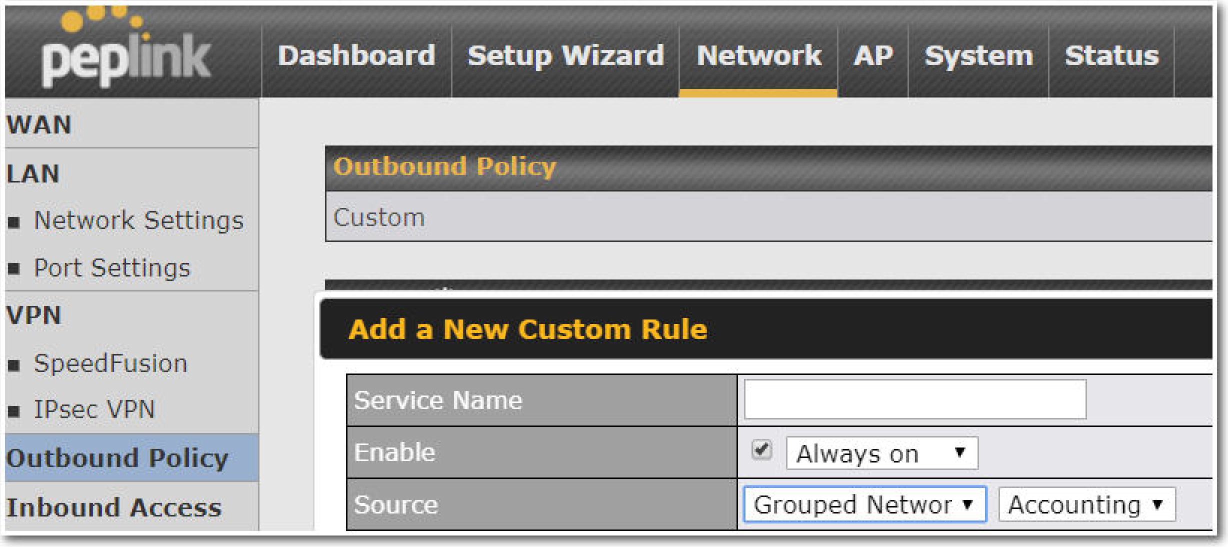


Outbound Policy

Custom

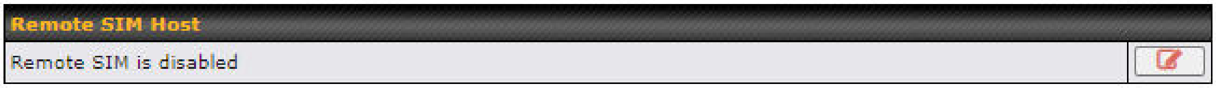
Add a New Custom Rule

| | |
|---|---|
| Service Name | |
| Enable | ☑ Always on ▾ |
| Source | Grouped Networ ▾ Accounting ▾ |

### 10.14.7 Remote SIM Management

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

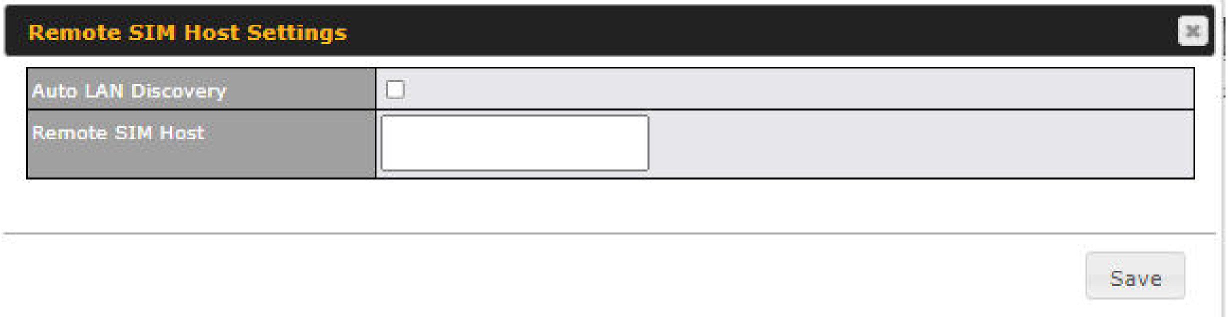
Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: https://www.peplink.com/products/sim-injector/ or Appendix C for more details on FusionSIM Manual.



Remote SIM Host

Remote SIM is disabled

### Remote SIM Host Settings

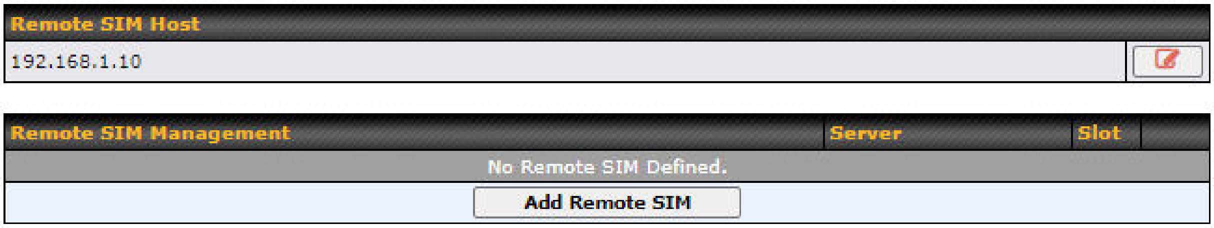


Remote SIM Host Settings

| | |
|---|---|
| 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. |

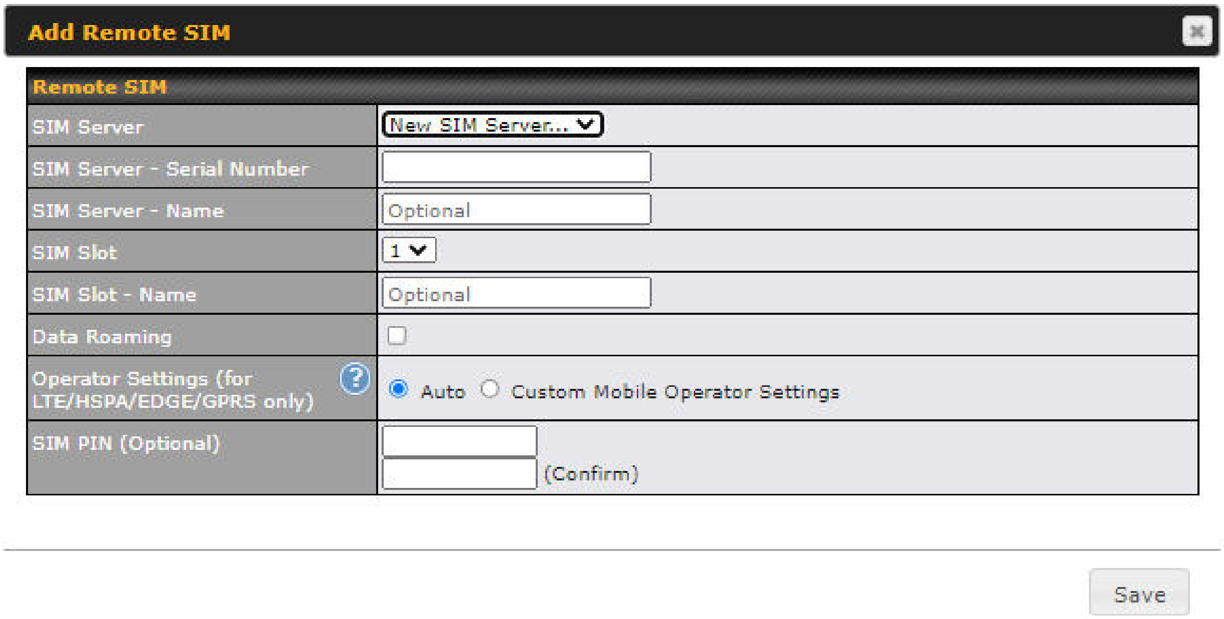
| | |
|---|---|
| **Remote SIM Host** | Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the “**Auto LAN Discovery**” box above. |



| Remote SIM Host | |
|---|---|
| 192.168.1.10 | |

| Remote SIM Management | Server | Slot | |
|---|---|---|---|
| No Remote SIM Defined. | | | |
| Add Remote SIM | | | |

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) | <br>(Confirm) |

Save

| 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. |

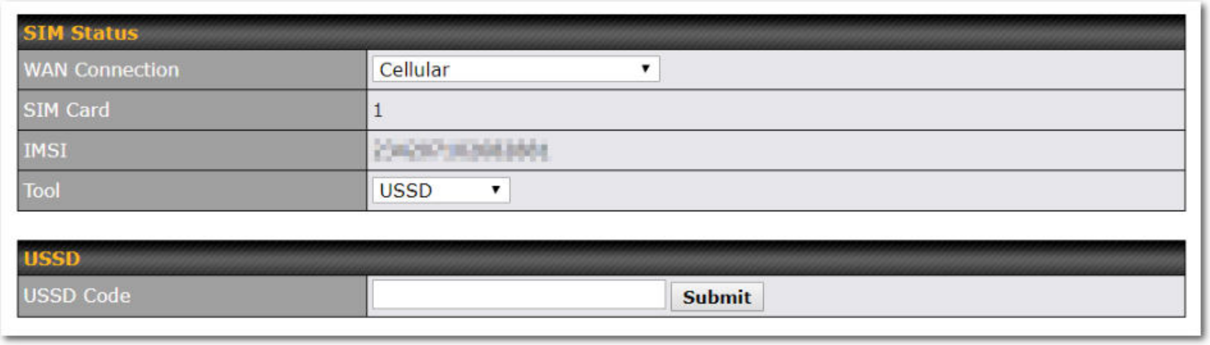
| | |
|---|---|
| **Data Roaming** | Enables data roaming on this particular SIM card. |
| **Operator Settings (for LTE//HSPA/EDGE/GPRS Only)** | This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The 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. |

### 10.14.8 SIM Toolkit

The SIM Toolkit can be found via **Networks > Misc Settings > SIM Toolkit**.This supports two functionalities, USSD and SMS.

#### USSD

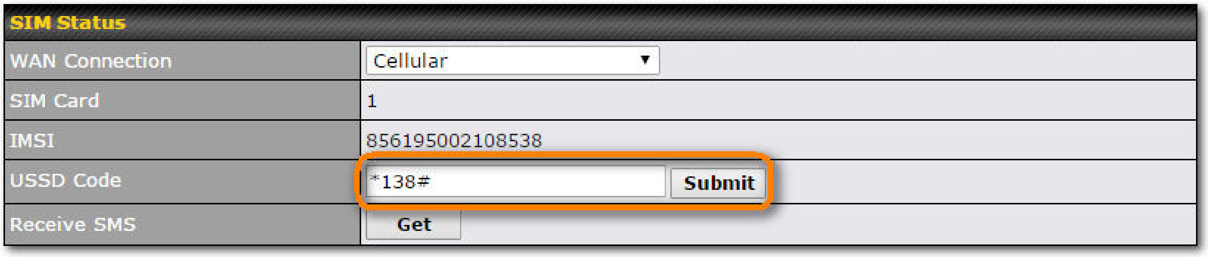
Unstructured Supplementary Service Data (USSD) is a protocol used by mobile phones to communicate with their service provider's computers. One of the most common uses is to query the available balance.



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

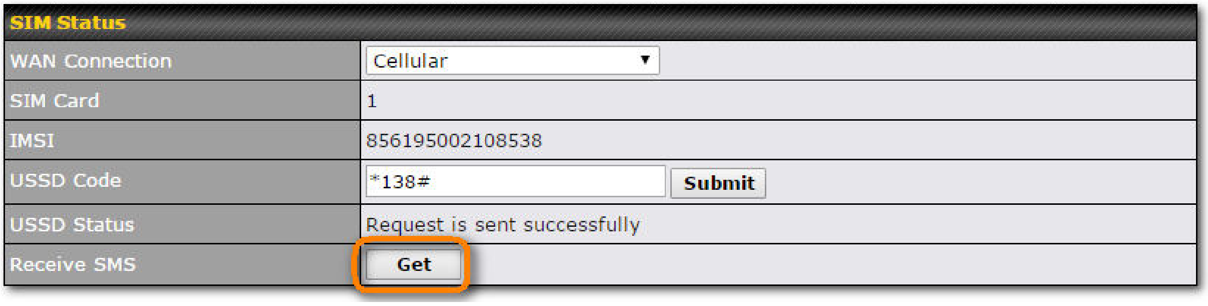
| USSD | |
|---|---|
| USSD Code | Submit |

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



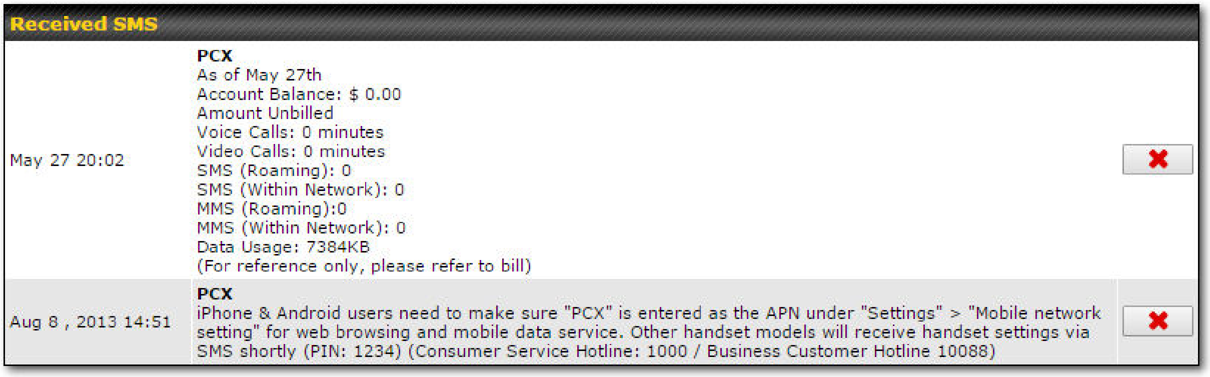
| SIM Status | |
|---|---|
| WAN Connection | Cellular ▾ |
| SIM Card | 1 |
| IMSI | 856195002108538 |
| USSD Code | *138# Submit |
| Receive SMS | Get |

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

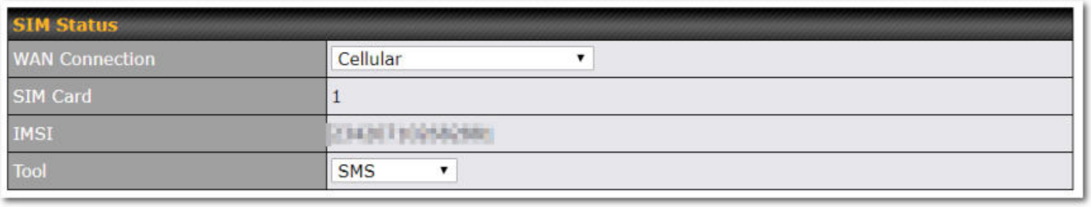


**Received SMS**

| | | |
|---|---|---|
| May 27 20:02 | **PCX**<br>As of May 27th<br>Account Balance: $ 0.00<br>Amount Unbilled<br>Voice Calls: 0 minutes<br>Video Calls: 0 minutes<br>SMS (Roaming): 0<br>SMS (Within Network): 0<br>MMS (Roaming):0<br>MMS (Within Network): 0<br>Data Usage: 7384KB<br>(For reference only, please refer to bill) | ✖ |
| Aug 8 , 2013 14:51 | **PCX**<br>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) | ✖ |

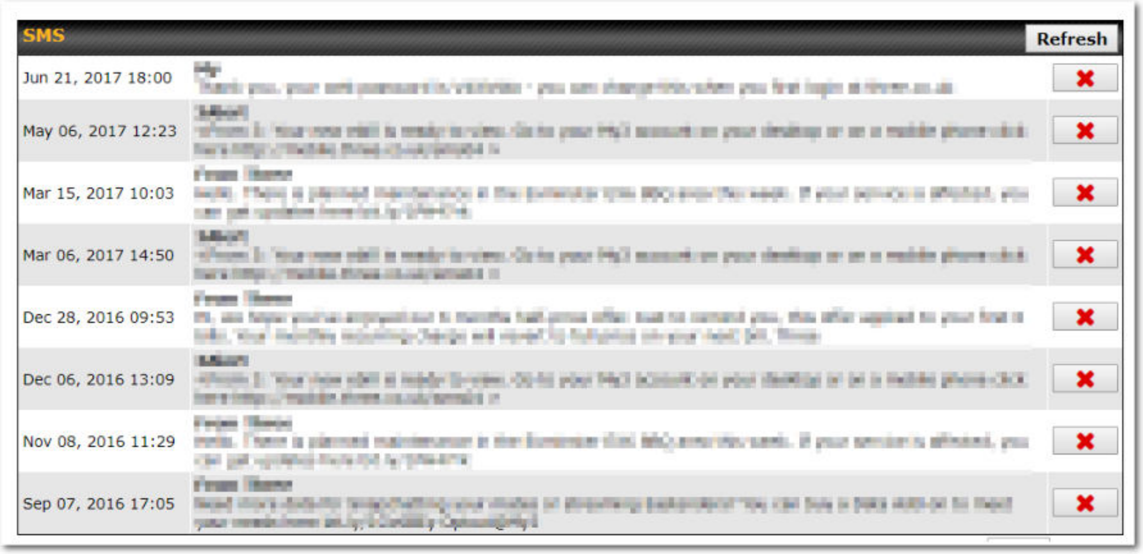
## SMS

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



**SIM Status**

| | |
|---|---|
| WAN Connection | Cellular ▾ |
| SIM Card | 1 |
| IMSI | [illegible] |
| Tool | SMS ▾ |



**SMS** Refresh

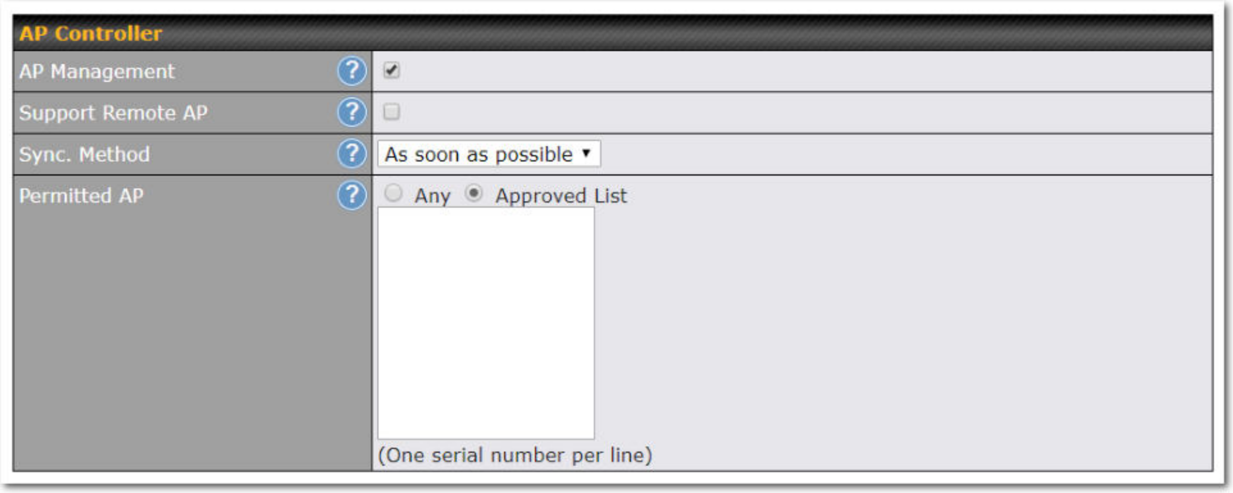
| | | |
|---|---|---|
| Jun 21, 2017 18:00 | [illegible] | ✖ |
| May 06, 2017 12:23 | [illegible] | ✖ |
| Mar 15, 2017 10:03 | [illegible] | ✖ |
| Mar 06, 2017 14:50 | [illegible] | ✖ |
| Dec 28, 2016 09:53 | [illegible] | ✖ |
| Dec 06, 2016 13:09 | [illegible] | ✖ |
| Nov 08, 2016 11:29 | [illegible]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

