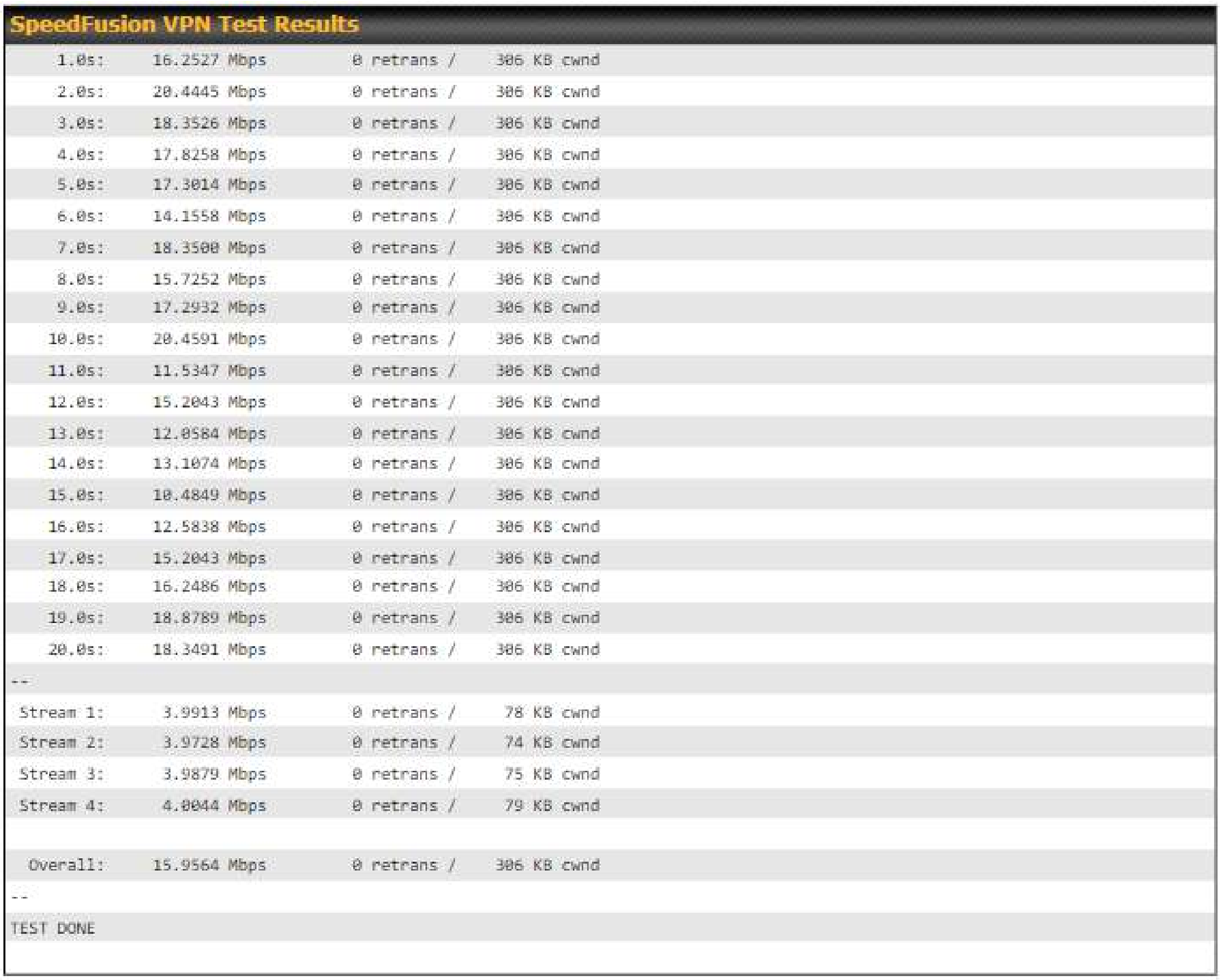
SpeedFusion VPN Test Configuration

Type	● TCP ○ UDP
Streams	4
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

Press the Start button to perform throughput test according to the configured options.

If TCP is selected, 4 parallel streams will be generated to get the optimal results by default. This can be customized by selecting a different value of streams.

Using more streams will typically get better results if the latency of the tunnel is high.



SpeedFusion VPN Test Results

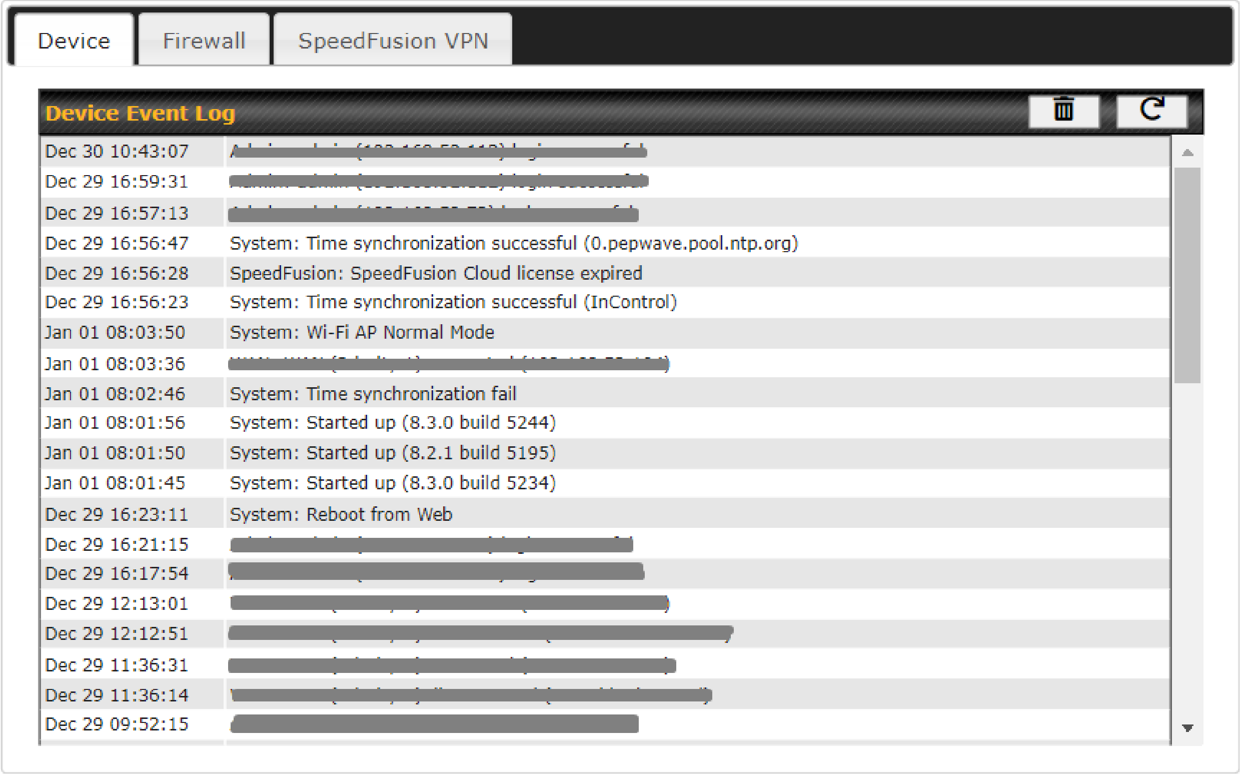
```
     1.0s:     16.2527 Mbps          0 retrans /    306 KB cwnd
     2.0s:     20.4445 Mbps          0 retrans /    306 KB cwnd
     3.0s:     18.3526 Mbps          0 retrans /    306 KB cwnd
     4.0s:     17.8258 Mbps          0 retrans /    306 KB cwnd
     5.0s:     17.3014 Mbps          0 retrans /    306 KB cwnd
     6.0s:     14.1558 Mbps          0 retrans /    306 KB cwnd
     7.0s:     18.3500 Mbps          0 retrans /    306 KB cwnd
     8.0s:     15.7252 Mbps          0 retrans /    306 KB cwnd
     9.0s:     17.2932 Mbps          0 retrans /    306 KB cwnd
    10.0s:     20.4591 Mbps          0 retrans /    306 KB cwnd
    11.0s:     11.5347 Mbps          0 retrans /    306 KB cwnd
    12.0s:     15.2043 Mbps          0 retrans /    306 KB cwnd
    13.0s:     12.0584 Mbps          0 retrans /    306 KB cwnd
    14.0s:     13.1074 Mbps          0 retrans /    306 KB cwnd
    15.0s:     10.4849 Mbps          0 retrans /    306 KB cwnd
    16.0s:     12.5838 Mbps          0 retrans /    306 KB cwnd
    17.0s:     15.2043 Mbps          0 retrans /    306 KB cwnd
    18.0s:     16.2486 Mbps          0 retrans /    306 KB cwnd
    19.0s:     18.8789 Mbps          0 retrans /    306 KB cwnd
    20.0s:     18.3491 Mbps          0 retrans /    306 KB cwnd
--
 Stream 1:      3.9913 Mbps          0 retrans /     78 KB cwnd
 Stream 2:      3.9728 Mbps          0 retrans /     74 KB cwnd
 Stream 3:      3.9879 Mbps          0 retrans /     75 KB cwnd
 Stream 4:      4.0044 Mbps          0 retrans /     79 KB cwnd

  Overall:     15.9564 Mbps          0 retrans /    306 KB cwnd
--
TEST DONE
```