# 11 AP Tab

## 11.1 AP

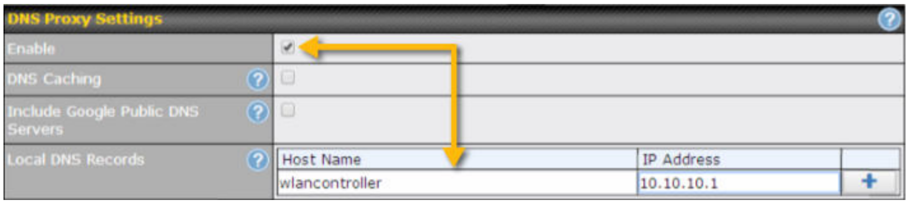
### 11.1.1 AP Controller

Clicking on the **AP** tab will default to this menu, where you can view basic AP management options:

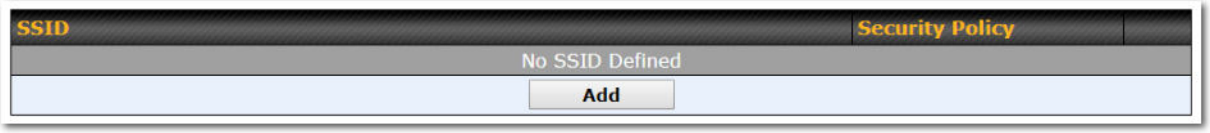


| AP Controller | |
|---|---|
| AP Management | ☑ |
| Support Remote AP | □ |
| Sync. Method | As soon as possible ▾ |
| Permitted AP | ○ Any ● Approved List<br>(One serial number per line) |

| 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. |
| **Support Remote AP** | The AP controller supports remote management of Pepwave APs. When this option is enabled, the AP controller will wait for management connections originating from remote APs over the WAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443.<br>The DHCP server and/or local DNS server of the remote AP's network should be configured in the **DNS Proxy Settings menu** under **Network>LAN**. The procedure is as follows:<br>1. Define an extended DHCP option, **CAPWAP Access Controller addresses** (field 138), in the DHCP server, where the values are the AP controller's public IP addresses; and/or<br>2. Create a local DNS record for the AP controller with a value corresponding to the AP controller's public IP address. |

| | |
|---|---|
| | <br>DNS Proxy Settings<br>Enable ☑<br>DNS Caching □<br>Include Google Public DNS Servers □<br>Local DNS Records<br>Host Name: wlancontroller<br>IP Address: 10.10.10.1 |
| **Sync. Method** | Select the required option to synchronize the managed AP's. Options are:<br>● As soon as possible (default)<br>● Progressively (synchronize AP's in groups)<br>● One at a time (synchronize one AP 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. |

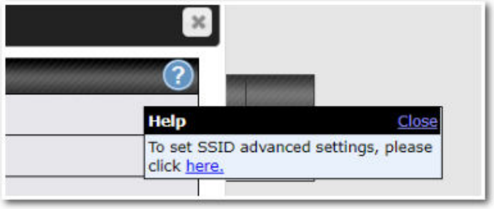
### 11.1.2 Wireless SSID



| SSID | Security Policy |
|---|---|
| No SSID Defined | |

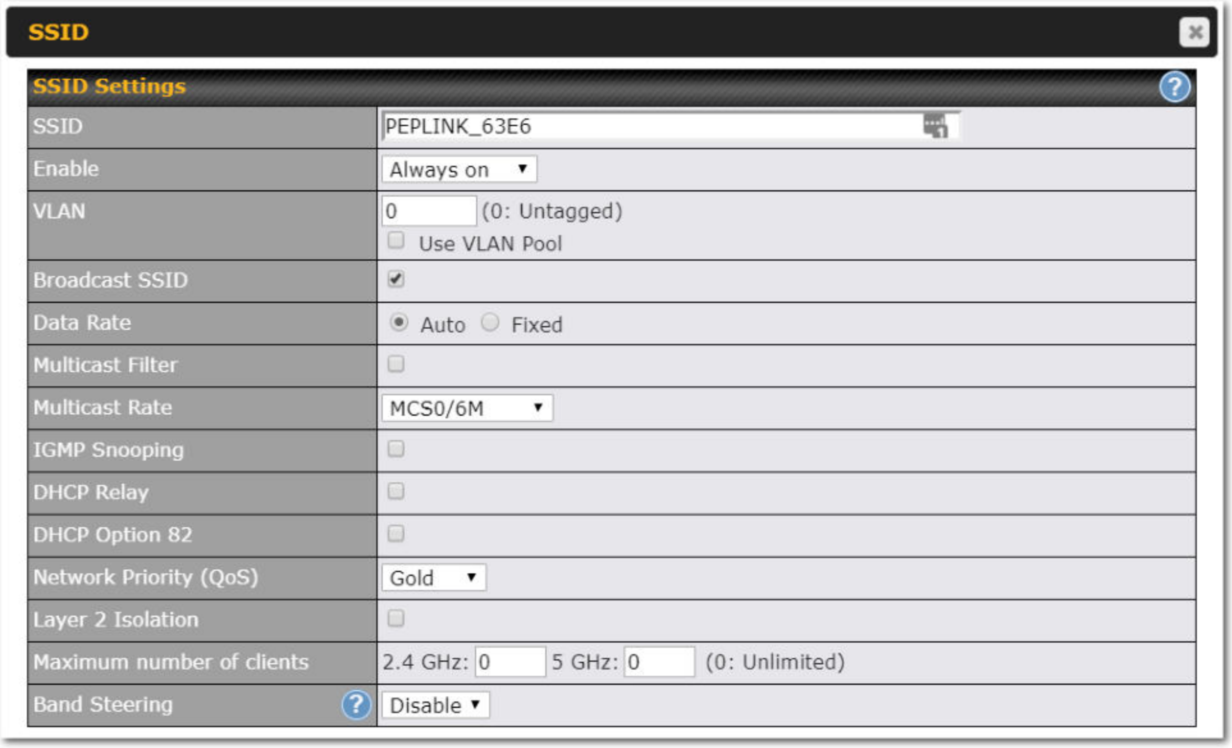
Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model.

The below settings show 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.



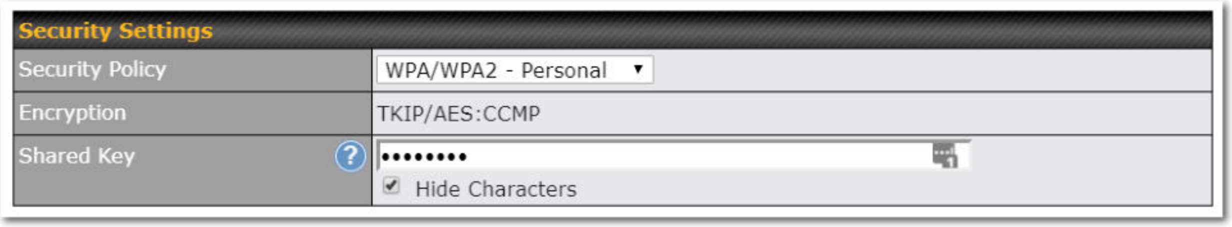
SSID

| SSID Settings | |
|---|---|
| SSID | PEPLINK_63E6 |
| Enable | Always on ▾ |
| VLAN | 0 (0: Untagged)<br>□ Use VLAN Pool |
| Broadcast SSID | ☑ |
| Data Rate | ● Auto ○ Fixed |
| Multicast Filter | □ |
| Multicast Rate | MCS0/6M ▾ |
| IGMP Snooping | □ |
| DHCP Relay | □ |
| DHCP Option 82 | □ |
| Network Priority (QoS) | Gold ▾ |
| Layer 2 Isolation | □ |
| Maximum number of clients | 2.4 GHz: 0 5 GHz: 0 (0: Unlimited) |
| Band Steering ? | Disable ▾ |

| SSID Settings | |
|---|---|
| **SSID** | This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients. |
| **Enable** | 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).<br>Use of a VLAN pool is enabled by selecting the checkbox. |
| **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. |

| | |
|---|---|
| **DHCP Relay** | Put the address of the DHCP server in this field..<br>DHCP requests will be relayed to this DHCP server |
| **DHCP Option 82** [A] | If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network. |
| **Layer 2 Isolation** [A] | **Layer 2** refers to the second layer in the ISO Open System Interconnect model.<br>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 upper communication layer(s). By default, the setting is disabled. |
| **Maximum Number of Clients** | Indicate the maximum number of clients that should be able to connect to each frequency. |
| **Band Steering** | To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency.<br>Choose between:<br>**Force** - Clients capable of 5 GHz operation are only offered with 5 GHz frequency.<br>**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.<br>**Disable** - Default |

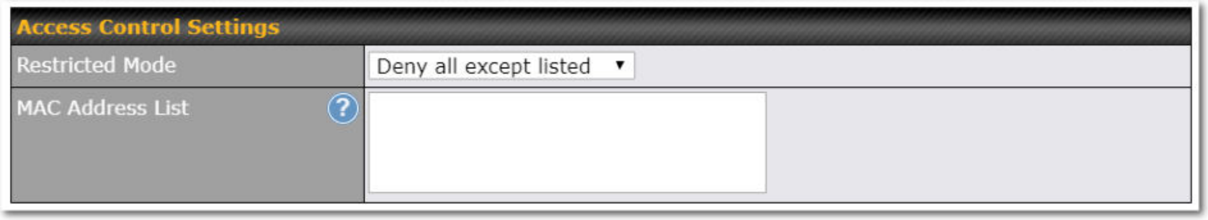
[A] - Advanced feature. Click the ? button on the top right-hand corner to activate.


Security Settings

| | |
|---|---|
| Security Policy | WPA/WPA2 - Personal ▼ |
| Encryption | TKIP/AES:CCMP |
| Shared Key ? | ••••••••<br>☑ Hide Characters |

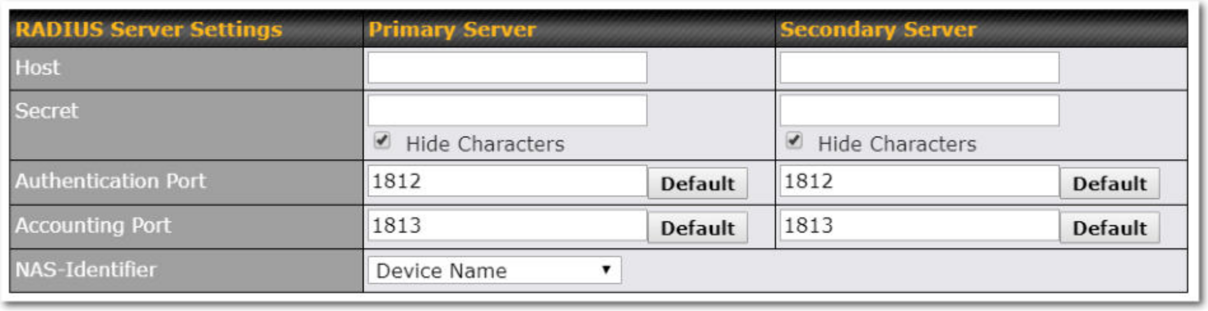
| Security Settings | |
|---|---|
| **Security Policy** | This setting configures the wireless authentication and encryption methods. Available options:<br>● **Open (**No Encryption)<br>● **Enhanced Open** (OWE)<br>● **WPA3 -Personal** (AES:CCMP)<br>● **WPA2/WPA3 -Personal** (AES:CCMP)<br>● **WPA2 -Personal**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

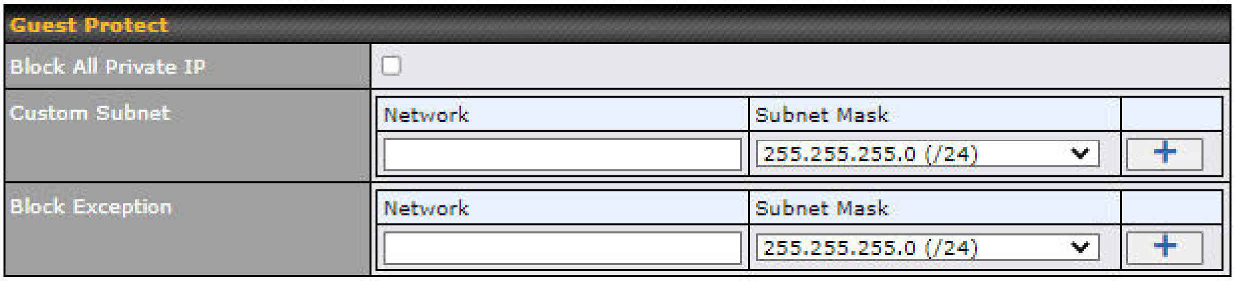
| Access Control Settings | |
|---|---|
| **Restricted Mode** | The settings allow the administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, **Accept all except listed** and **Radius MAC Authentication.** |
| **MAC Address List** | Connections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



| RADIUS Server Settings | Primary Server | Secondary Server |
|---|---|---|
| Host | | |
| Secret | ☑ Hide Characters | ☑ Hide Characters |
| Authentication Port | 1812 Default | 1812 Default |
| Accounting Port | 1813 Default | 1813 Default |
| NAS-Identifier | Device Name ▾ | |

| RADIUS Server Settings | |
|---|---|
| **Host** | Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server. |
| **Secret** | Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server. |
| **Authentication Port** | In the field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the **Default** button to enter **1812**. |
| **Accounting** | In the field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the |

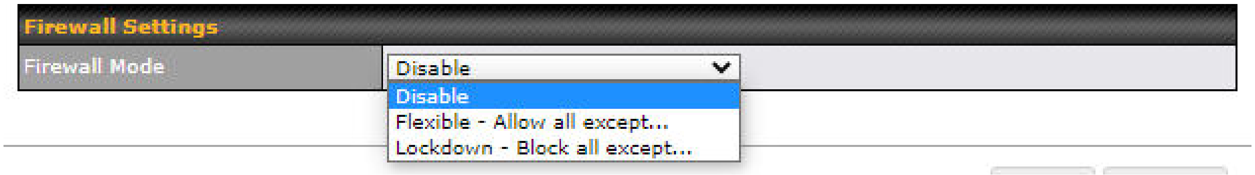
| | |
|---|---|
| **Port** | **Default** button to enter **1813**. |
| **NAS-Identifier** | Choose between **Device Name**, **LAN MAC address**, **Device Serial Number** and **Custom Value** |



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. |



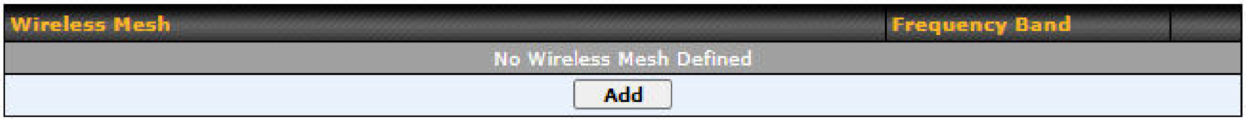
Firewall Settings

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.<br>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** |

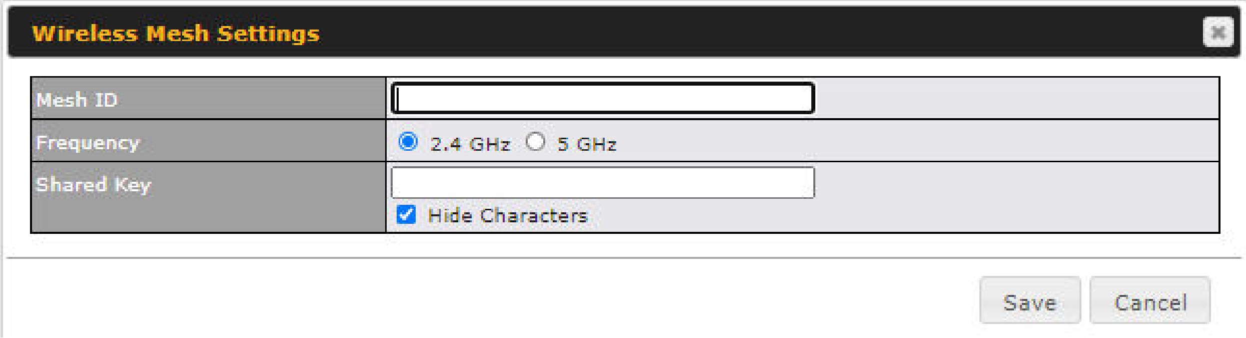
### 11.1.3 Wireless Mesh



| Wireless Mesh | Frequency Band | |
|---|---|---|
| No Wireless Mesh Defined | | |
| Add | | |

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**.