Peplink also published a whitepaper about Speedfusion which can be downloaded from the following url:
http://download.peplink.com/resources/whitepaper-speedfusion-and-best-practices-2019.pdf

30.9 Event Log

Event log information is located at **Status > Event Log**.

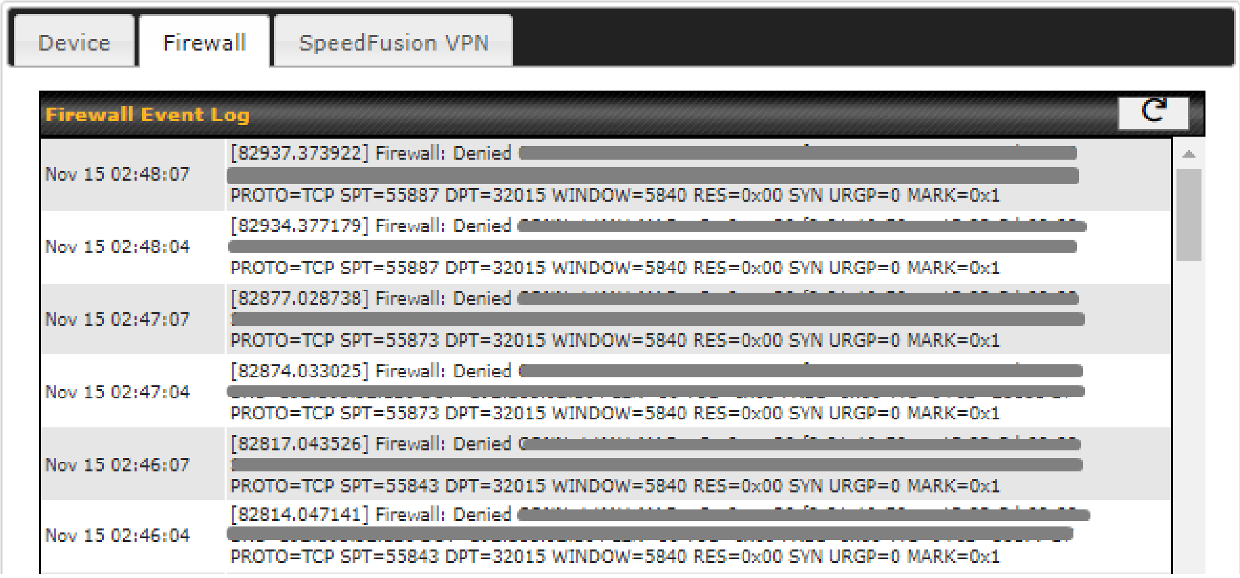
30.9.1 Device Event Log



```
Dec 30 10:43:07   [redacted]
Dec 29 16:59:31   [redacted]
Dec 29 16:57:13   [redacted]
Dec 29 16:56:47   System: Time synchronization successful (0.pepwave.pool.ntp.org)
Dec 29 16:56:28   SpeedFusion: SpeedFusion Cloud license expired
Dec 29 16:56:23   System: Time synchronization successful (InControl)
Jan 01 08:03:50   System: Wi-Fi AP Normal Mode
Jan 01 08:03:36   [redacted]
Jan 01 08:02:46   System: Time synchronization fail
Jan 01 08:01:56   System: Started up (8.3.0 build 5244)
Jan 01 08:01:50   System: Started up (8.2.1 build 5195)
Jan 01 08:01:45   System: Started up (8.3.0 build 5234)
Dec 29 16:23:11   System: Reboot from Web
Dec 29 16:21:15   [redacted]
Dec 29 16:17:54   [redacted]
Dec 29 12:13:01   [redacted]
Dec 29 12:12:51   [redacted]
Dec 29 11:36:31   [redacted]
Dec 29 11:36:14   [redacted]
Dec 29 09:52:15   [redacted]
```

The log section displays a list of events that has taken place on the Pepwave router. Click the ⟳ to refresh log entries automatically. Click the 🗑 button to clear the log.

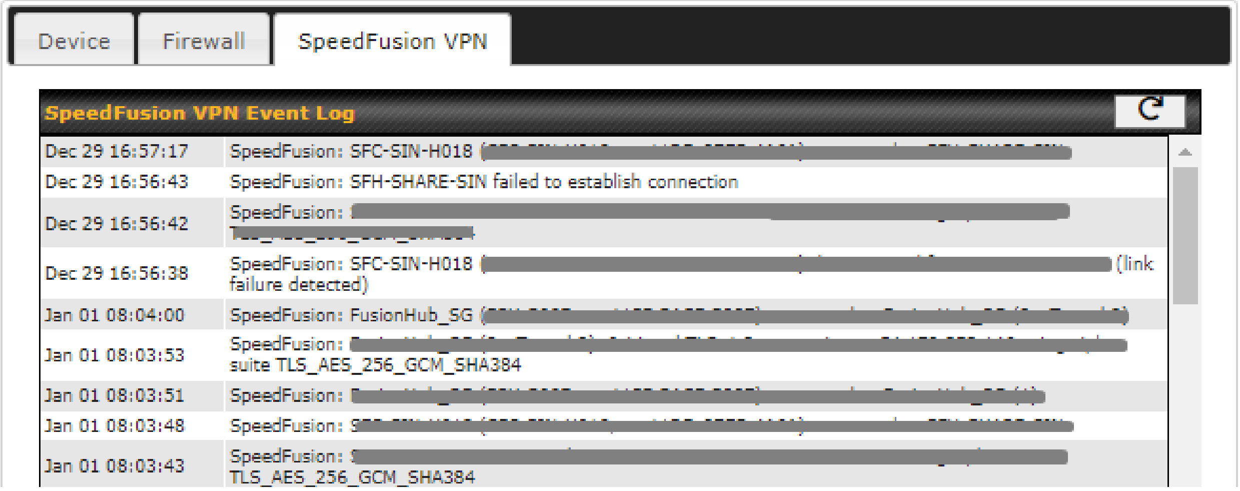
30.9.2 Firewall Event log



```
Nov 15 02:48:07  [82937.373922] Firewall: Denied [redacted]
                 PROTO=TCP SPT=55887 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1
Nov 15 02:48:04  [82934.377179] Firewall: Denied [redacted]
                 PROTO=TCP SPT=55887 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1
Nov 15 02:47:07  [82877.028738] Firewall: Denied [redacted]
                 PROTO=TCP SPT=55873 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1
Nov 15 02:47:04  [82874.033025] Firewall: Denied [redacted]
                 PROTO=TCP SPT=55873 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1
Nov 15 02:46:07  [82817.043526] Firewall: Denied [redacted]
                 PROTO=TCP SPT=55843 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1
Nov 15 02:46:04  [82814.047141] Firewall: Denied [redacted]
                 PROTO=TCP SPT=55843 DPT=32015 WINDOW=5840 RES=0x00 SYN URGP=0 MARK=0x1
```

This section displays a list of events that have taken place within a firewall. Click the ⟳ button and the log will be refreshed.

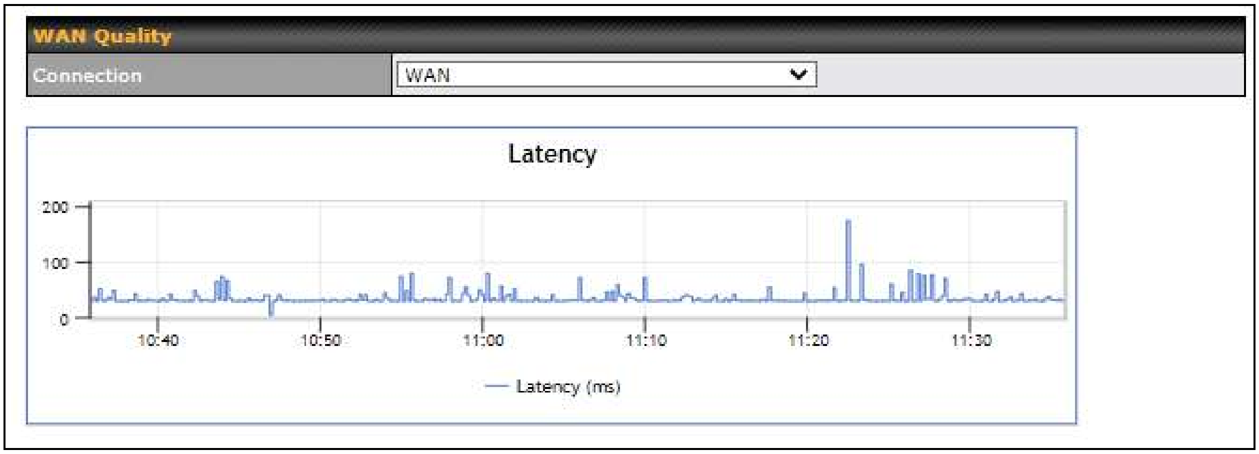
30.9.3 SpeedFusion VPN Event log



```
Dec 29 16:57:17  SpeedFusion: SFC-SIN-H018 [redacted]
Dec 29 16:56:43  SpeedFusion: SFH-SHARE-SIN failed to establish connection
Dec 29 16:56:42  SpeedFusion: [redacted]
Dec 29 16:56:38  SpeedFusion: SFC-SIN-H018 [redacted] (link
                 failure detected)
Jan 01 08:04:00  SpeedFusion: FusionHub_SG [redacted]
Jan 01 08:03:53  SpeedFusion: [redacted]
                 suite TLS_AES_256_GCM_SHA384
Jan 01 08:03:51  SpeedFusion: [redacted]
Jan 01 08:03:48  SpeedFusion: [redacted]
Jan 01 08:03:43  SpeedFusion: [redacted]
                 TLS_AES_256_GCM_SHA384
```

This section displays a list of events that have taken place within a SpeedFusion VPN connection. Click the ⟳ button and the log will be refreshed.

31 WAN Quality



WAN Quality

Connection	WAN

The **Status > WAN Quality** allow to show detailed information about each connected WAN connection.

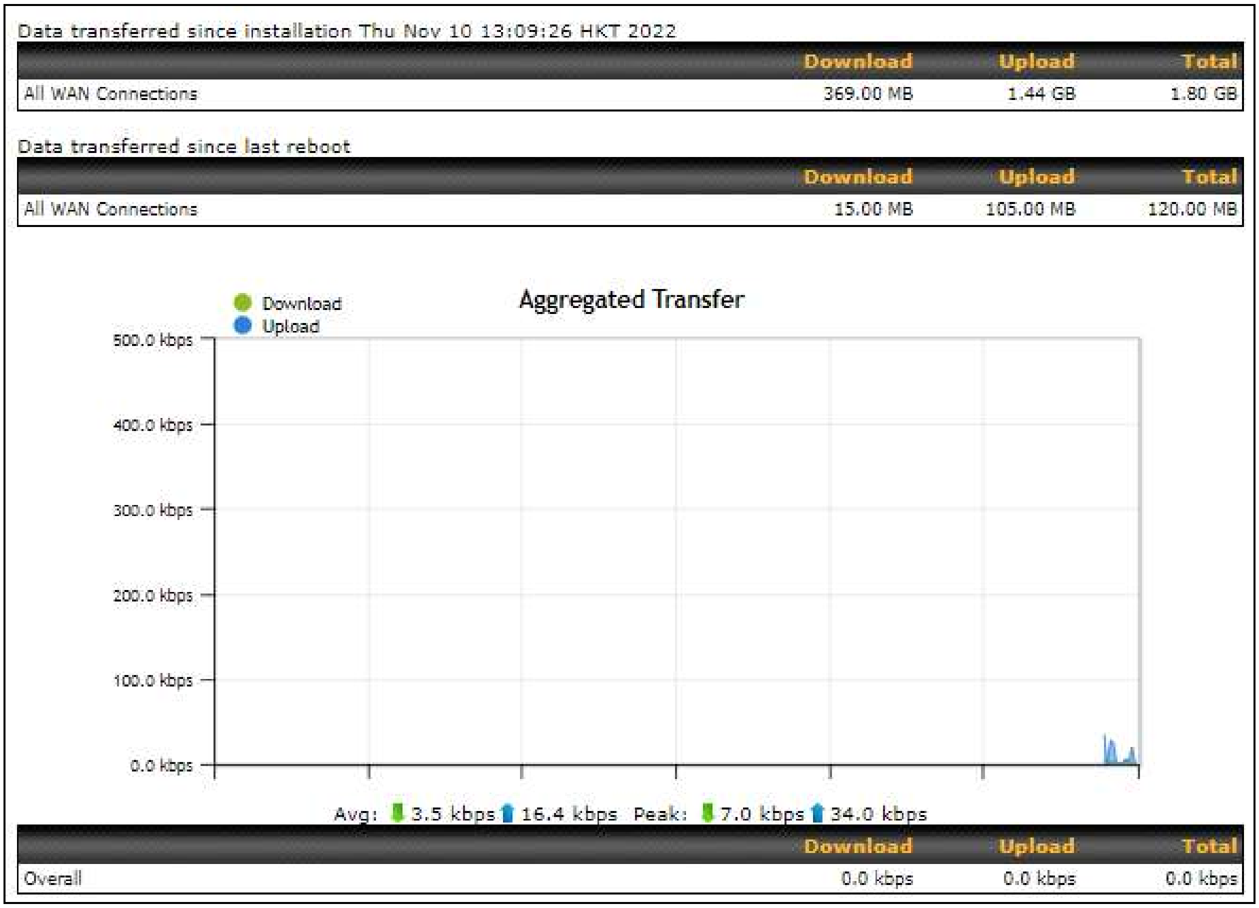
For cellular connections it shows signal strength, quality, throughput and latency for the past hour.

32 Usage Reports

This section shows bandwidth usage statistics and is located at **Status > Usage Reports** Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

32.1 Real-Time

The **Data transferred since installation** table indicates how much network traffic has been processed by the device since the first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last bootup.