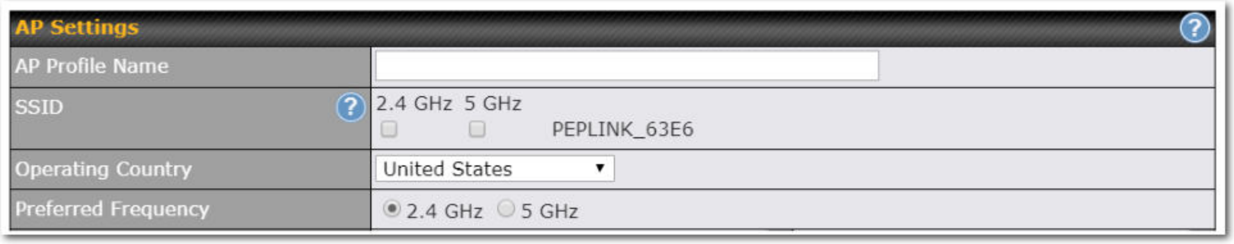
Wireless Mesh Settings

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

Save Cancel

| 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.<br>Click **Hide / Show Characters** to toggle visibility. |

### 11.1.4 AP > Profiles

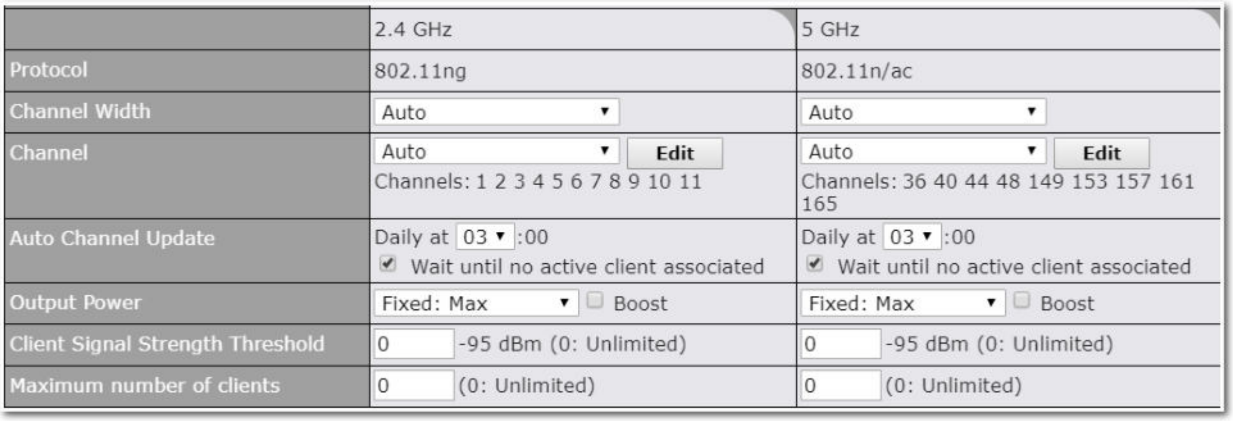


| AP Settings | |
|---|---|
| AP Profile Name | |
| SSID | 2.4 GHz 5 GHz<br>□ □ PEPLINK_63E6 |
| Operating Country | United States |
| Preferred Frequency | ● 2.4 GHz ○ 5 GHz |

| AP Settings | |
|---|---|
| **AP Profile Name** | Ap Profile name |

| | |
|---|---|
| **SSID** | You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID. |
| **Operating Country** | This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow.<br>● 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).<br>● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).<br>NOTE: Users are required to choose an option suitable to local laws and regulations. |
| **Preferred Frequency** | Indicate the preferred frequency to use for clients to connect. |

| 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. |

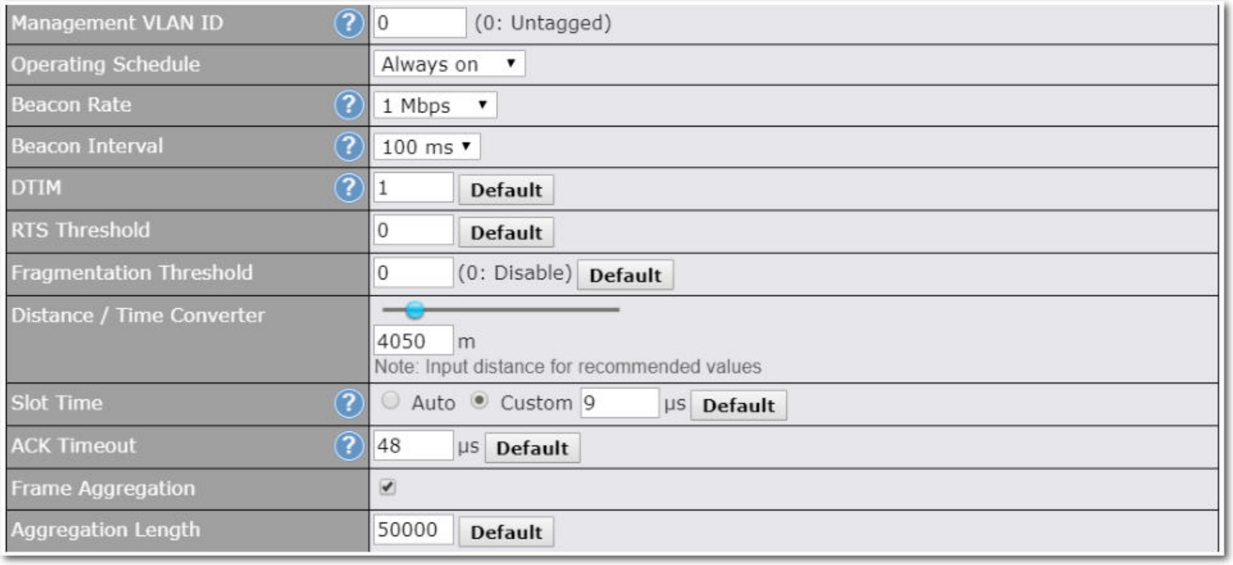


| | 2.4 GHz | 5 GHz |
|---|---|---|
| Protocol | 802.11ng | 802.11n/ac |
| Channel Width | Auto ▾ | Auto ▾ |
| Channel | Auto ▾ Edit<br>Channels: 1 2 3 4 5 6 7 8 9 10 11 | Auto ▾ Edit<br>Channels: 36 40 44 48 149 153 157 161 165 |
| Auto Channel Update | Daily at 03 ▾ :00<br>☑ Wait until no active client associated | Daily at 03 ▾ :00<br>☑ Wait until no active client associated |
| Output Power | Fixed: Max ▾ □ Boost | Fixed: Max ▾ □ Boost |
| Client Signal Strength Threshold | 0 -95 dBm (0: Unlimited) | 0 -95 dBm (0: Unlimited) |
| Maximum number of clients | 0 (0: Unlimited) | 0 (0: Unlimited) |

| AP Settings (part 2) | |
|---|---|
| **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** | Available options are **20 MHz**, **40 MHz**, and **Auto (20/40 MHz)** . Default is **Auto (20/40 MHz),** which allows both widths to be used simultaneously. |
| **Channel** | This option allows you to select which 802.11 RF channel will be utilized. **Channel 1 (2.412 GHz)** is selected by default. |
| **Auto Channel Update** | Indicate the time of day at which update automatic channel selection. |
| **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. |
| **Client Signal Strength Threshold** | Clients with signal strength lower than this value will not be allowed to connect. |

| | |
|---|---|
| **Maximum number of clients** | This setting determines the maximum number of clients that can connect to this Wi-Fi frequency. |

Advanced Wi-Fi AP settings can be displayed by clicking the ? on the top right-hand corner of the **Wi-Fi AP Settings** section, which can be found at **AP>Settings**. Other models will display a separate section called **Wi-Fi AP Advanced Settings**, which can be found at **Advanced>Wi-Fi Settings**.

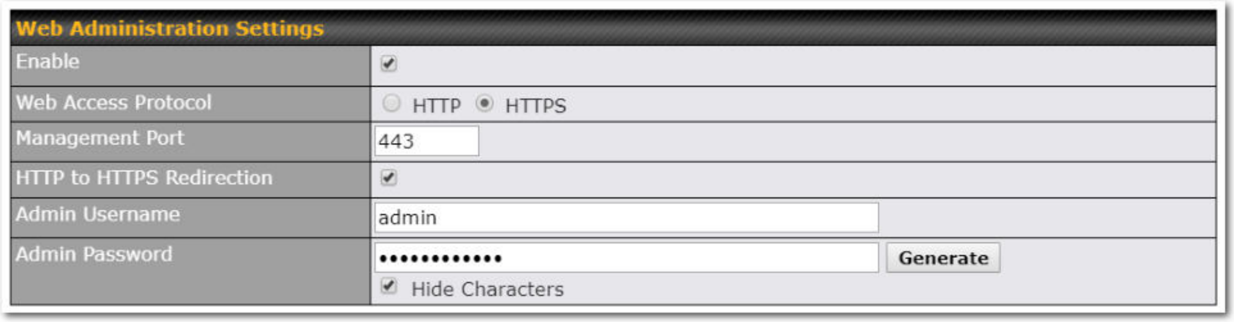


| | |
|---|---|
| Management VLAN ID | 0 (0: Untagged) |
| Operating Schedule | Always on ▾ |
| Beacon Rate | 1 Mbps ▾ |
| Beacon Interval | 100 ms ▾ |
| DTIM | 1 Default |
| RTS Threshold | 0 Default |
| Fragmentation Threshold | 0 (0: Disable) Default |
| Distance / Time Converter | 4050 m<br>Note: Input distance for recommended values |
| Slot Time | ○ Auto ● Custom 9 μs Default |
| ACK Timeout | 48 μs Default |
| Frame Aggregation | ☑ |
| Aggregation Length | 50000 Default |

| Advanced AP Settings | |
|---|---|
| **Management VLAN ID** | This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means that no VLAN tagging will be applied.<br>NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller. |
| **Operating Schedule** | Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu. |
| **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. |
| **DTIM** [A] | This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**. |
| **RTS Threshold** [A] | The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500. |

| | |
|---|---|
| **Fragmentation Threshold** [A] | This setting determines the maximum size of a packet before it gets fragmented into multiple pieces. |
| **Distance / Time Convertor** | Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout. |
| **Slot Time** [A] | This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 μs**. |
| **ACK Timeout** [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 Aggregation** [A] | This option allows you to enable frame aggregation to increase transmission throughput. |

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



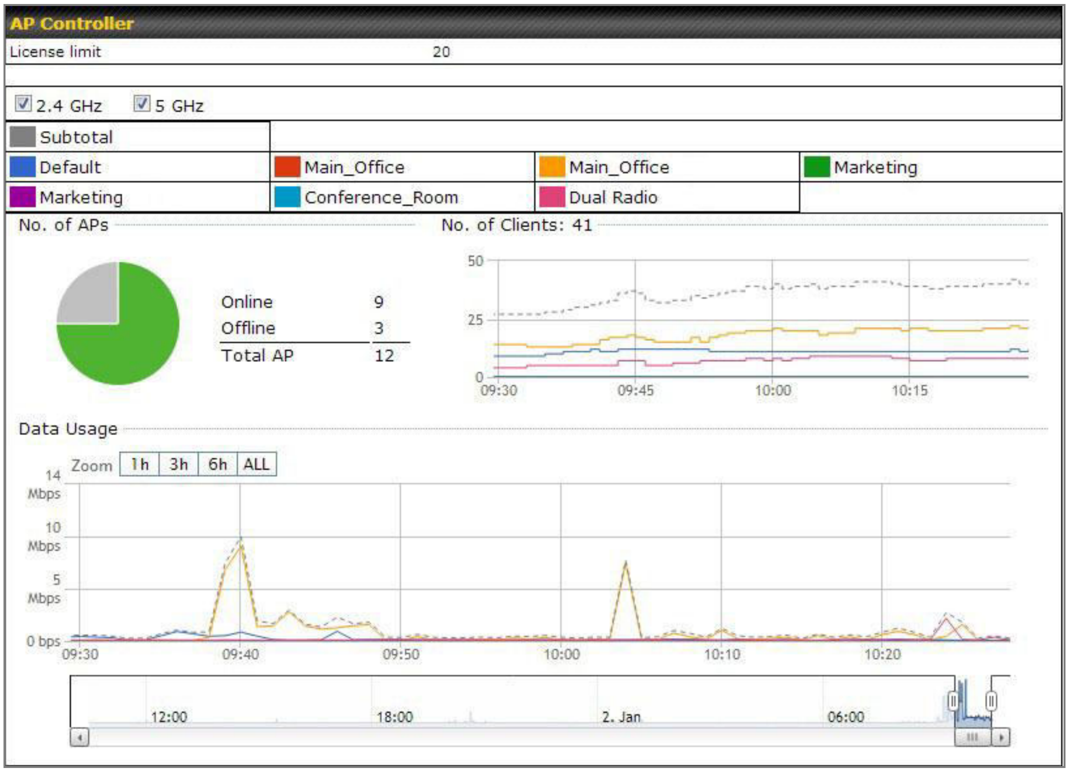
| Web Administration Settings | |
|---|---|
| Enable | ☑ |
| Web Access Protocol | ○ HTTP ● HTTPS |
| Management Port | 443 |
| HTTP to HTTPS Redirection | ☑ |
| Admin Username | admin |
| Admin Password | •••••••••••• Generate<br>☑ Hide Characters |

| Web Administration Settings | |
|---|---|
| **Enable** | Ticking this box enables web admin access for APs located on the WAN. |
| **Web Access Protocol** | Determines whether the web admin portal can be accessed through HTTP or HTTPS |
| **Management Port** | Determines the port at which the management UI can be accessed. |
| **HTTP to HTTPS redirection** | Redirects HTTP request to HTTPS |
| **Admin Username** | Determines the username to be used for logging into the web admin portal |
| **Admin Password** | Determines the password for the web admin portal on external AP. |

## 11.2 AP Controller Status

### 11.2.1 Info

A comprehensive overview of your AP can be accessed by navigating to **AP > 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

Data Usage

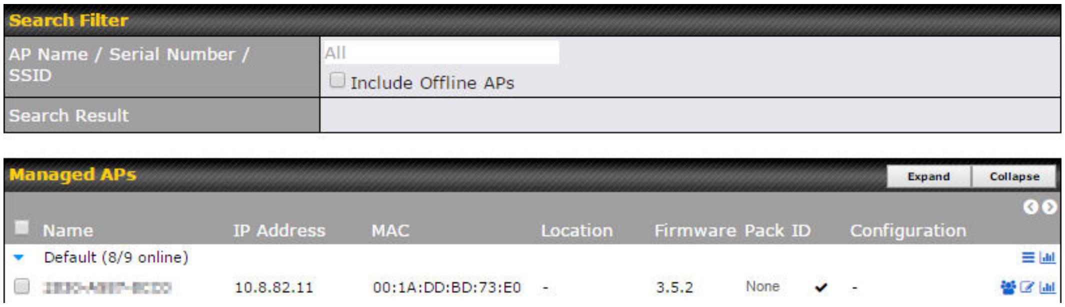
| AP Controller | |
|---|---|
| **License Limit** | This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage. |
| **Frequency** | Underneath, there are two check boxes labeled **2.4 Ghz** and **5 Ghz**. Clicking 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.

### 11.2.2 Access Points (Usage)

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



**Search Filter**

| | |
|---|---|
| AP Name / Serial Number / SSID | All<br>□ Include Offline APs |
| Search Result | |

**Managed APs** Expand Collapse

| □ | Name | IP Address | MAC | Location | Firmware | Pack ID | | Configuration | |
|---|---|---|---|---|---|---|---|---|---|
| ▾ | Default (8/9 online) | | | | | | | | ☰ 📊 |
| □ | [redacted] | 10.8.82.11 | 00:1A:DD:BD:73:E0 | - | 3.5.2 | None | ✓ | - | 👥 ✎ 📊 |

## Usage

**AP Name/Serial Number**

This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.

**Online Status**

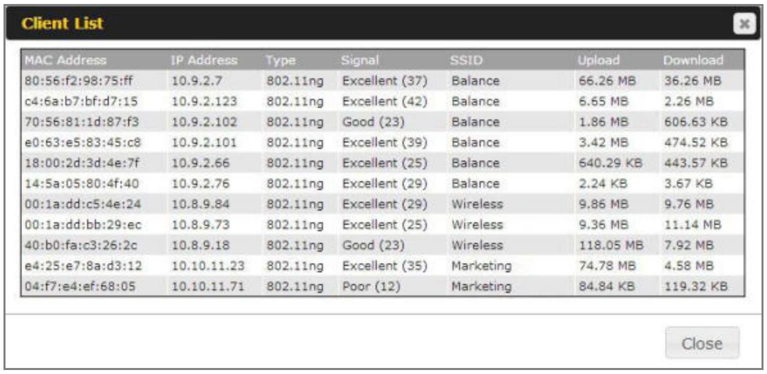
This button toggles whether your search will include offline devices.

**Managed Wireless Devices**

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. You could also expand and collapse all groups by using the Expand Collapse buttons.

On the right of the table, you will see the following icons: 👥 ✎ 📊 .

Click the 👥 icon to see a usage table for each client:

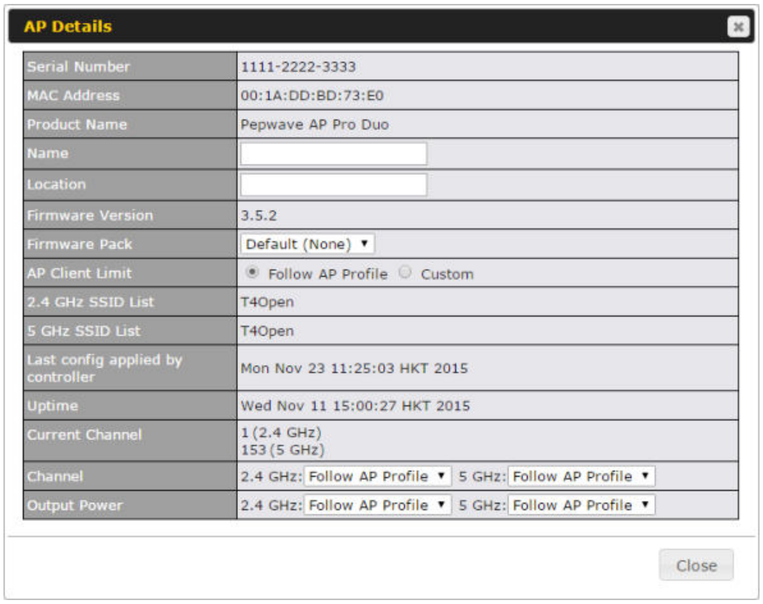


**Client List** ✖

| 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 |

Close

Click the ✎ icon to configure each client

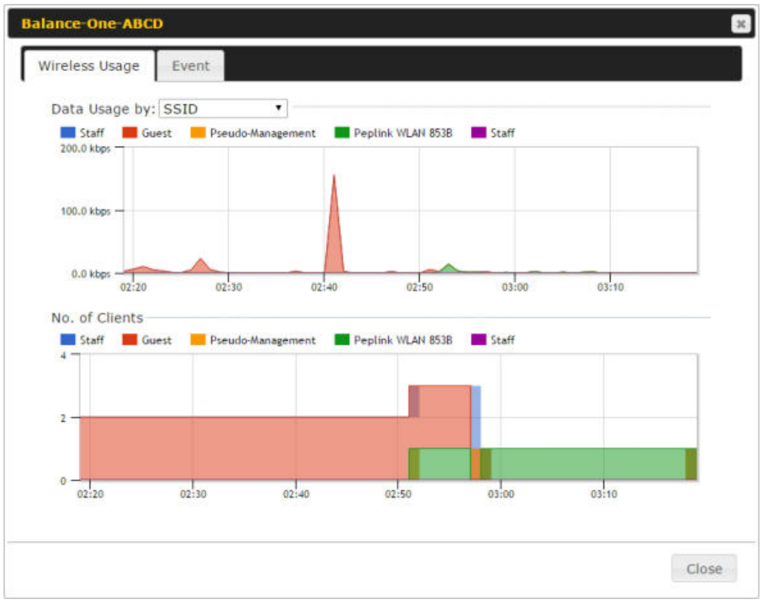


AP Details

| | |
|---|---|
| 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)<br>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 ▾ |

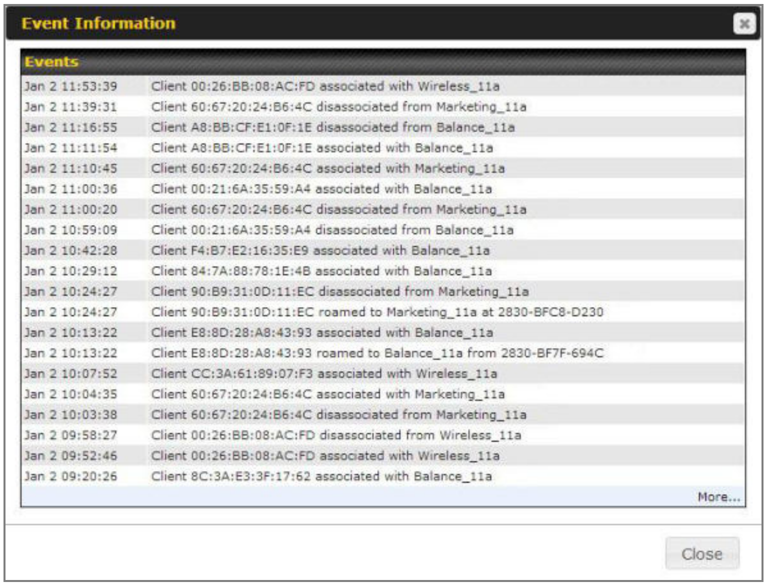
For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

Click the 📊 icon to see a graph displaying usage:



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.