Data transferred since installation Thu Nov 10 13:09:26 HKT 2022

	Download	Upload	Total
All WAN Connections	369.00 MB	1.44 GB	1.80 GB

Data transferred since last reboot

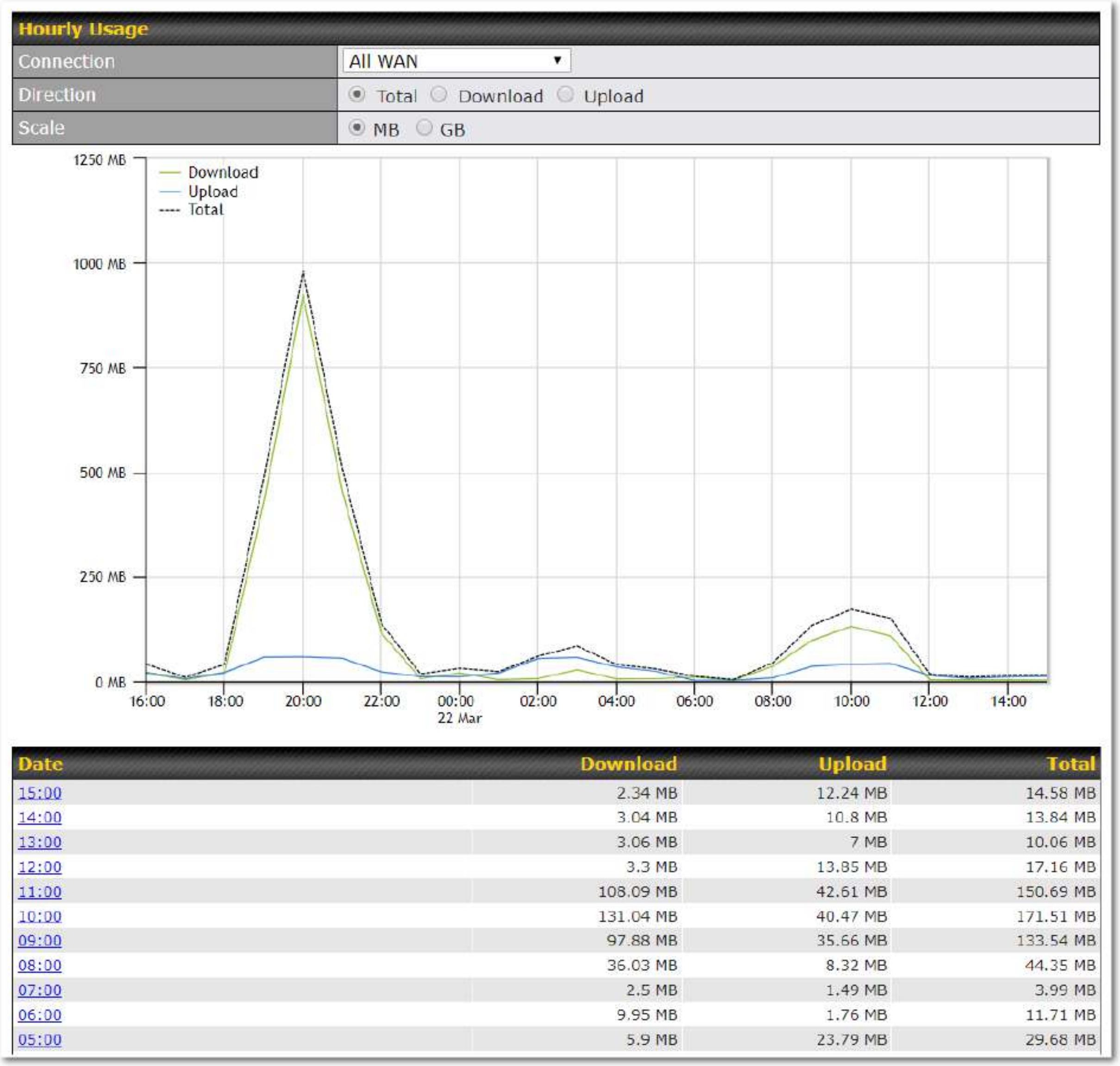
	Download	Upload	Total
All WAN Connections	15.00 MB	105.00 MB	120.00 MB

Avg: ⬇ 3.5 kbps ⬆ 16.4 kbps Peak: ⬇ 7.0 kbps ⬆ 34.0 kbps

	Download	Upload	Total
Overall	0.0 kbps	0.0 kbps	0.0 kbps

32.2 Hourly

This page shows the hourly bandwidth usage for all WAN connections, with the option of viewing each individual connection. Select the desired connection to check from the drop-down menu.



Hourly Usage

Connection	All WAN ▾
Direction	● Total ○ Download ○ Upload
Scale	● MB ○ GB

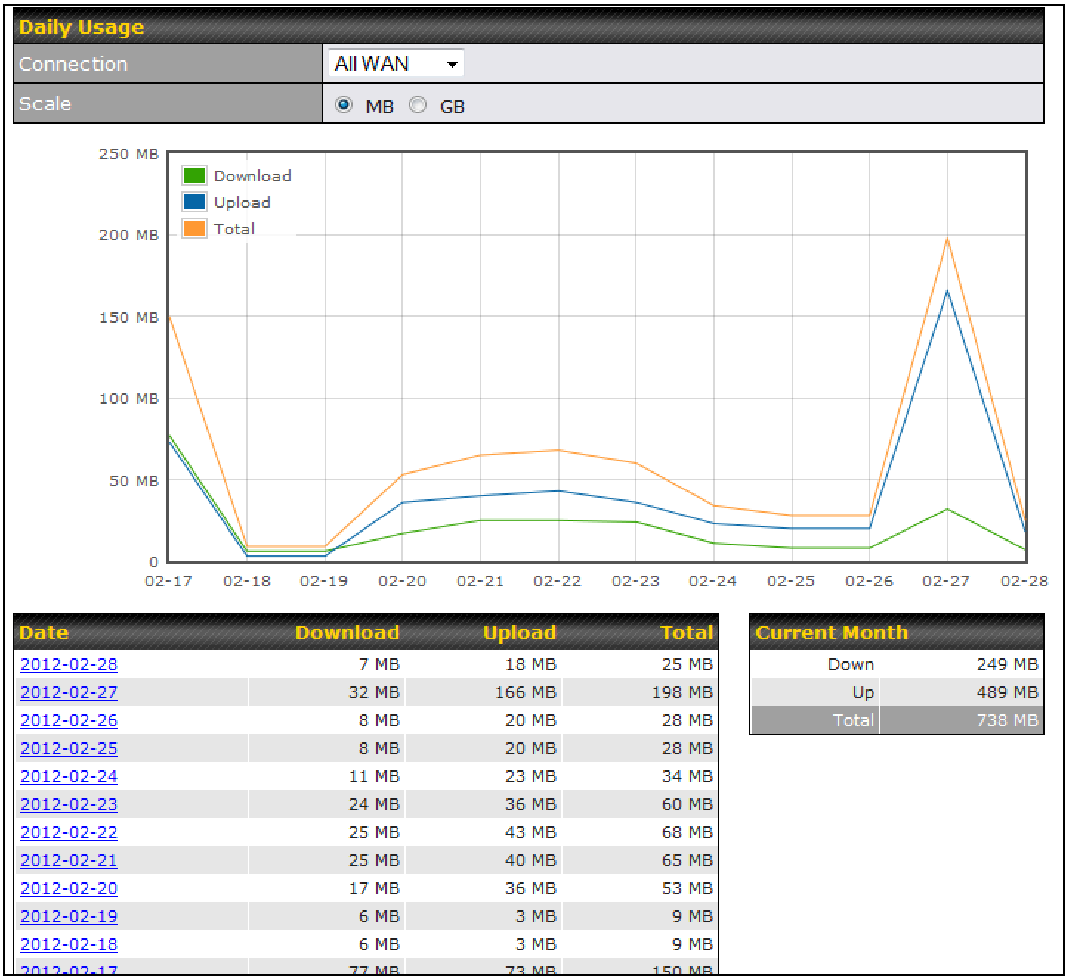
Date	Download	Upload	Total
15:00	2.34 MB	12.24 MB	14.58 MB
14:00	3.04 MB	10.8 MB	13.84 MB
13:00	3.06 MB	7 MB	10.06 MB
12:00	3.3 MB	13.85 MB	17.16 MB
11:00	108.09 MB	42.61 MB	150.69 MB
10:00	131.04 MB	40.47 MB	171.51 MB
09:00	97.88 MB	35.66 MB	133.54 MB
08:00	36.03 MB	8.32 MB	44.35 MB
07:00	2.5 MB	1.49 MB	3.99 MB
06:00	9.95 MB	1.76 MB	11.71 MB
05:00	5.9 MB	23.79 MB	29.68 MB

32.3 Daily

This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature**,** the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



Daily Usage

Connection	All WAN
Scale	● MB ○ GB

Date	Download	Upload	Total
2012-02-28	7 MB	18 MB	25 MB
2012-02-27	32 MB	166 MB	198 MB
2012-02-26	8 MB	20 MB	28 MB
2012-02-25	8 MB	20 MB	28 MB
2012-02-24	11 MB	23 MB	34 MB
2012-02-23	24 MB	36 MB	60 MB
2012-02-22	25 MB	43 MB	68 MB
2012-02-21	25 MB	40 MB	65 MB
2012-02-20	17 MB	36 MB	53 MB
2012-02-19	6 MB	3 MB	9 MB
2012-02-18	6 MB	3 MB	9 MB
2012-02-17	77 MB	73 MB	150 MB

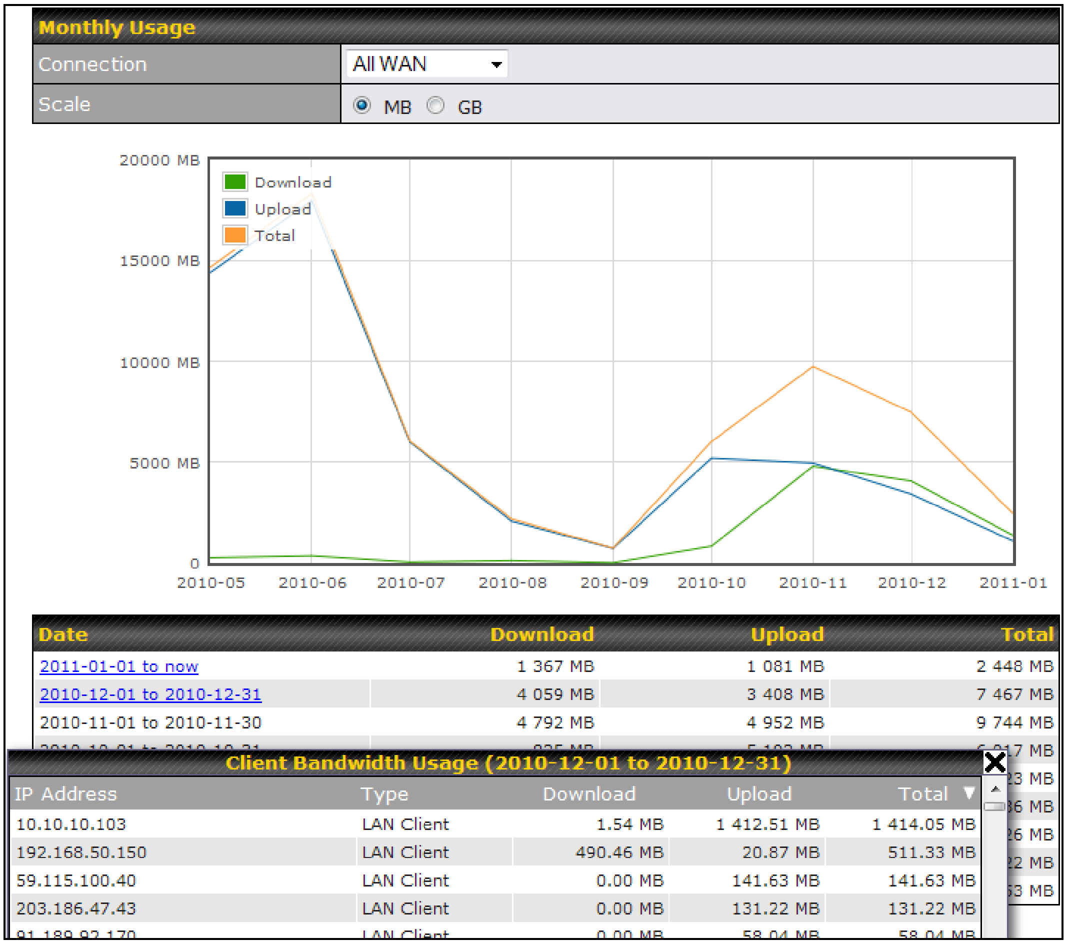
Current Month	
Down	249 MB
Up	489 MB
Total	738 MB

All WAN Daily Bandwidth Usage

32.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled the **Bandwidth Monitoring** feature, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

Click the first two rows to view the client bandwidth usage in the last two months. This feature is not available if you have chosen to view the bandwidth of an individual WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



Monthly Usage

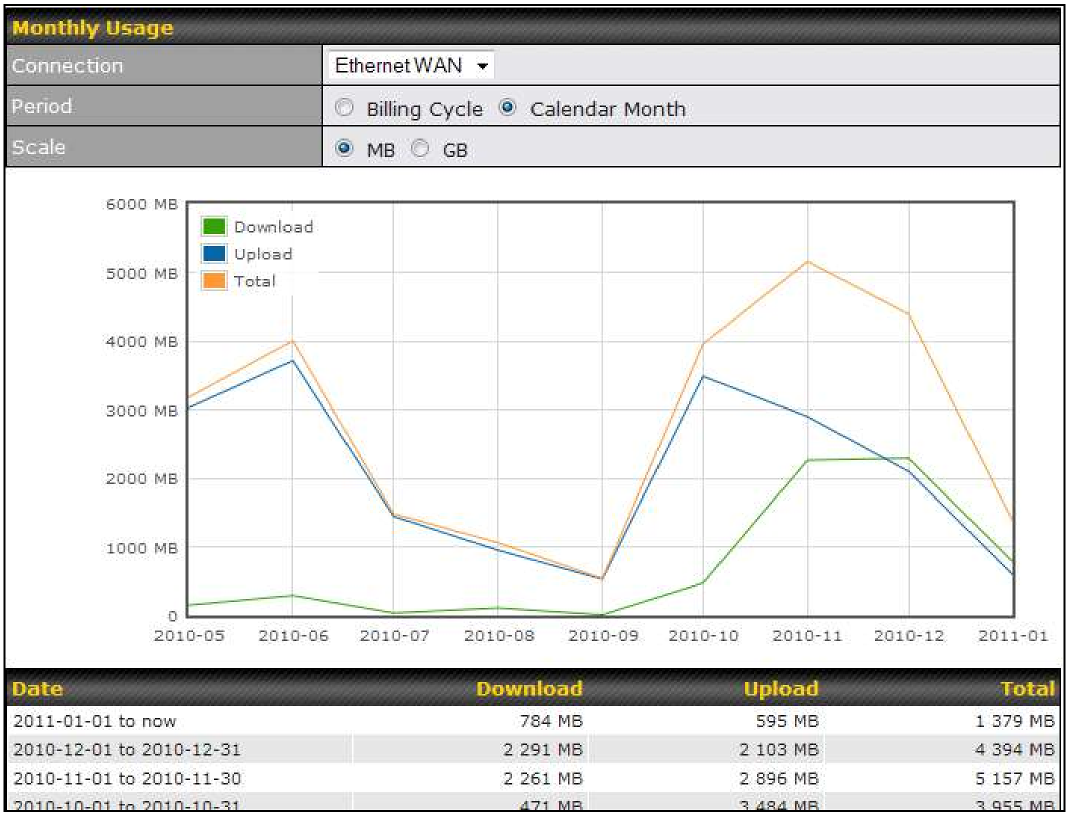
Connection	All WAN
Scale	● MB ○ GB

Date	Download	Upload	Total
2011-01-01 to now	1 367 MB	1 081 MB	2 448 MB
2010-12-01 to 2010-12-31	4 059 MB	3 408 MB	7 467 MB
2010-11-01 to 2010-11-30	4 792 MB	4 952 MB	9 744 MB
2010-10-01 to 2010-10-31	[illegible]	[illegible]	6 017 MB

Client Bandwidth Usage (2010-12-01 to 2010-12-31)

IP Address	Type	Download	Upload	Total ▼
10.10.10.103	LAN Client	1.54 MB	1 412.51 MB	1 414.05 MB
192.168.50.150	LAN Client	490.46 MB	20.87 MB	511.33 MB
59.115.100.40	LAN Client	0.00 MB	141.63 MB	141.63 MB
203.186.47.43	LAN Client	0.00 MB	131.22 MB	131.22 MB
91.189.92.170	LAN Client	0.00 MB	58.04 MB	58.04 MB

All WAN Monthly Bandwidth Usage



Monthly Usage

Connection	Ethernet WAN ▾
Period	○ Billing Cycle ● Calendar Month
Scale	● MB ○ GB

Date	Download	Upload	Total
2011-01-01 to now	784 MB	595 MB	1 379 MB
2010-12-01 to 2010-12-31	2 291 MB	2 103 MB	4 394 MB
2010-11-01 to 2010-11-30	2 261 MB	2 896 MB	5 157 MB
2010-10-01 to 2010-10-31	471 MB	3 484 MB	3 955 MB

Ethernet WAN Monthly Bandwidth Usage

Tip
By default, the scale of data size is in **MB**. 1GB equals 1024MB.