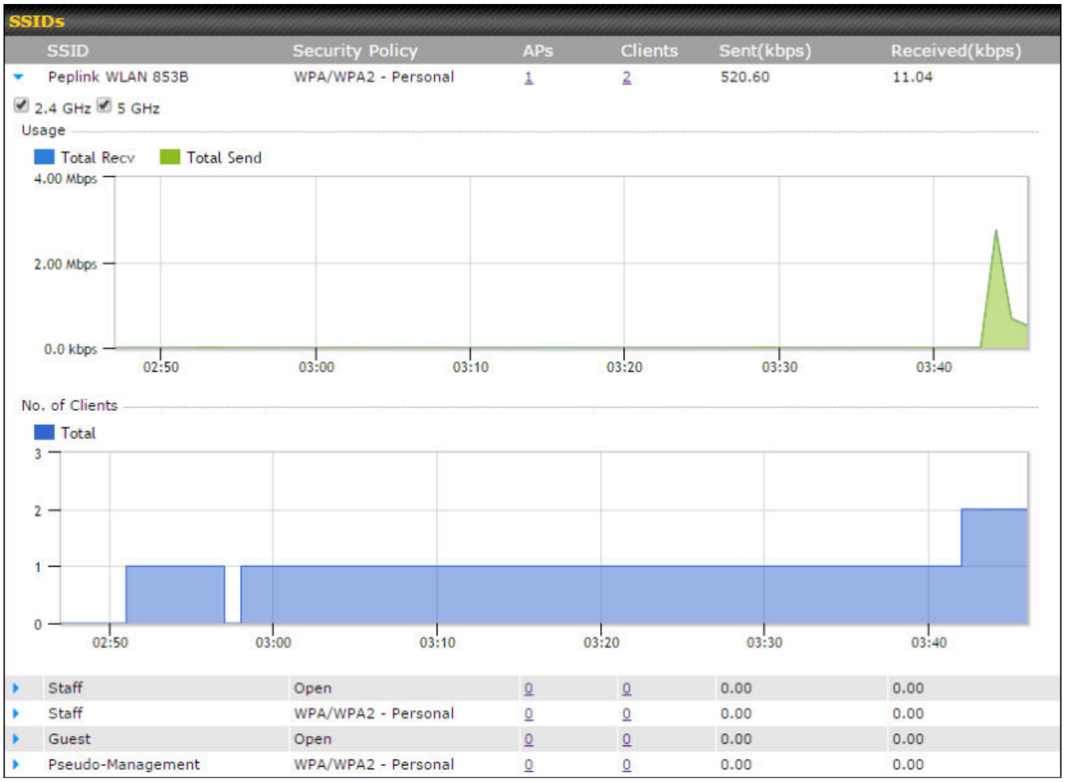
Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:



```
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
```

### 11.2.3 Wireless SSID

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



**SSIDs**

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

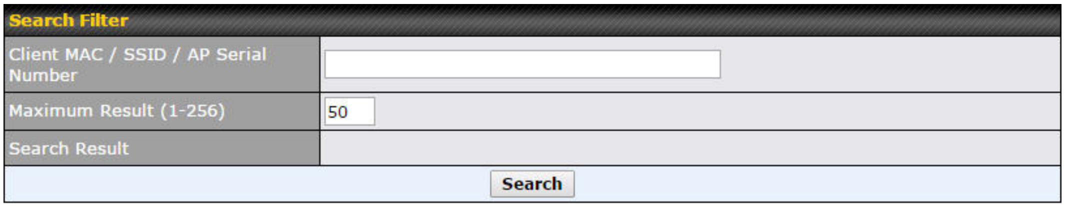
☑ 2.4 GHz ☑ 5 GHz

| | 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.

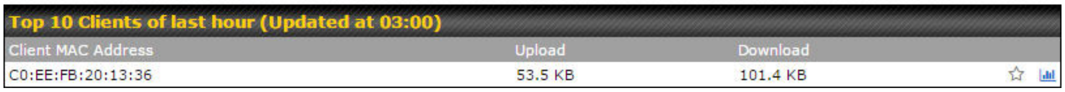
### 11.2.4 Wireless Client

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



**Search Filter**

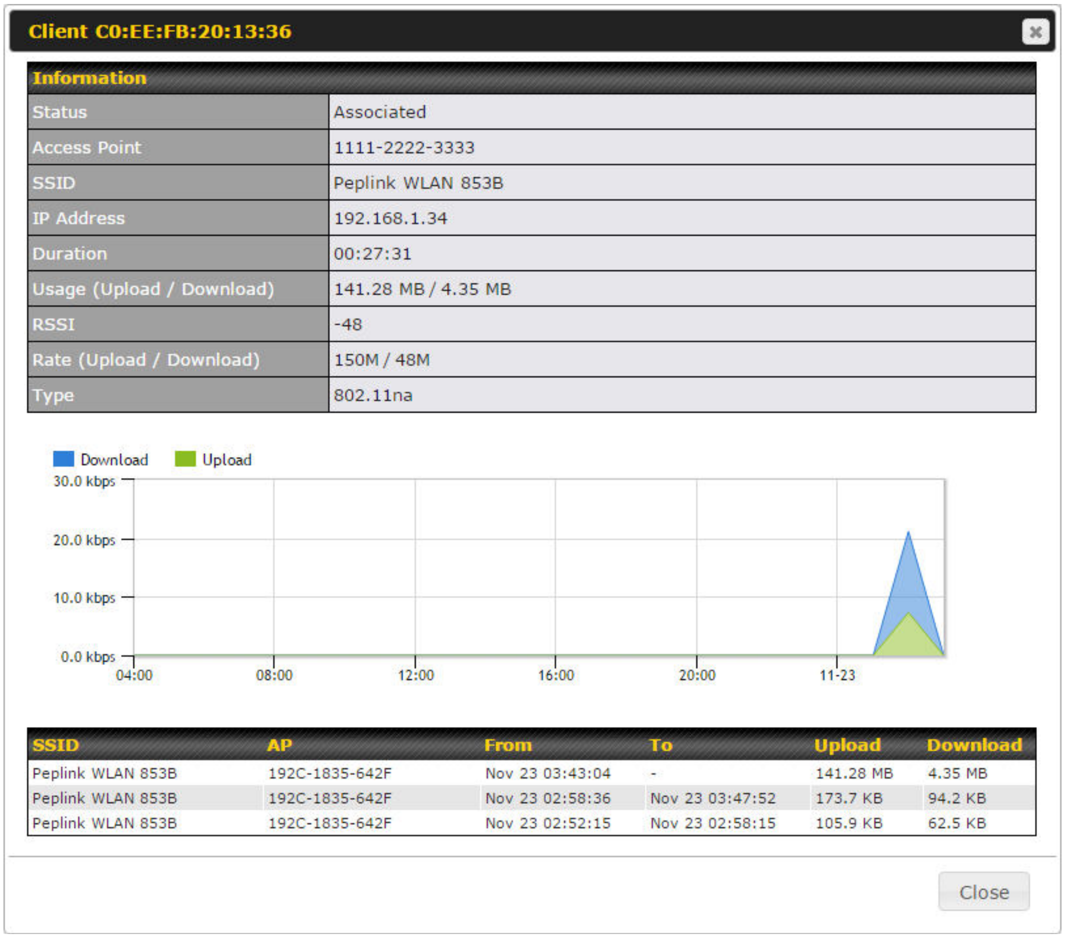
| | |
|---|---|
| Client MAC / SSID / AP Serial Number | |
| Maximum Result (1-256) | 50 |
| Search Result | |



**Top 10 Clients of last hour (Updated at 03:00)**

| Client MAC Address | Upload | Download | |
|---|---|---|---|
| C0:EE:FB:20:13:36 | 53.5 KB | 101.4 KB | ☆ 📊 |

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:



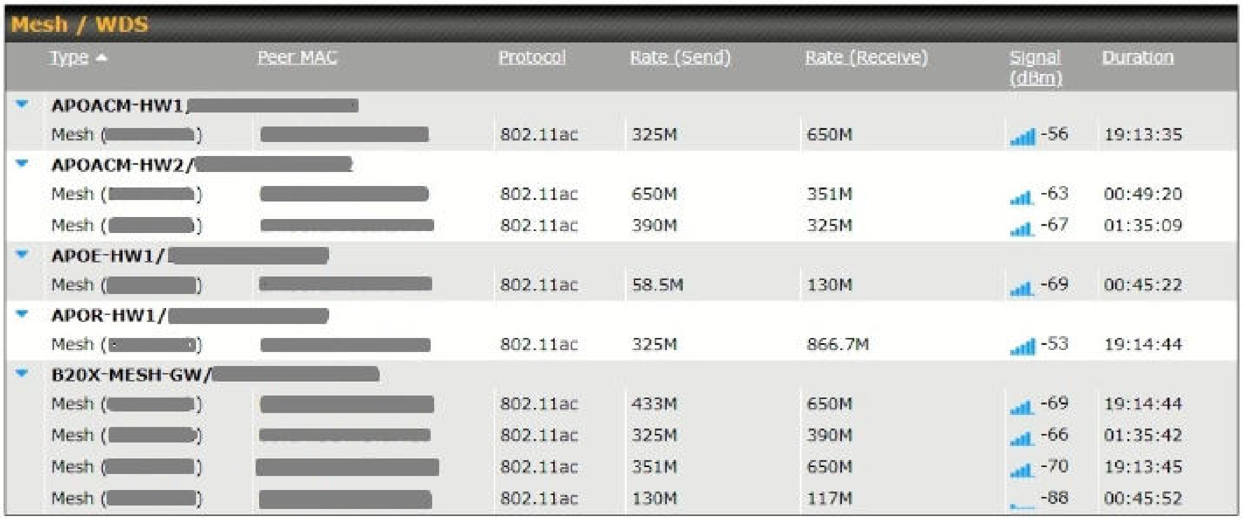
Client C0:EE:FB:20:13:36

| 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 |

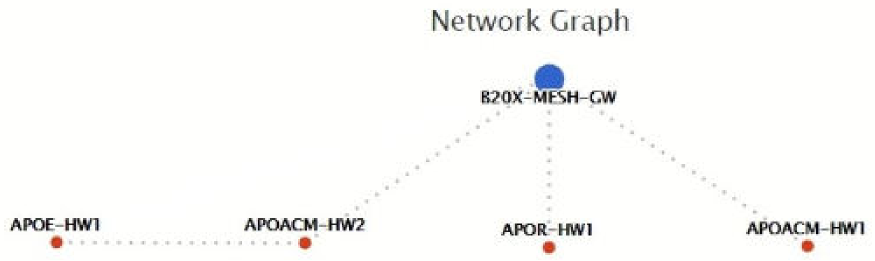
### 11.2.5 Mesh / WDS

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.



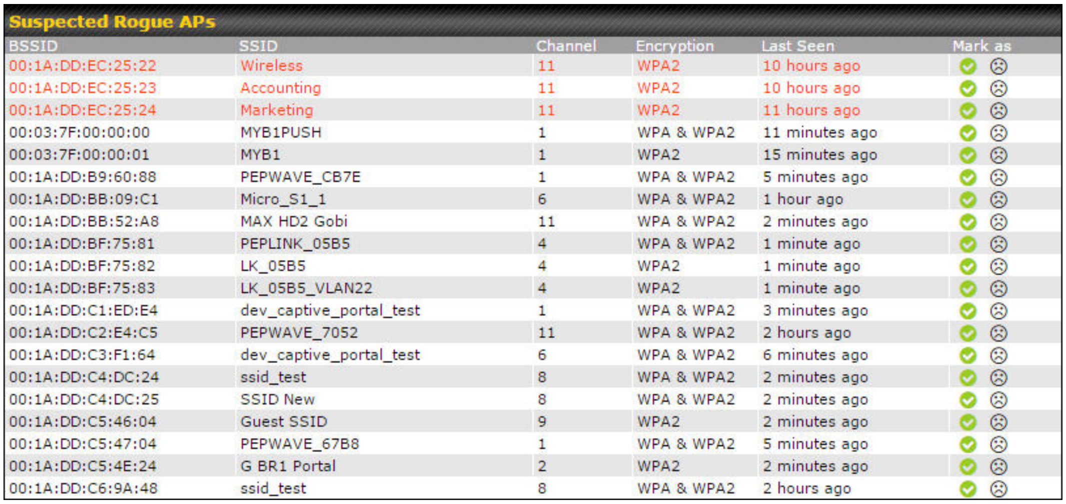
Mesh / WDS

| 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 |



### 11.2.6 Nearby Device

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



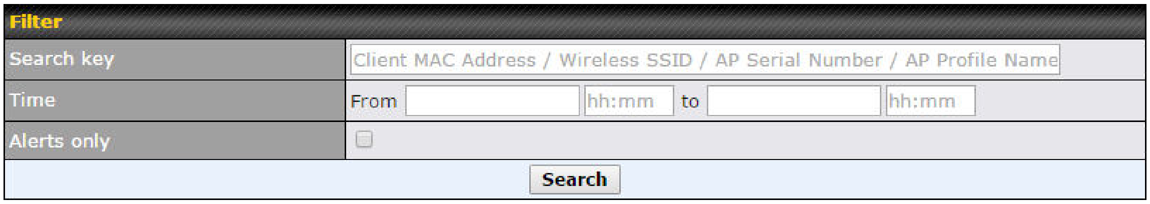
Suspected Rogue APs

| 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 | ✓ ☹ |

| Nearby 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. |

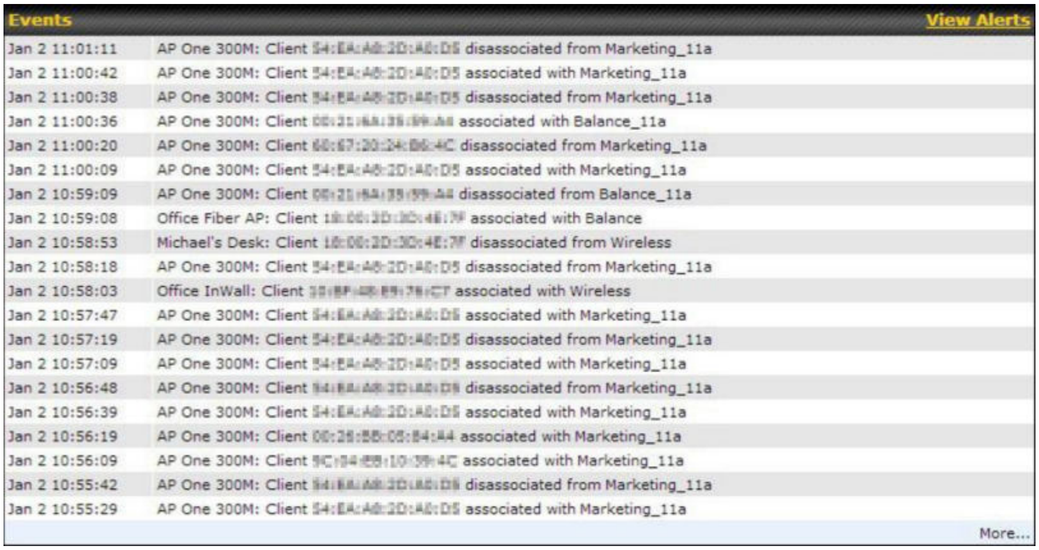
### 11.2.7 Event Log

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 | □ |

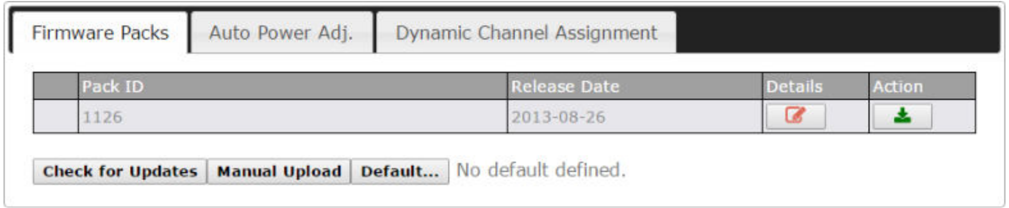


```
Jan 2 11:01:11   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client [redacted] associated with Balance_11a
Jan 2 11:00:20   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 11:00:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:59:09   AP One 300M: Client [redacted] disassociated from Balance_11a
Jan 2 10:59:08   Office Fiber AP: Client [redacted] associated with Balance
Jan 2 10:58:53   Michael's Desk: Client [redacted] disassociated from Wireless
Jan 2 10:58:18   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:58:03   Office InWall: Client [redacted] associated with Wireless
Jan 2 10:57:47   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:57:19   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:57:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:48   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:56:39   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:19   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:56:09   AP One 300M: Client [redacted] associated with Marketing_11a
Jan 2 10:55:42   AP One 300M: Client [redacted] disassociated from Marketing_11a
Jan 2 10:55:29   AP One 300M: Client [redacted] 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. |

## 11.3 Toolbox

Additional tools for managing firmware packs, power adjustment, and channel assignment can be found at **AP>Toolbox**.



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

No default defined.

| Firmware Packs |
|---|
| This is the first menu that will appear. Here, you can manage the firmware of your AP. Clicking on 📝 will display information regarding each firmware pack. To receive new firmware packs, you can either press Check for Updates to download new packs or you can press Manual Upload to manually upload a firmware pack. Press Default... to define which firmware pack is default. |

# 12 System Tab

## 12.1 System

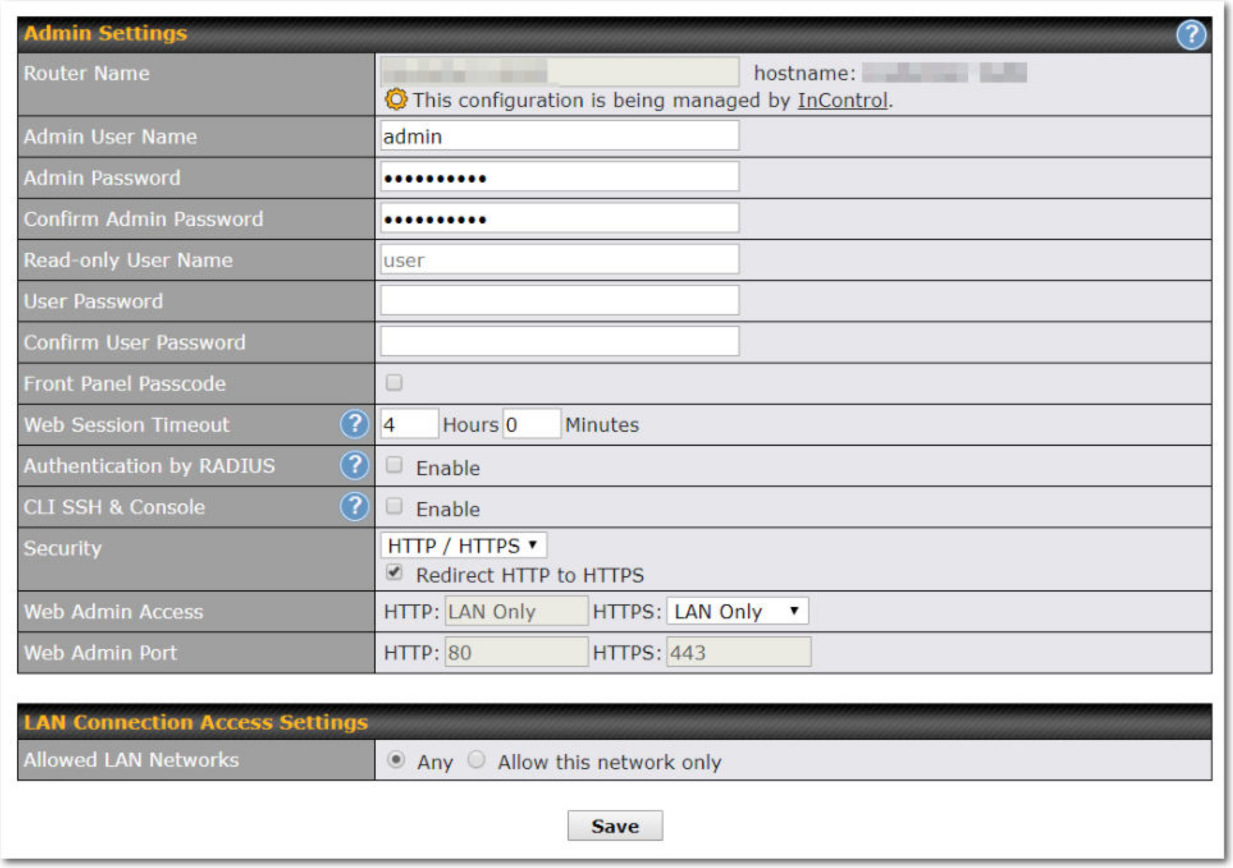
### 12.1.1 Admin Security

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**.

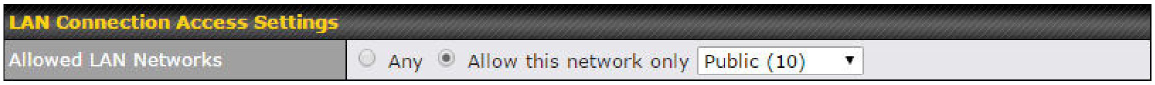


| | |
|---|---|
| **Admin Settings** | |
| Router Name | [redacted] hostname: [redacted]<br>This configuration is being managed by InControl. |
| Admin User Name | admin |
| Admin Password | •••••••••• |
| Confirm Admin Password | •••••••••• |
| Read-only User Name | user |
| User Password | |
| Confirm User Password | |
| Front Panel Passcode | □ |
| Web Session Timeout | 4 Hours 0 Minutes |
| Authentication by RADIUS | □ Enable |
| CLI SSH & Console | □ Enable |
| Security | HTTP / HTTPS<br>☑ Redirect HTTP to HTTPS |
| Web Admin Access | HTTP: LAN Only HTTPS: LAN Only |
| Web Admin Port | HTTP: 80 HTTPS: 443 |
| **LAN Connection Access Settings** | |
| Allowed LAN Networks | ● Any ○ Allow this network only |

| Admin Settings | |
|---|---|
| **Router Name** | This field allows you to define a name for this Pepwave router. By default, **Router 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. |
| **User 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 User 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 by RADIUS** | 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. |
| **Auth Protocol** | This specifies the authentication protocol used. Available options are **MS-CHAP v2** and **PAP**. |
| **Auth Server** | This specifies the access address and port of the external RADIUS server. |
| **Auth Server Secret** | This field is for entering the secret key for accessing the RADIUS server. |
| **Auth Timeout** | This option specifies the time value for authentication timeout. |
| **Accounting Server** | This specifies the access address and port of the external accounting server. |
| **Accounting Server Secret** | This field is for entering the secret key for accessing the accounting server. |
| **Network Connection** | This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections. |
| **CLI SSH** | The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to **Section 15.3.** |
| **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 Login Grace Time** | This option specifies the time for CLI SSH login. The default value is 120. |
| **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:<br>● HTTP |

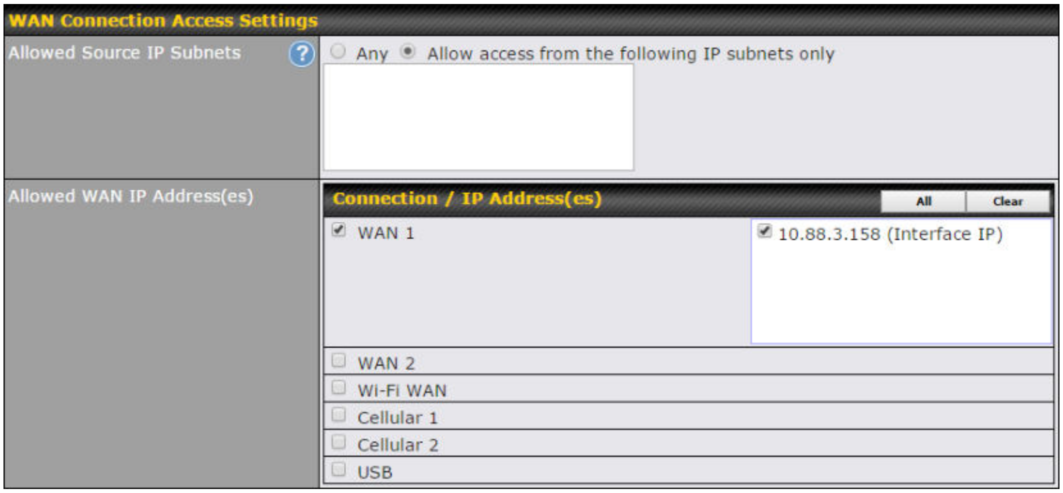
| | |
|---|---|
| | - HTTPS<br>- HTTP/HTTPS<br>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface. |
| **Web Admin Port** | This field is for specifying the port number on which the web admin interface can be accessed. |
| **Web Admin Access** | This option is for specifying the network interfaces through which the web admin interface can be accessed:<br>- LAN only<br>- LAN/WAN<br>If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed. |



LAN Connection Access Settings

Allowed LAN Networks ○ Any ● Allow this network only Public (10) ▾

| LAN Connection Access Settings | |
|---|---|
| **Allowed LAN Networks** | This field allows you to permit only specific networks or VLANs to access the Web UI. |



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

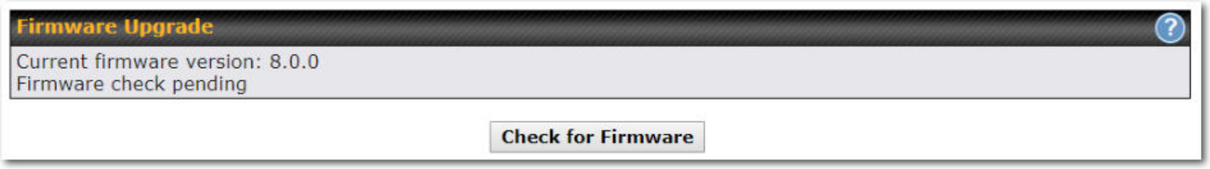
☐ USB

| WAN Connection Access Settings | |
|---|---|
| **Allowed Source IP Subnets** | This field allows you to restrict web admin access only from defined IP subnets.<br>- **Any** - Allow web admin accesses to be from anywhere, without IP address restriction.<br>- **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:<br>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*).<br>To define multiple subnets, separate each IP subnet one in a line. For example:<br>● 192.168.0.0/24<br>● 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. |

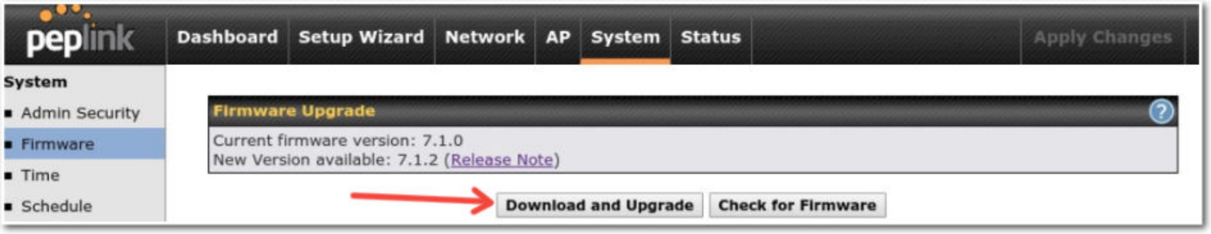
### 12.1.2 Firmware

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: 8.0.0
Firmware check pending

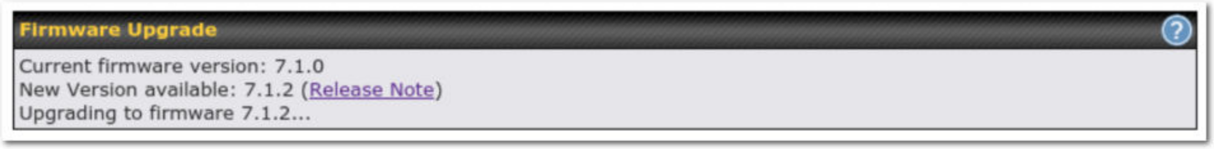
If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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

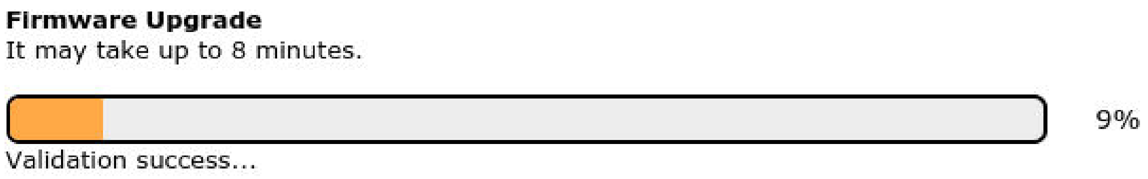
Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

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%

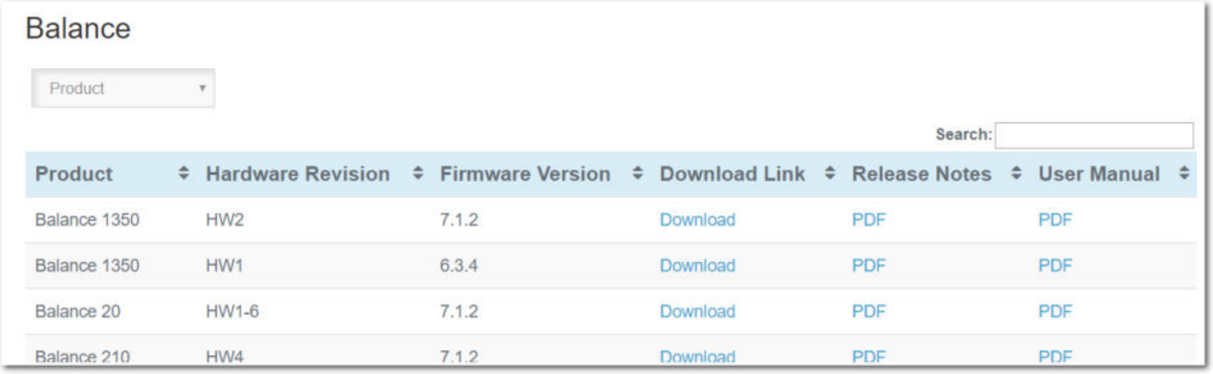
Validation success...

***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.



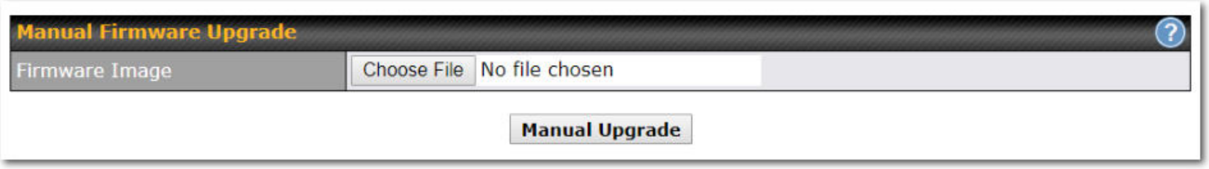
Balance

| 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.

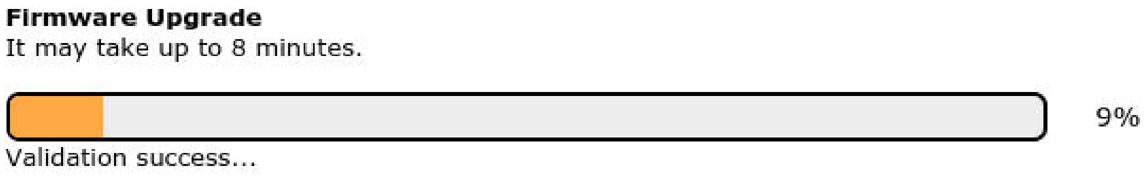
Click on the Manual Upgrade button to start the upgrade process.



**Manual Firmware Upgrade**

Firmware Image: Choose File No file chosen

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...

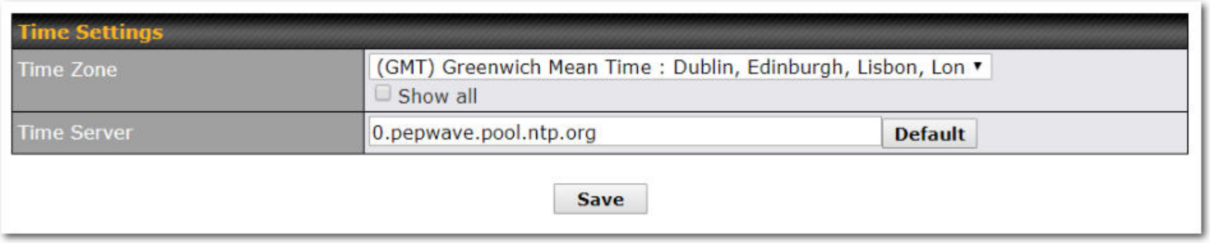
***Upgrading the firmware will cause the router to reboot.**

### The InControl method

[Described in this knowledgebase article on our forum.]

### 12.1.3 Time

The time server functionality enables the system clock of the Peplink Balance to be synchronized with a specified time server. The settings for time server configuration are located at **System>Time**.

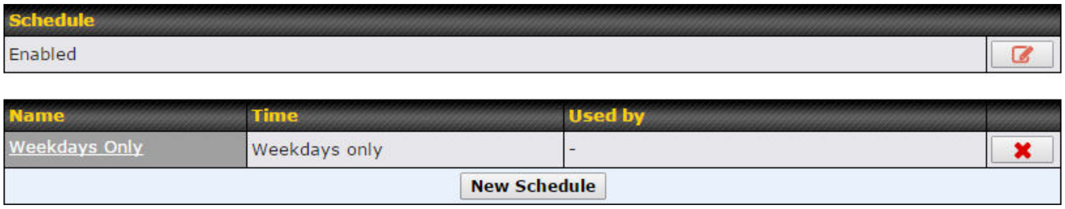


| Time Settings | |
|---|---|
| Time Zone | (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▾<br>□ Show all |
| Time Server | 0.pepwave.pool.ntp.org [Default] |

| Time Settings | |
|---|---|
| **Time Zone** | This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which Peplink Balance operates. The **Time Zone** value affects the time stamps in the event log of the Peplink Balance and e-mail notifications. Check **Show all** to show all time zone options. |
| **Time Server** | This setting specifies the NTP network time server to be utilized by the Peplink Balance. |

### 12.1.4 Schedule

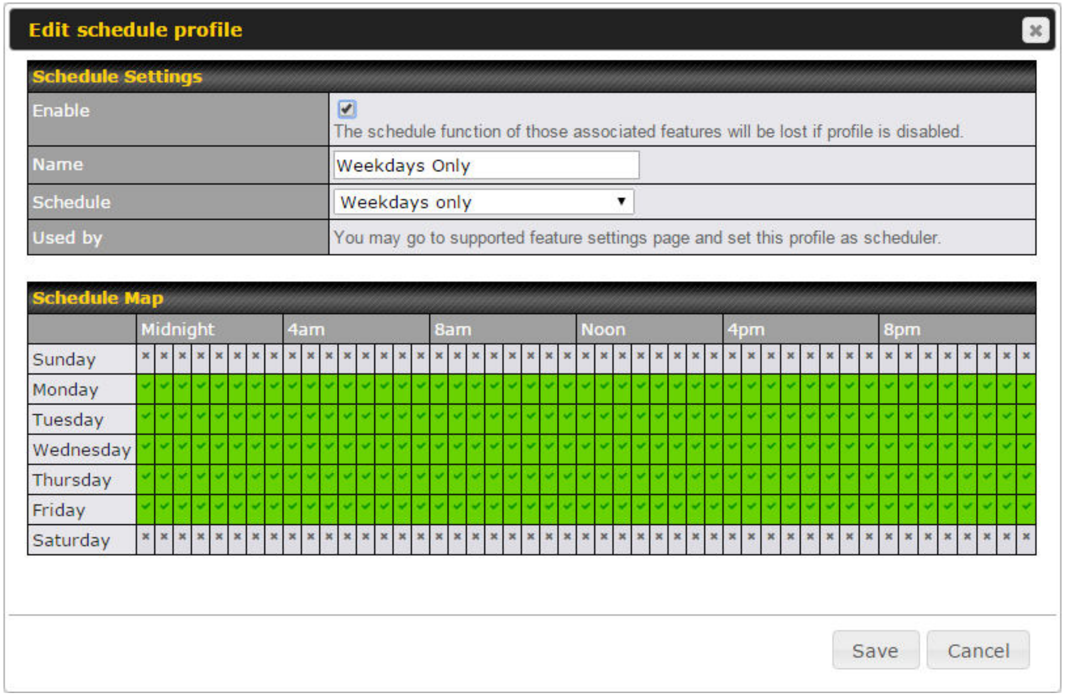
Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**



| Schedule | |
|---|---|
| Enabled | |

| Name | Time | Used by | |
|---|---|---|---|
| Weekdays Only | Weekdays only | - | ✖ |

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



| Schedule Settings | |
|---|---|
| Enable | ☑<br>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. |

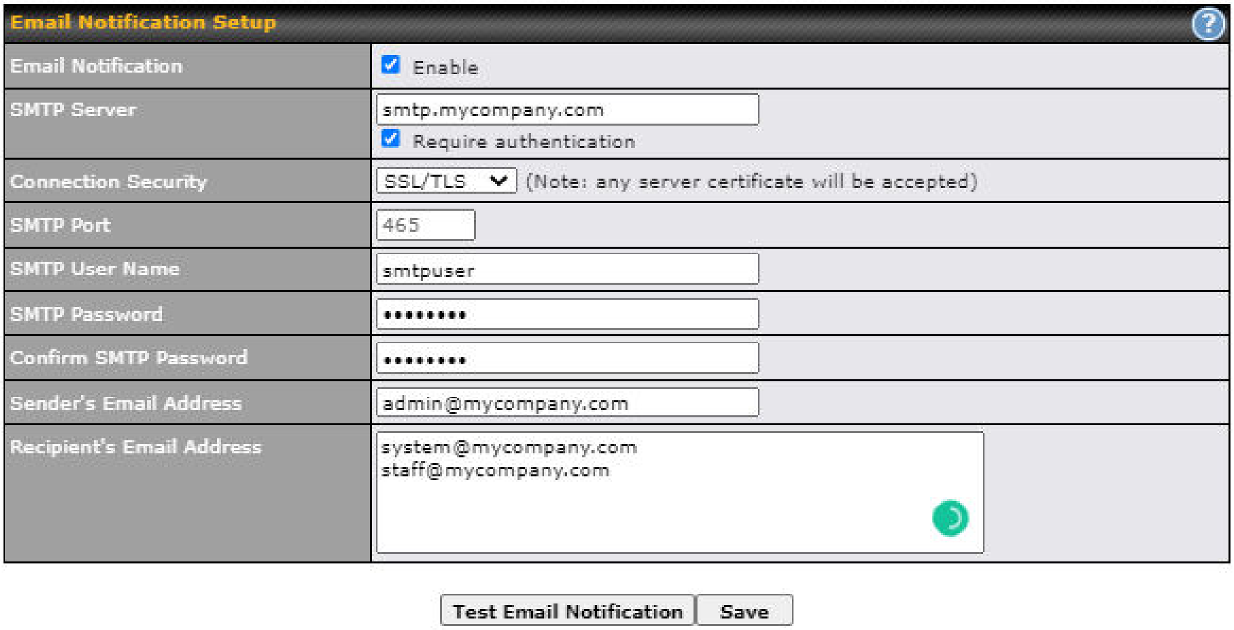
Schedule Map

|  | 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. |

### 12.1.5 Email Notification

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

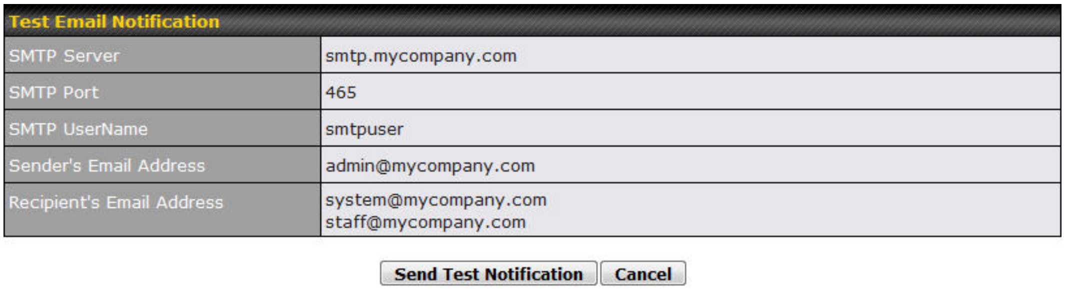


| Email Notification Setup | |
|---|---|
| Email Notification | ☑ Enable |
| SMTP Server | smtp.mycompany.com<br>☑ Require authentication |
| Connection Security | SSL/TLS (Note: any server certificate will be accepted) |
| SMTP Port | 465 |
| SMTP User Name | smtpuser |
| SMTP Password | •••••••• |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

| Email Notification Settings | |
|---|---|
| **Email Notification** | This setting specifies whether or not to enable email notification. If **Enable** is checked, the Peplink Balance 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 Peplink Balance 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:<br>● None<br>● STARTTLS<br>● 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**.<br>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. |

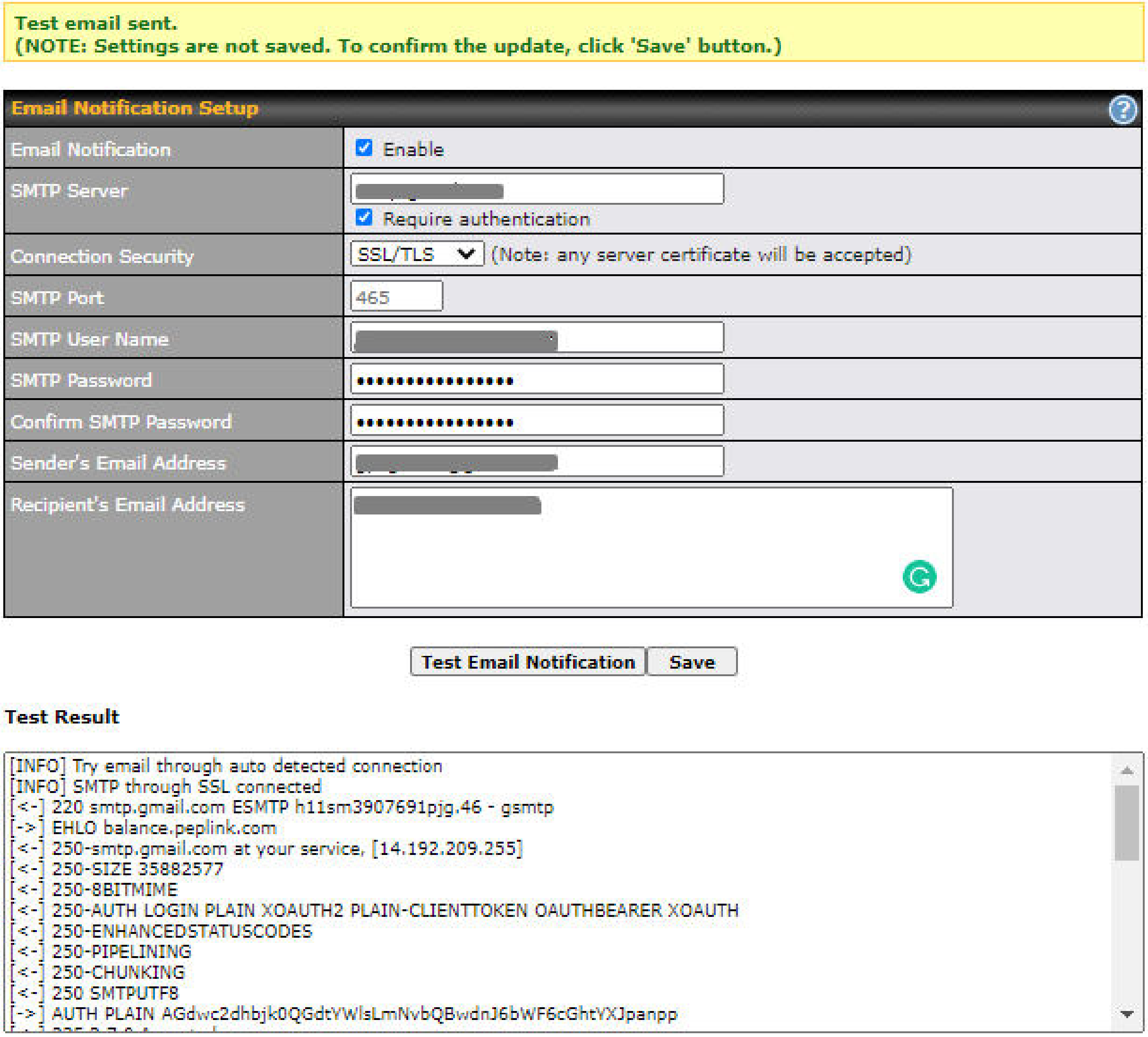
| | |
|---|---|
| **Confirm SMTP Password** | This field allows you to verify and confirm the new administrator password. |
| **Sender's Email Address** | This setting specifies the email address which the Peplink Balance will use to send its reports. |
| **Recipient's Email Address** | This setting specifies the email address(es) to which the Peplink Balance will send email notifications. For multiple recipients, separate each email 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<br>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.)**

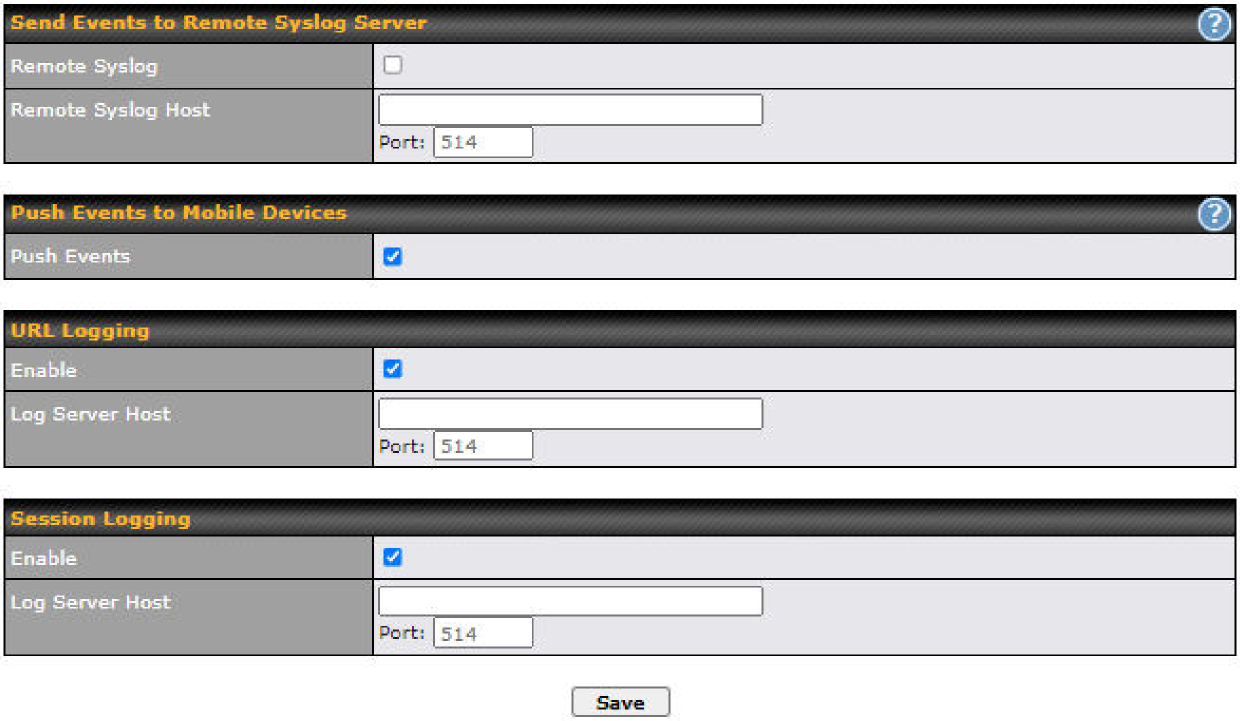
| Email Notification Setup | |
|---|---|
| Email Notification | ☑ Enable |
| SMTP Server | [redacted]<br>☑ Require authentication |
| Connection Security | SSL/TLS (Note: any server certificate will be accepted) |
| SMTP Port | 465 |
| SMTP User Name | [redacted] |
| SMTP Password | ●●●●●●●●●●●●●●●● |
| 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
```