Appendix A: Restoration of Factory Defaults

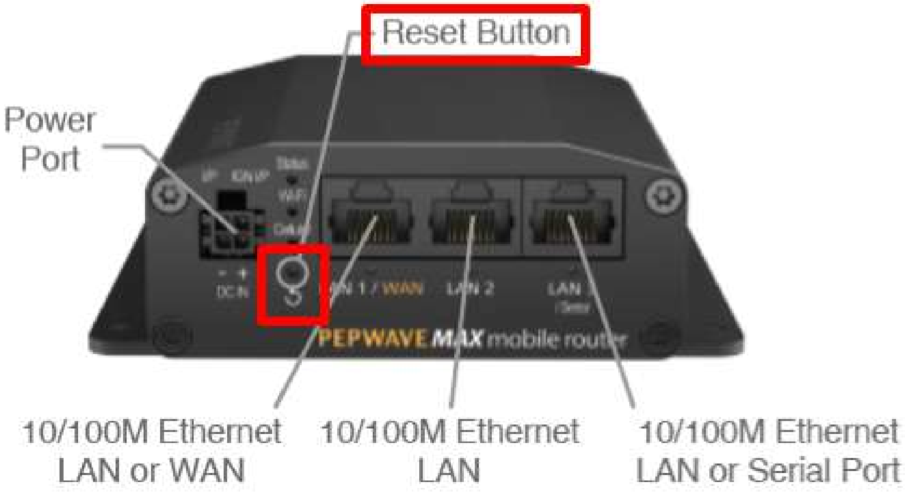
To restore the factory default settings on a Pepwave router, follow the steps below:

1. Locate the reset button on the front or back panel of the Pepwave router.
2. With a paperclip, press and keep the reset button pressed.

Hold for approximately 20 seconds for factory reset (Note: The LED status light shows in RED, all WAN/LAN port lights start blinking, and release the button)

After the Pepwave router finishes rebooting, the factory default settings will be restored.

Important Note
All previous configurations and bandwidth usage data will be lost after restoring factory default settings. Regular backup of configuration settings is strongly recommended.


Reset Button
Power Port
10/100M Ethernet LAN or WAN
10/100M Ethernet LAN
10/100M Ethernet LAN or Serial Port
PEPWAVE MAX mobile router

Appendix B: FusionSIM Manual

Peplink has developed a unique technology called FusionSIM, which allows SIM cards to remotely link to a cellular router. This can be done via cloud or within the same physical network. There are a few key scenarios to fit certain applications.

The purpose of this manual is to provide an introduction on where to start and how to set up for the most common scenarios and uses.

Requirements

1. A Cellular router that supports FusionSIM technology
2. SIM Injector
3. SIM card

Notes:

- Always check for the latest Firmware version for both the cellular router and the SIM Injector. You can also check for the latest Firmware version on the device's WEB configuration page.
- A list of products that support FusionSIM can be found on the SIM Injector WEB page. Please check under the section **Supported models**.

SIM Injector reset and login details

How to reset a SIM Injector:

- Hold the reset button for 5-10 seconds. Once the LED status light turns RED, the reset button can be released. SIM Injector will reboot and start with the factory default settings.

The default WEB login settings:

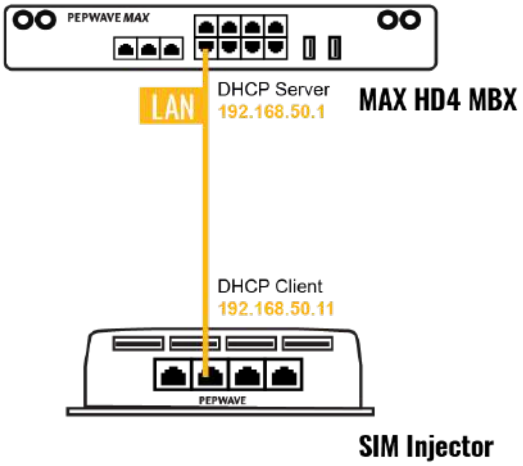
- **User**: admin
- **Password**: admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

Notes:

- The SIM Injector can be monitored via InControl 2. Configuration is not supported.

Scenario 1: SIM Injector in LAN of Cellular Router

Setup topology



This is the most basic scenario in which the SIM Injector is connected directly to the cellular router's LAN port via an ethernet cable. This allows for the cellular router to be positioned for the best possible signal. Meanwhile, the SIM cards can be conveniently located in other locations such as the office, passenger area, or the bridge of a ship. The SIM Injector allows for easily swapping SIM cards without needing to access a cellular router.

IMPORTANT: Cellular WAN will not fallback to the local SIM if it is configured to use the SIM Injector.

Configuring the SIM Injector

1. Connect the SIM Injector to the LAN port of the cellular router.
2. Insert SIM cards into the SIM Injector. The SIM cards will be automatically detected.

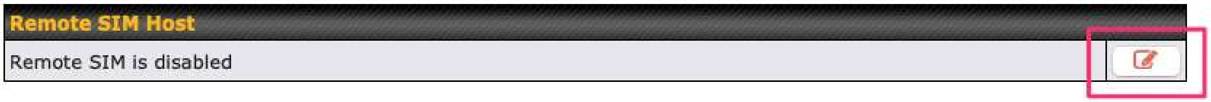
IMPORTANT: SIM cards inserted into SIM Injector must not have a PIN code.

Note 1: The SIM Injector gets its IP address via DHCP and doesn't have a static IP address. To find it's address, please check the DHCP lease on the cellular router.

Configuring the Cellular Router

Step 1. Enable the SIM Injector communication protocol.

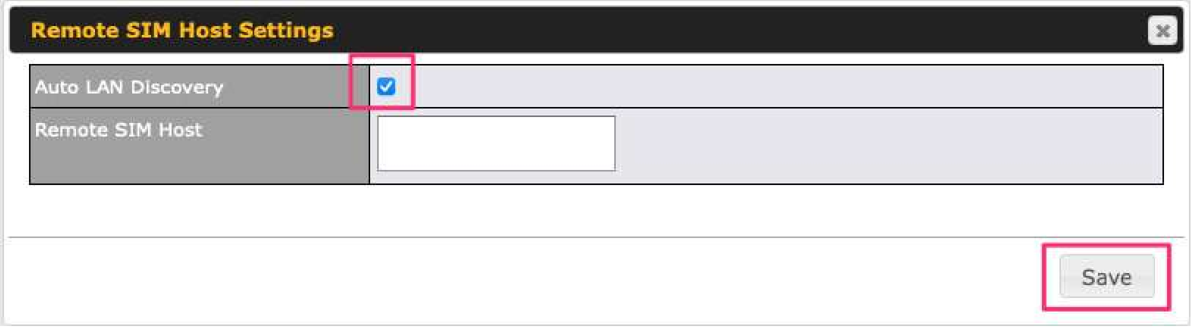
1a. If you are using a Balance cellular router, go to the **Network** tab (top navigation bar).
1b. If you are using a MAX cellular router, go to the **Advanced** tab (top navigation bar).
2. Under **Misc. settings** (left navigation bar) find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.