### 12.1.6 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 |

**Push Events to Mobile Devices**

| | |
|---|---|
| Push Events | ☑ |

**URL Logging**

| | |
|---|---|
| Enable | ☑ |
| Log Server Host | Port: 514 |

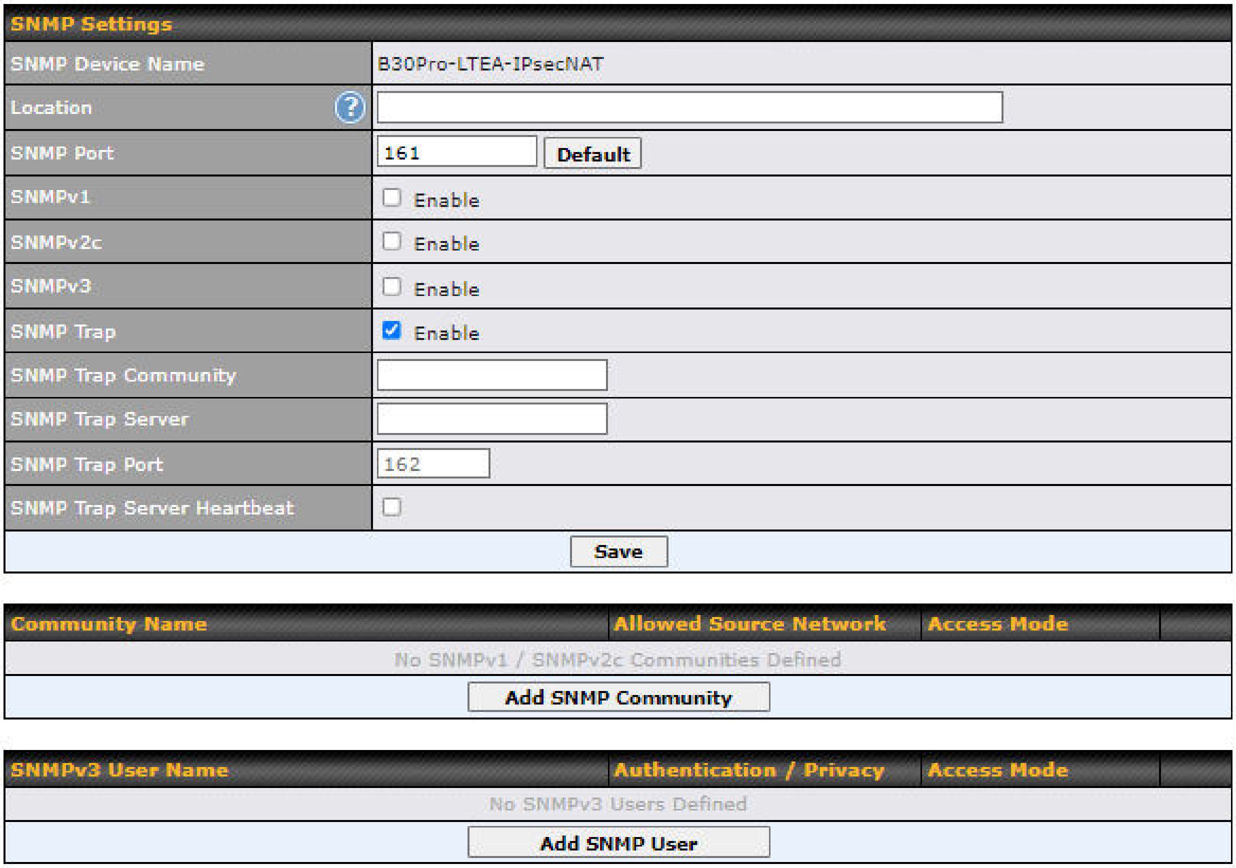
**Session Logging**

| | |
|---|---|
| Enable | ☑ |
| Log Server Host | Port: 514 |

| Remote Syslog 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. |
| **Push Events** | The Peplink Balance 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. |
| | For more information on the Router Utility, go to: www.peplink.com/products/router-utility |

### 12.1.7 SNMP

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



| SNMP Settings | |
|---|---|
| SNMP Device Name | B30Pro-LTEA-IPsecNAT |
| 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 | □ |

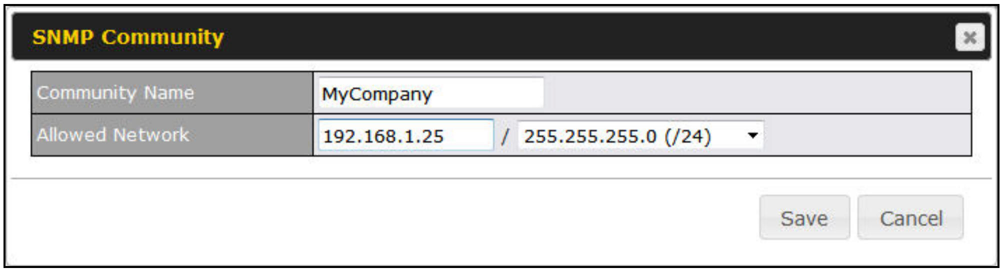
| Community Name | Allowed Source Network | Access Mode |
|---|---|---|
| No SNMPv1 / SNMPv2c Communities Defined | | |

| SNMPv3 User Name | Authentication / Privacy | Access Mode |
|---|---|---|
| No SNMPv3 Users Defined | | |

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

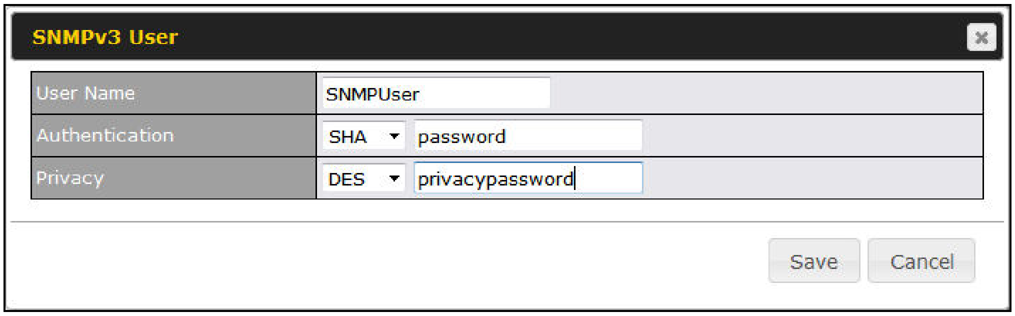
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:


SNMP Community

| | |
|---|---|
| Community Name | MyCompany |
| 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 |

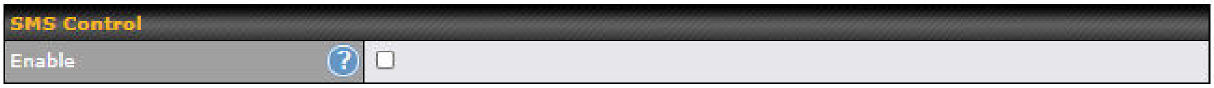
| SNMPv3 User Settings | |
|---|---|
| **User Name** | This setting specifies a user name to be used in SNMPv3. |
| **Authentication Protocol** | This setting specifies via a drop-down menu one of the following valid authentication protocols:<br>● NONE<br>● MD5<br>● SHA<br>When MD5 or SHA is selected,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

### 12.1.8 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**.

Note: Supported Models

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



**SMS Control**

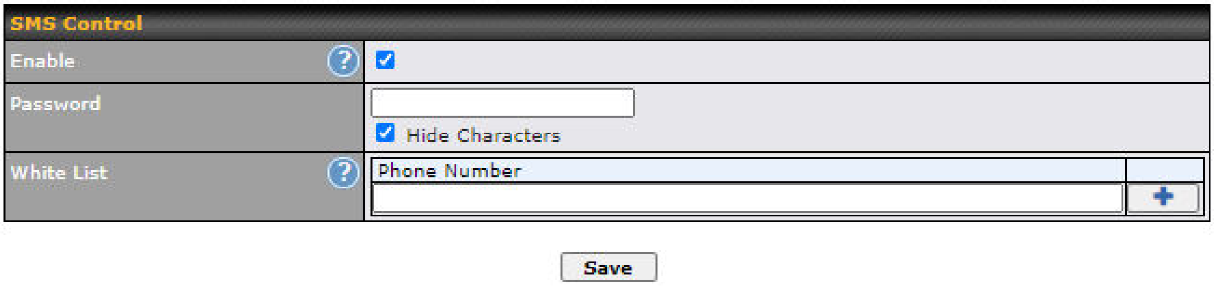
| | |
|---|---|
| Enable ? | □ |

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 an active data connection.

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

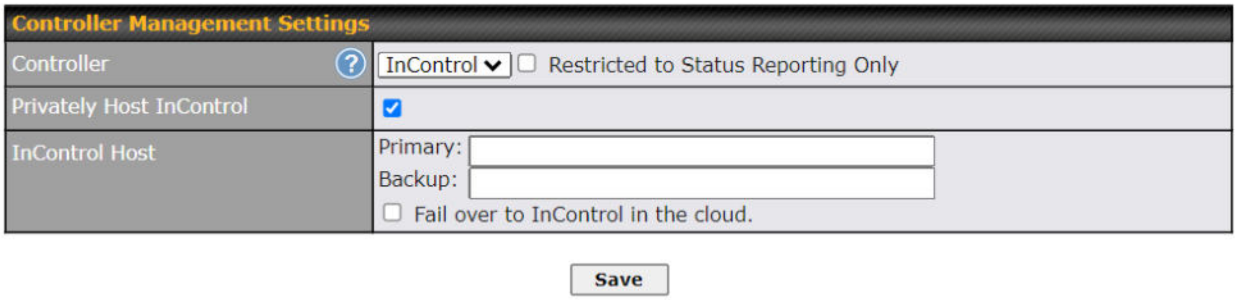


**SMS Control**

| | |
|---|---|
| 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. |

## 12.1.9 InControl



Controller Management Settings

| | |
|---|---|
| Controller | InControl □ Restricted to Status Reporting Only |
| Privately Host InControl | ☑ |
| InControl Host | Primary:<br>Backup:<br>□ 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 checkbox 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.

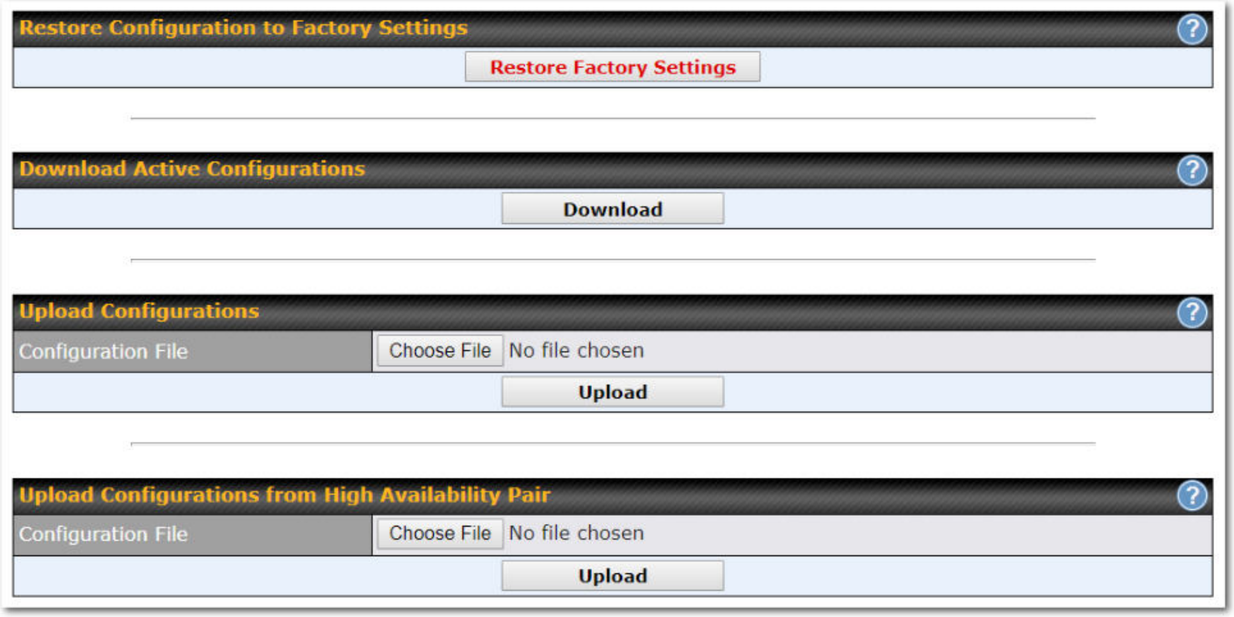
When the box **Restricted to Status Reporting Only** is ticked, the router will only report its status, but can't be managed or configured by InControl.

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.

### 12.1.10 Configuration

Backing up Peplink Balance settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Peplink Balance settings is found at **System>Configuration**.



**Restore Configuration to Factory Settings**

**Download Active Configurations**

**Upload Configurations**

| | |
|---|---|
| Configuration File | Choose File No file chosen |

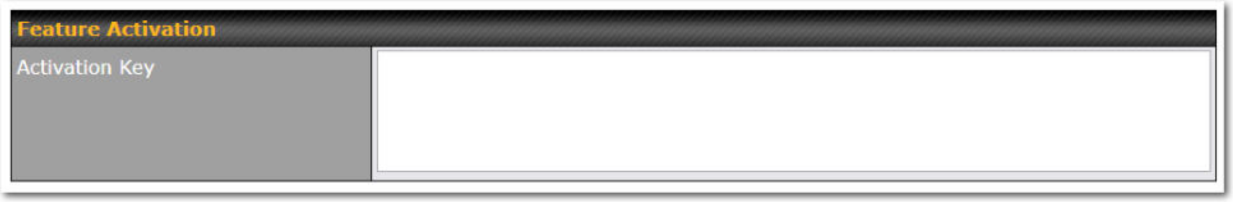
**Upload Configurations from High Availability Pair**

| | |
|---|---|
| Configuration File | Choose File No file chosen |

| Configuration | |
|---|---|
| **Restore Configuration to Factory Settings** | 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 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, the Balance unit 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 Peplink Balance unit so that it is different from the HA counterpart. |

### 12.1.11 Feature Add-ons

Some balance models 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**.



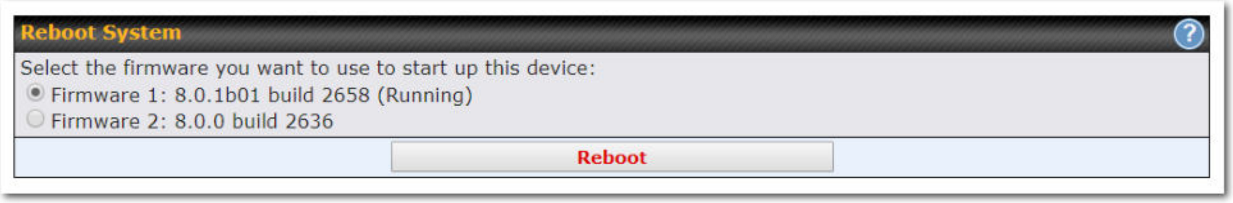
Feature Activation

Activation Key

### 12.1.12 Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Peplink Balance Series can be equipped with two copies of firmware, and 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:

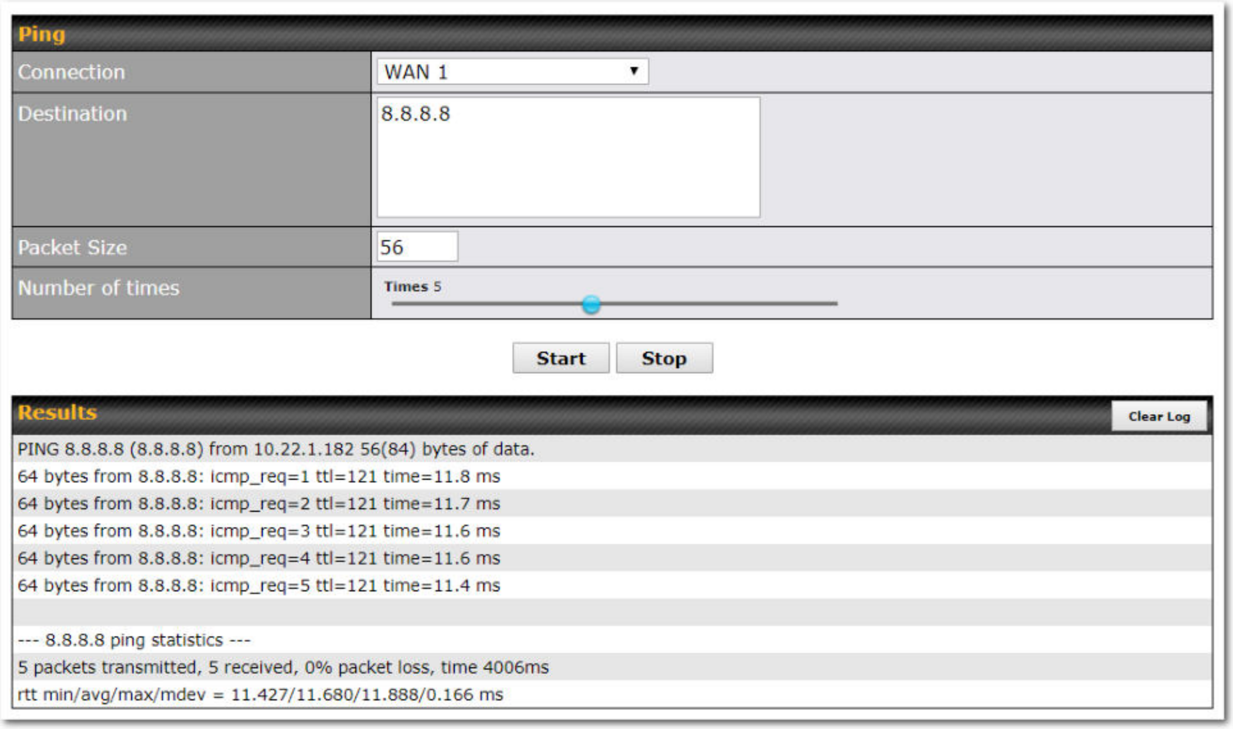
● Firmware 1: 8.0.1b01 build 2658 (Running)

○ Firmware 2: 8.0.0 build 2636

## 12.2 Tools

### 12.2.1 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:



| | |
|---|---|
| Connection | WAN 1 |
| Destination | 8.8.8.8 |
| Packet Size | 56 |
| Number of times | Times 5 |

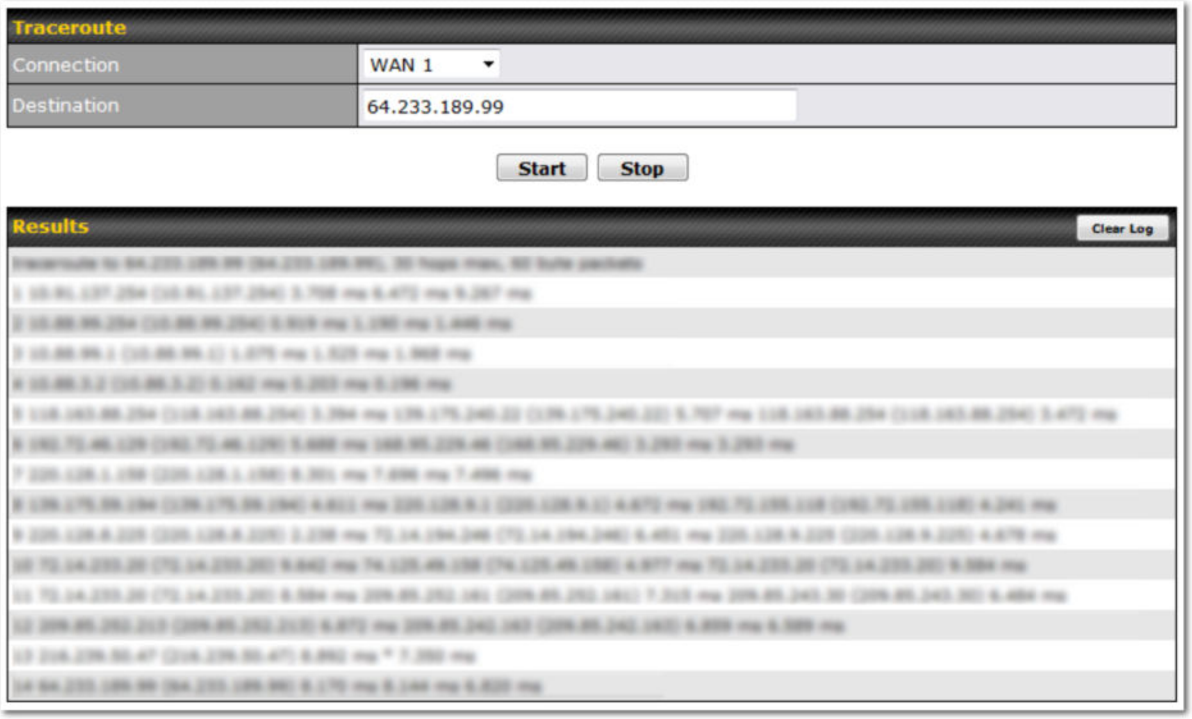
```
PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=121 time=11.8 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=121 time=11.7 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=121 time=11.4 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 11.427/11.680/11.888/0.166 ms
```

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

### 12.2.2 Traceroute

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 |

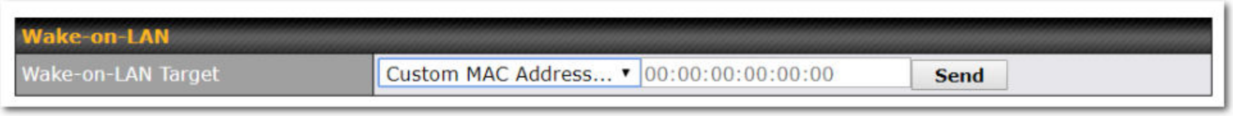
[illegible]

**Tip**

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

### 12.2.3 Wake-on-LAN

Peplink 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**

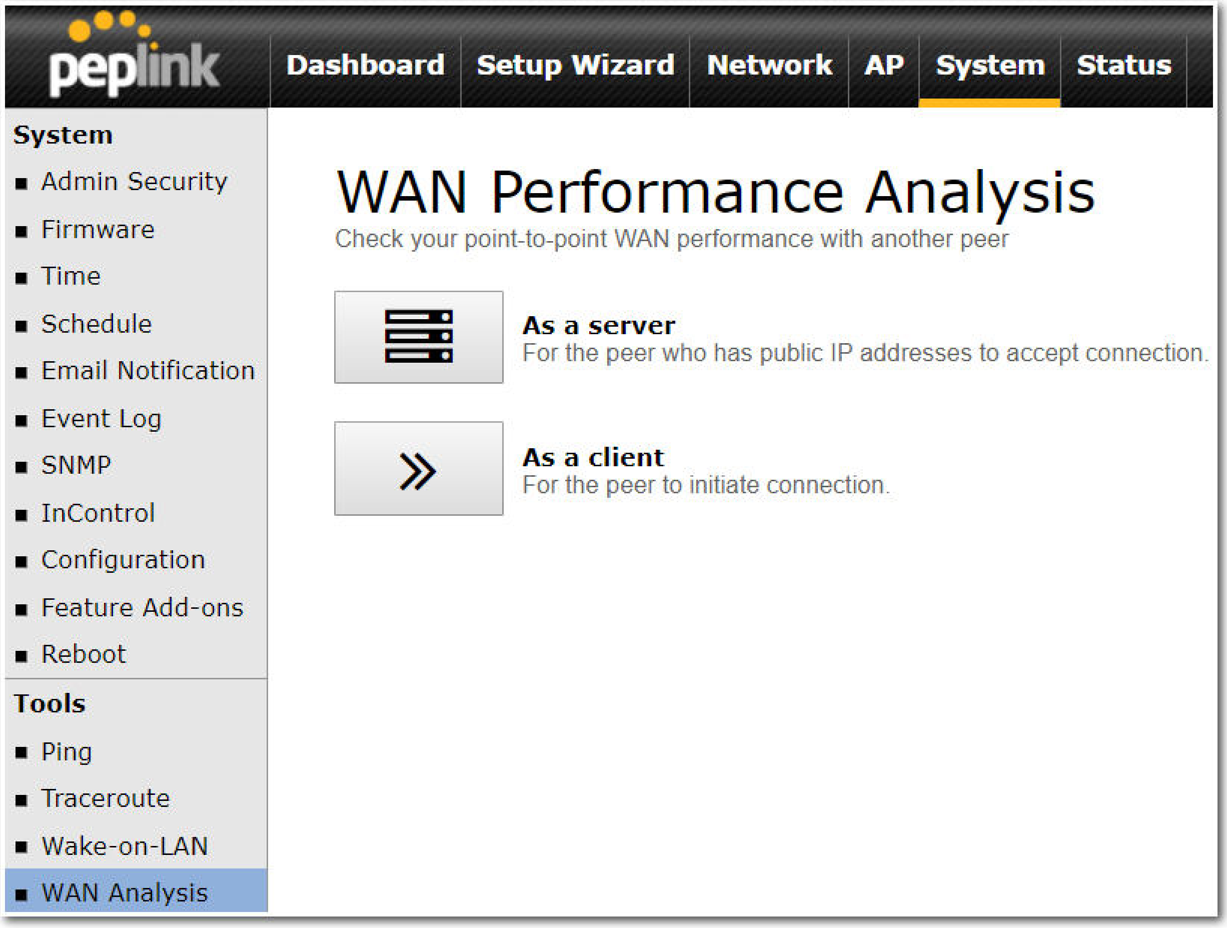
| | |
|---|---|
| Wake-on-LAN Target | Custom MAC Address... 00:00:00:00:00:00 |

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

### 12.2.4 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.



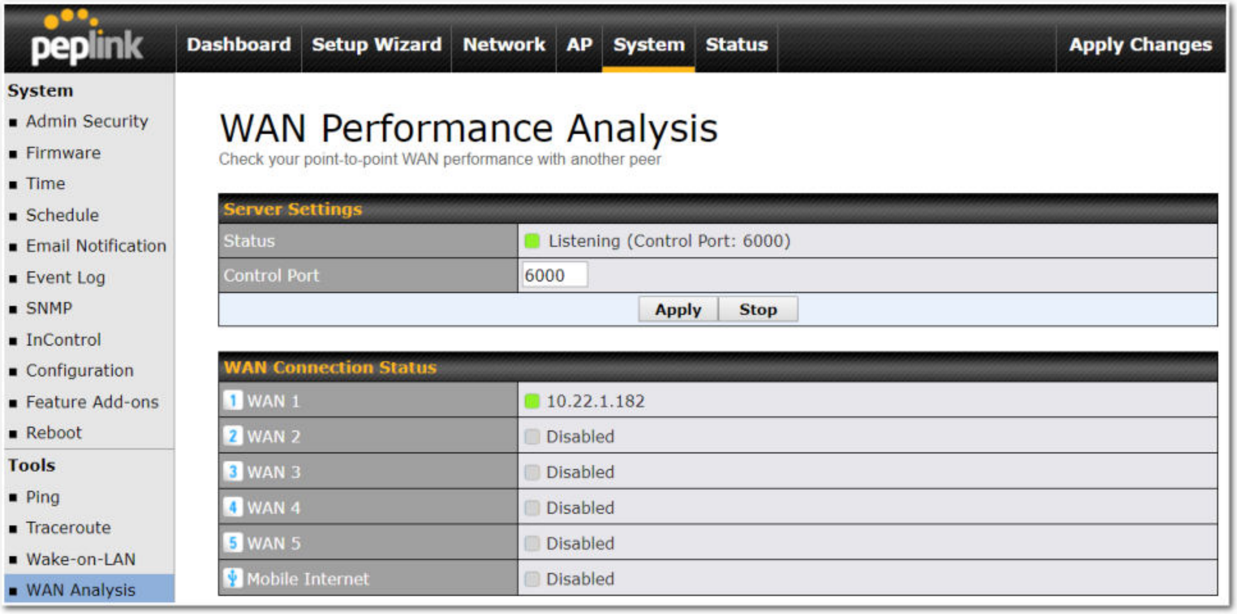
WAN Performance Analysis

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.