Remote SIM Host

Remote SIM is disabled

4. Check the **Auto LAN discovery** checkbox and click **Save** and **Apply Changes**.



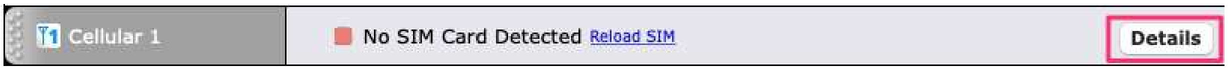
Remote SIM Host Settings

Auto LAN Discovery	☑
Remote SIM Host	

5. Click **Save** and then **Apply Changes**.

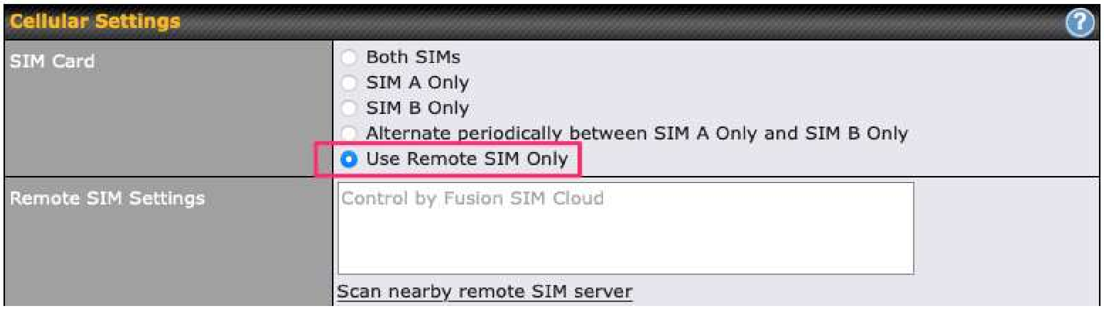
Step 2. Enable RemoteSIM for the selected Cellular interface.

1. Go to **Network** (top navigation bar), then **WAN** (left navigation bar) and click **Details** for a selected cellular WAN. This will open the WAN Connection Settings page.



Cellular 1 — No SIM Card Detected

2. Scroll down to **Cellular settings**.
3. In the **SIM Card** section, select **Use Remote SIM Only**.



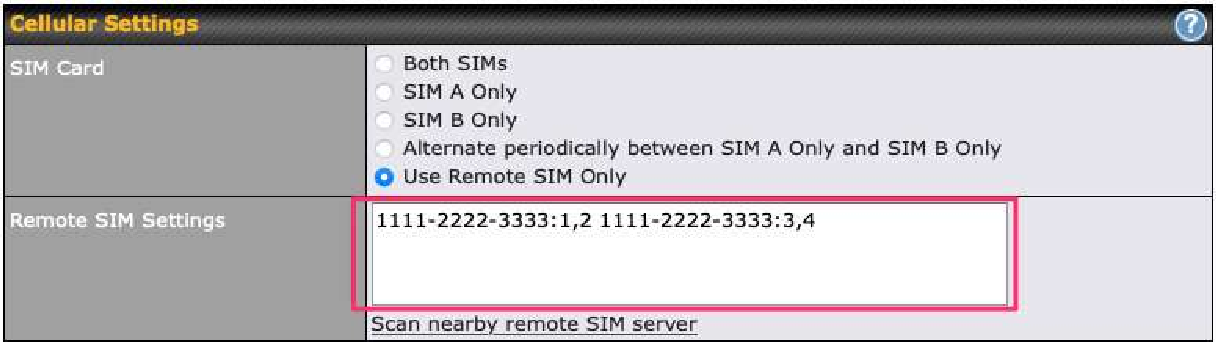
Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only
Remote SIM Settings	Control by Fusion SIM Cloud Scan nearby remote SIM server

4. Enter configuration settings in **Remote SIM Settings** section. Click on **Scan nearby remote SIM server** to show the serial number(s) of the connected SIM Injector(s). Available configuration options for cellular interface are shown below:

A. Defining SIM Injector(s)
- Format: <S/N>
- Example 1: 1111-2222-3333
- Example 2: 1111-2222-3333 4444-5555-6666

B. Defining SIM Injector(s) SIM slot(s):
- Format: <S/N:slot number>
- Example 1: 1111-2222-3333:7,5 (the Cellular Interface will use SIM in slot 7, then 5)
- Example 2: 1111-2222-3333:1,2 1111-2222-3333:3,4 (the cellular Interface will use SIM in slot 1, then in 2 from the first SIM Injector, and then it will use 3 and 4 from the second SIM Injector).



Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only
Remote SIM Settings	1111-2222-3333:1,2 1111-2222-3333:3,4 Scan nearby remote SIM server

Note: It is recommended to use different SIM slots for each cellular interface.

5. Click **Save** and **Apply Changes**.

Step 3. (Optional) Custom SIM cards settings.

1a. For a Balance router, go to the **Network** (Top tab).

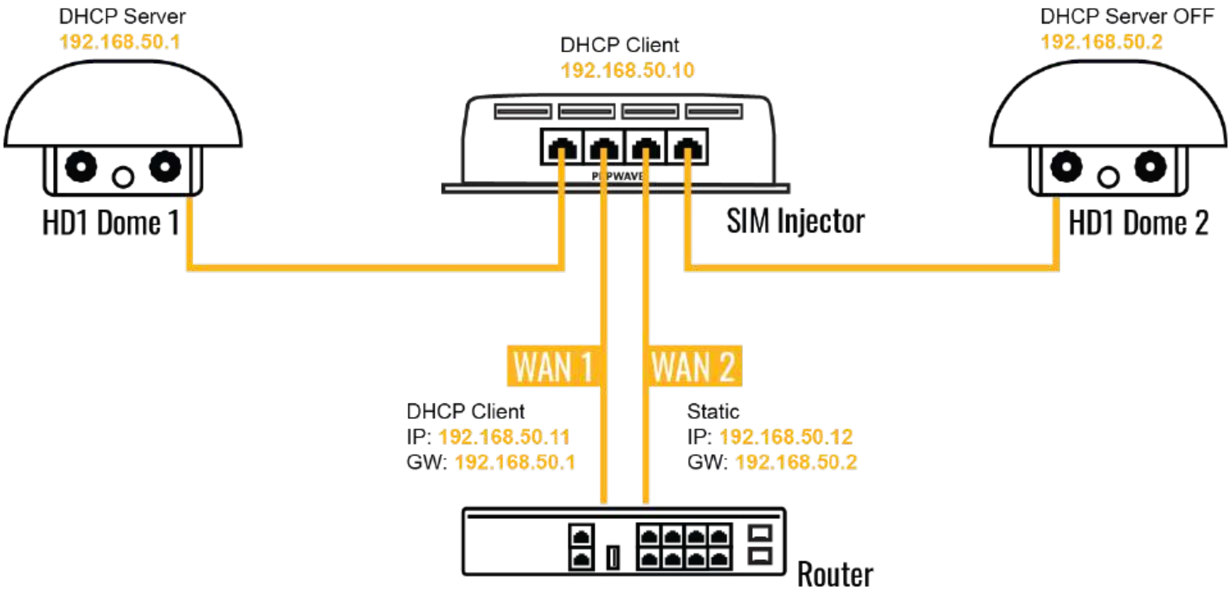
1b. For a MAX router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab) find **Remote SIM Management**.
3. Click on the **Add Remote SIM** button, fill in all the required info and click **Save**. This section allows defining custom requirements for a SIM card located in a certain SIM slot:

- Enable/Disable roaming (by default roaming is disabled).
- Add Custom mobile operator settings (APN, user name, password).

4. Repeat configuration for all SIM cards which need custom settings.
5. Click **Apply Changes** to take effect.

Scenario 2: SIM Injector in WAN of main Router and multiple Cellular Routers

Setup topology



In this scenario, each HD Dome creates a WAN connection to the main router. A single SIM Injector is used to provide SIM cards for each HD Dome. The HD Dome can be replaced with any Peplink cellular router supporting RemoteSIM technology.

This scenario requires the completion of the configuration steps shown in Scenario 1 in addition to the configuration steps explained below.

Additional configurations for Cellular Routers

Step 1. Disable the DHCP server.

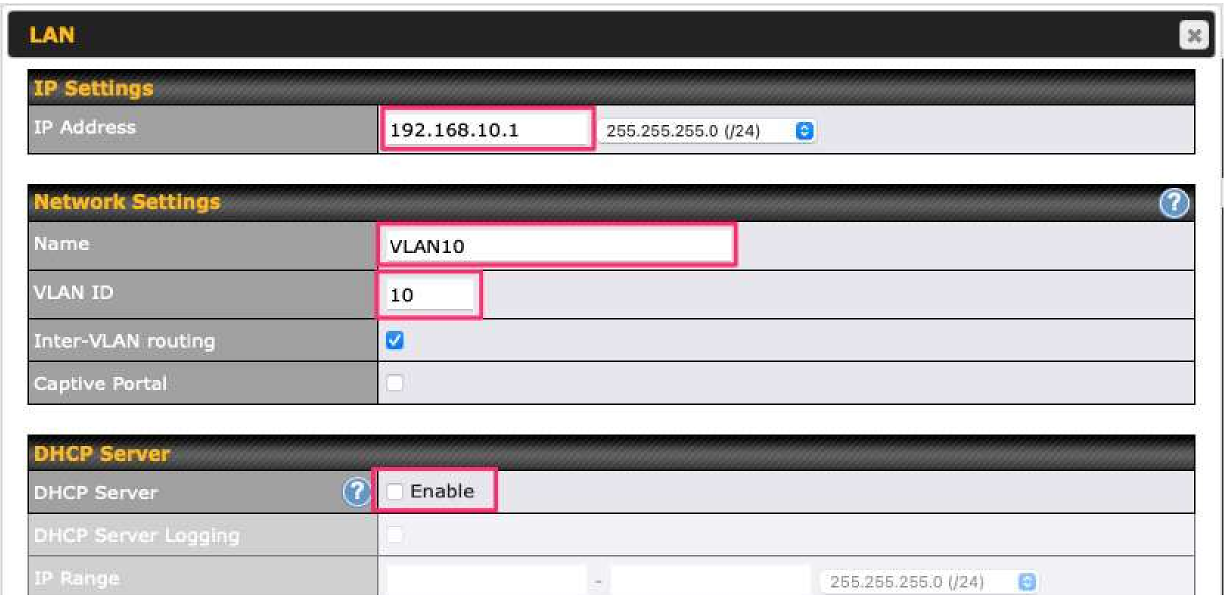
- HD Dome 1 should act as a DHCP server.
- HD Dome 2 should be configured to have a static IP address with DHCP disabled.
- Both routers should be in the same subnet (e.g. 192.168.50.1 and 192.168.50.2).

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **Untagged LAN**. This will open up the LAN settings page.
2. Change the IP address to 192.168.50.2.
3. In the **DHCP Server** section, uncheck the checkbox to disable DHCP Server.
4. Click **Save** and **Apply Changes**.

Step 2. Ethernet port configuration

The Ethernet port must be set to **ACCESS** mode for each HD Dome. To do this, dummy VLANs need to be created first.

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **New LAN**. This will open the settings page to create a dummy VLAN.
2. The image below shows the values that need to be changed to create a new VLAN:



LAN

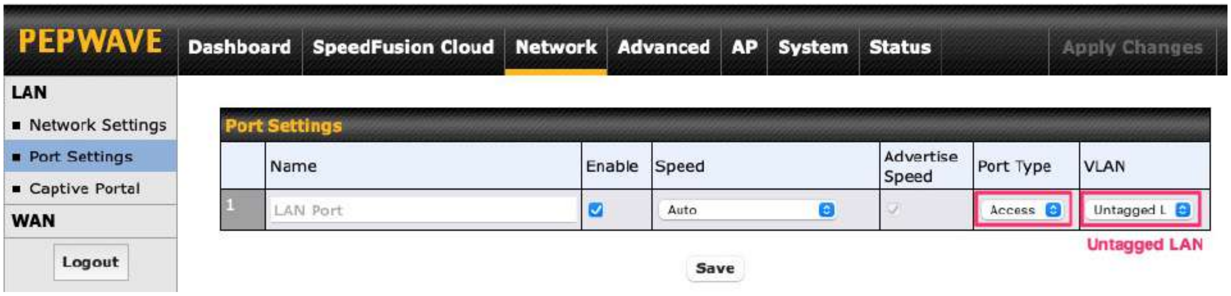
IP Settings	
IP Address	192.168.10.1 255.255.255.0 (/24)

Network Settings	
Name	VLAN10
VLAN ID	10
Inter-VLAN routing	☑
Captive Portal	□

DHCP Server	
DHCP Server	□ Enable
DHCP Server Logging	□
IP Range	- 255.255.255.0 (/24)

Note: set different IP addresses for each HD dome (e.g. 192.168.10.1 and 192.168.10.2).

3. Click Save and **Apply Changes**.
4. Go to **Network** (Top tab), then **Port Settings** (Left-side tab).
5. Set the Port Type to **Access** and set VLAN to **Untagged LAN** (see picture below).



Port Settings

	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port	☑	Auto	✓	Access	Untagged L

Untagged LAN

6. Click **Save** and **Apply Changes**.

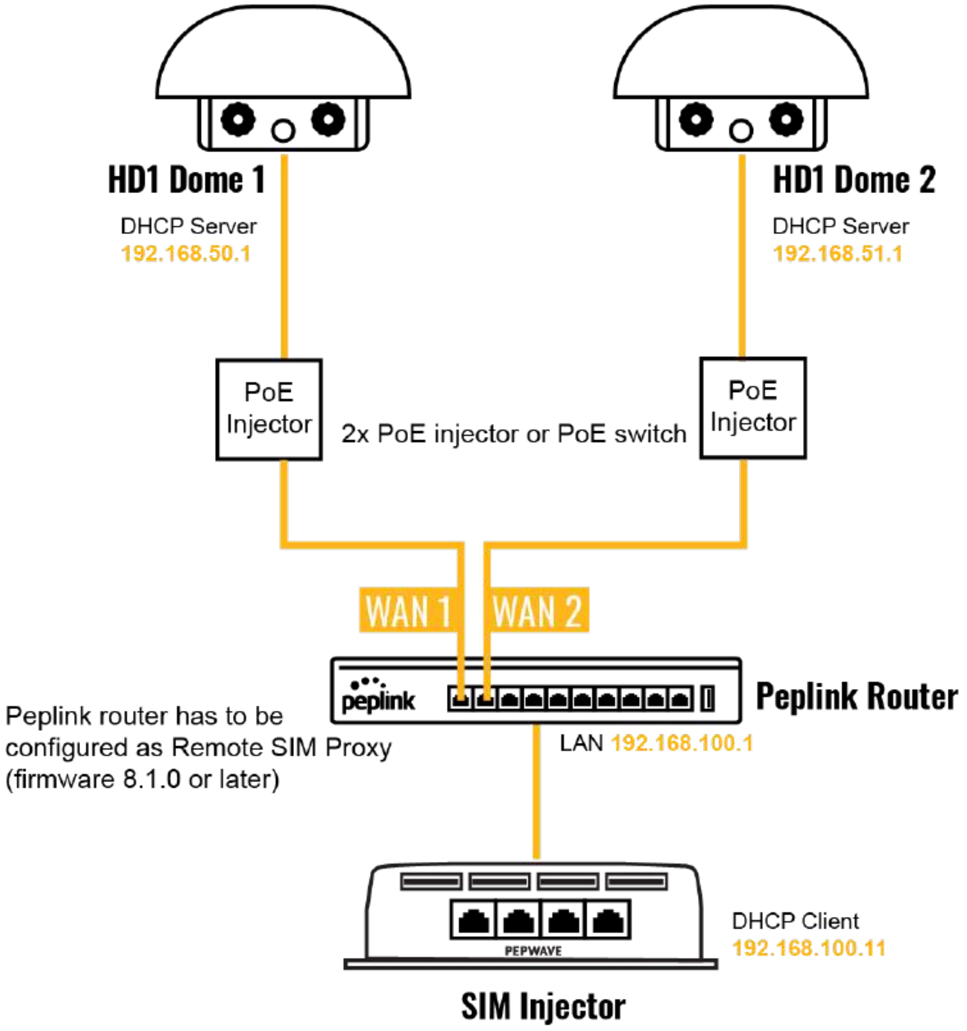
Configuration requirements for the main Router

Requirements for the main router are:

- Configure **WAN 1** as a DHCP client.
- **WAN 1** will automatically get the Gateway IP address from HD Dome 1.
- Configure **WAN 2** as a Static IP and set it to 192.168.50.12.
- Configure **WAN 2** Gateway to 192.168.50.2. Same as the HD Dome 2’s IP address.

Scenario 3: SIM Injector in LAN of main Router and multiple Cellular Routers

Setup topology



In this scenario, SIMs are provided to the HD Domes via the main router. In this example, the **Remote SIM Proxy** functionality needs to be enabled on the main router.

Notes:

- HD Dome can be replaced with any other cellular router that supports RemoteSIM.
- It is recommended to use Peplink Balance series or X series routers as the main router.