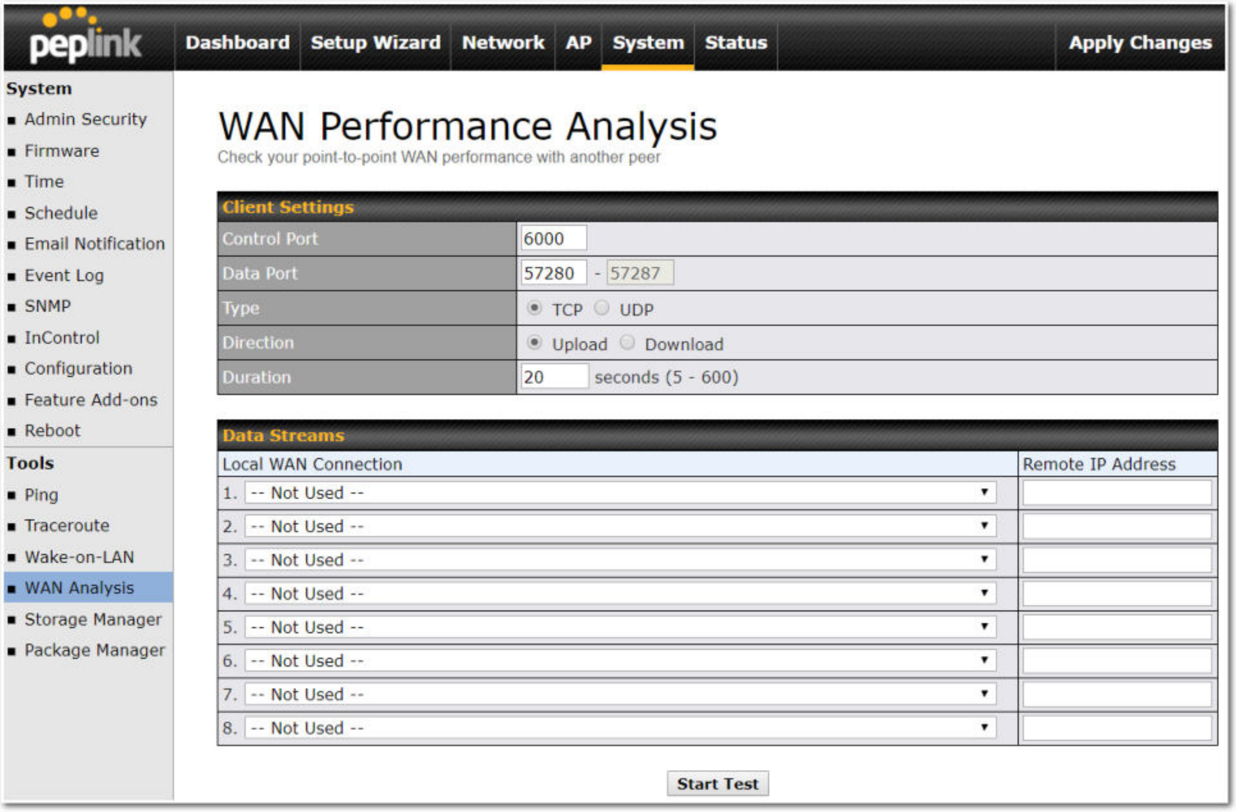
WAN Performance Analysis

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.



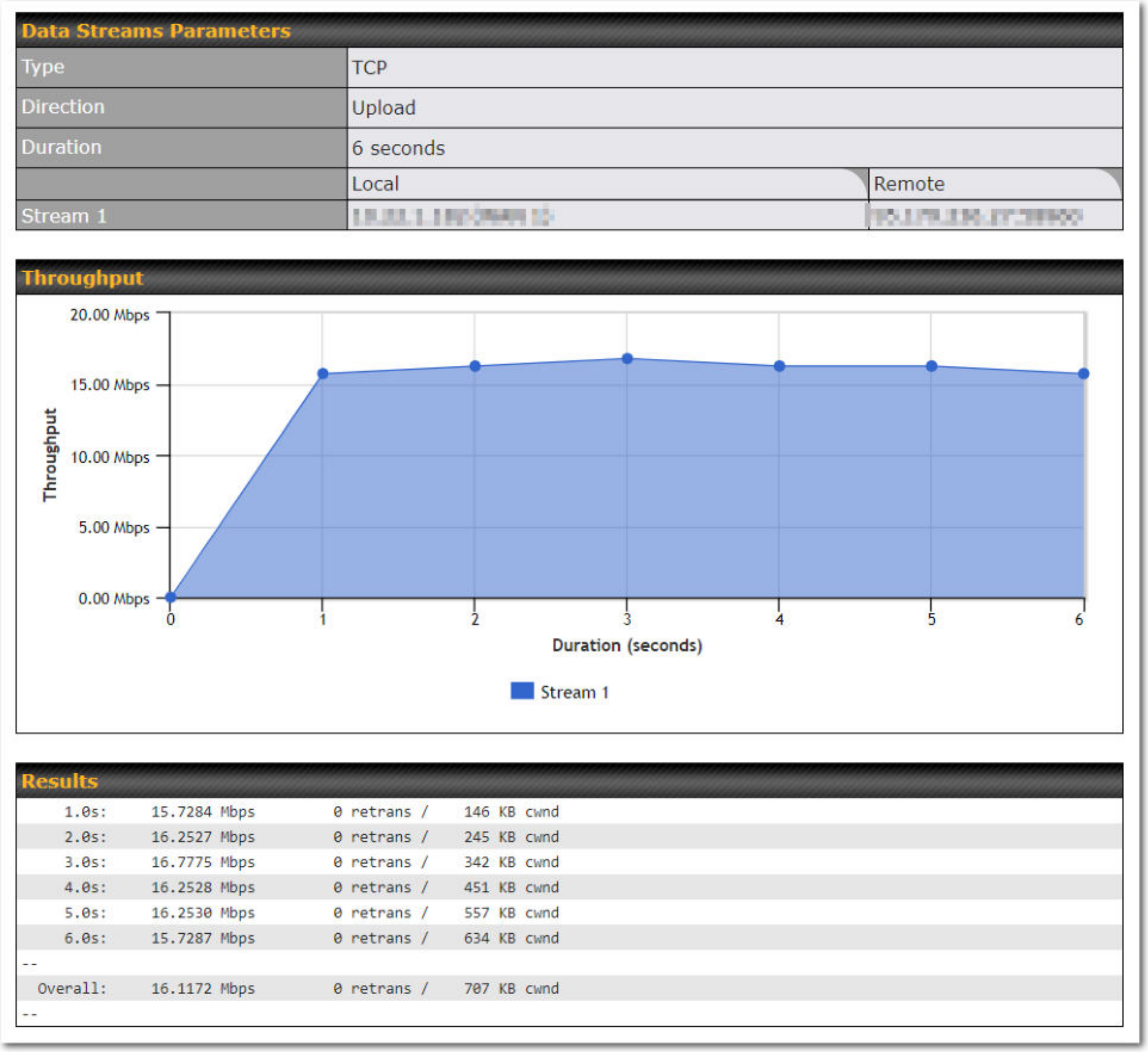
WAN Performance Analysis

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**

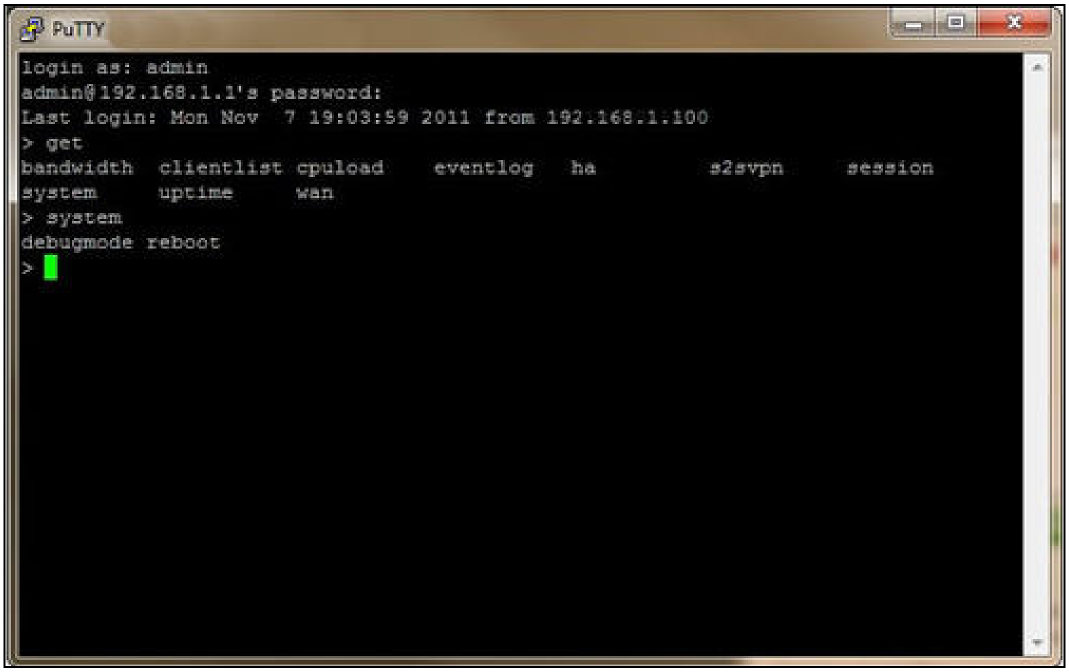
```
     1.0s:     15.7284 Mbps        0 retrans /    146 KB cwnd
     2.0s:     16.2527 Mbps        0 retrans /    245 KB cwnd
     3.0s:     16.7775 Mbps        0 retrans /    342 KB cwnd
     4.0s:     16.2528 Mbps        0 retrans /    451 KB cwnd
     5.0s:     16.2530 Mbps        0 retrans /    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.

## 12.3 CLI (Command Line) Support

The serial console connector on some Peplink Balance units is RJ-45. To access the serial console port, prepare a RJ-45 to DB-9 console cable. Connect the RJ-45 end to the unit's console port and the DB-9 end to a terminal's serial port. The port setting will be *115200,8N1*.

The serial console connector on other Peplink Balance units is a DB-9 male connector. To access the serial console port, connect a null modem cable with a DB-9 connector on both ends to a terminal with the port setting of *115200,8N1*.



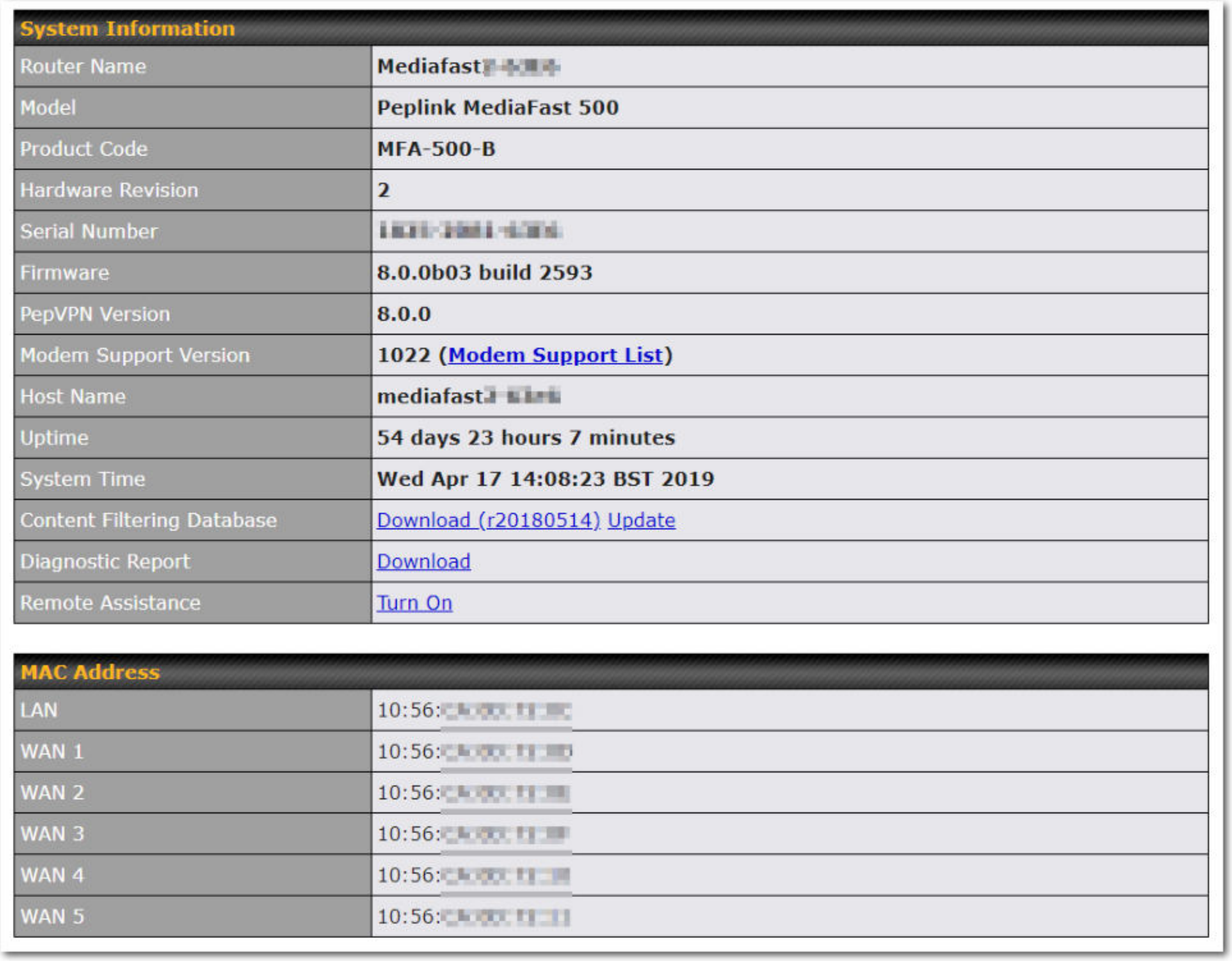
```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist cpuload    eventlog   ha         s2svpn     session
system     uptime     wan
> system
debugmode reboot
>
```

# 13 Status Tab

## 13.1 Status

### 13.1.1 Device

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



| System Information | |
|---|---|
| Router Name | Mediafast[redacted] |
| Model | Peplink MediaFast 500 |
| Product Code | MFA-500-B |
| Hardware Revision | 2 |
| Serial Number | [redacted] |
| Firmware | 8.0.0b03 build 2593 |
| PepVPN Version | 8.0.0 |
| Modem Support Version | 1022 (Modem Support List) |
| Host Name | mediafast[redacted] |
| Uptime | 54 days 23 hours 7 minutes |
| System Time | Wed Apr 17 14:08:23 BST 2019 |
| Content Filtering Database | Download (r20180514) Update |
| Diagnostic Report | Download |
| Remote Assistance | Turn On |

| MAC Address | |
|---|---|
| LAN | 10:56:[redacted] |
| WAN 1 | 10:56:[redacted] |
| WAN 2 | 10:56:[redacted] |
| WAN 3 | 10:56:[redacted] |
| WAN 4 | 10:56:[redacted] |
| WAN 5 | 10:56:[redacted] |

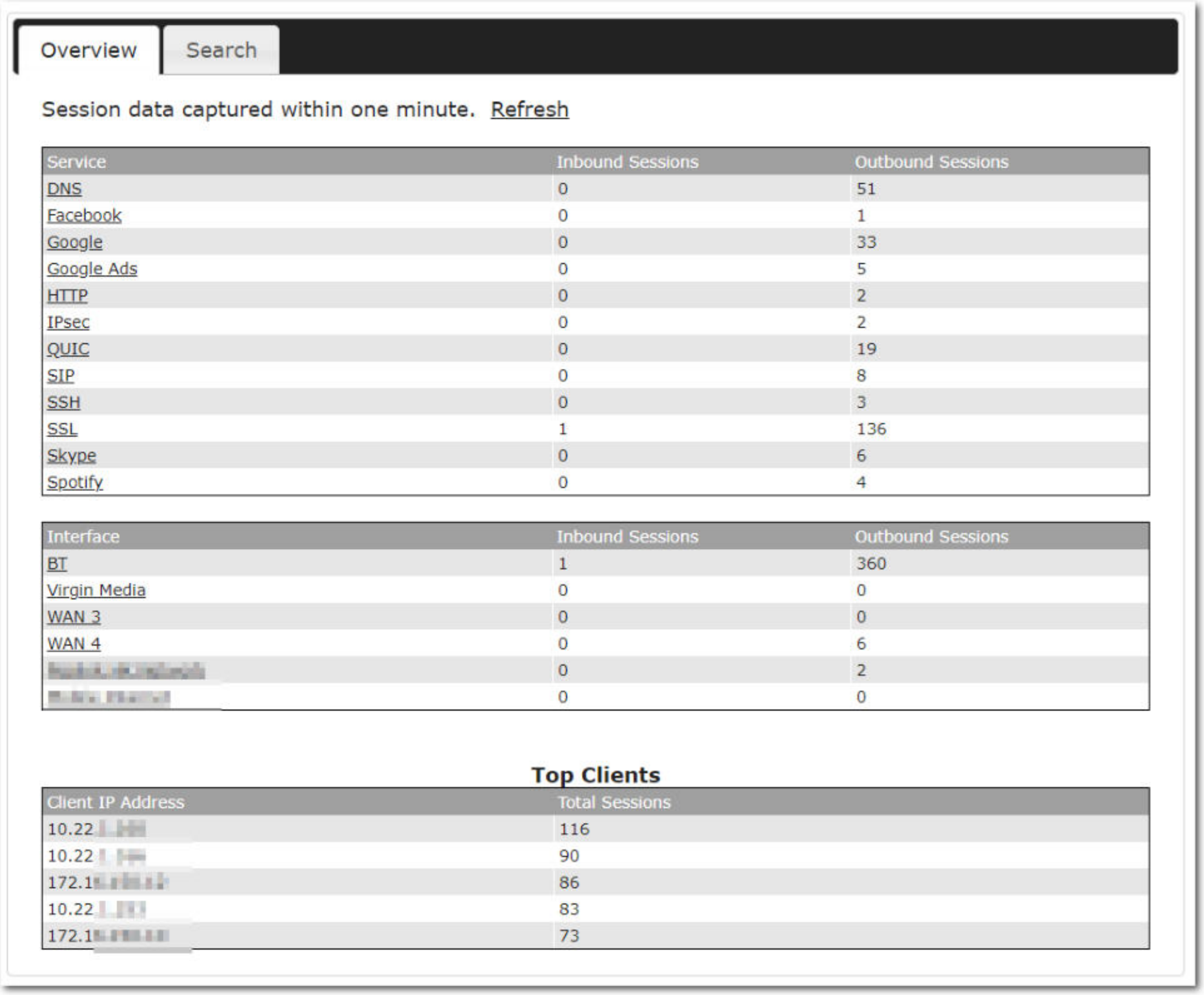
| System Information | |
|---|---|
| **Router Name** | This is the name specified in the **Router Name** field located at **System>Admin Security**. |
| **Model** | This shows the model name and number of this device. |
| **Hardware Revision** | This shows the hardware version of this device. |
| **Serial Number** | This shows the serial number of this device. |
| **Firmware** | This shows the firmware version this device is currently running. |
| **Uptime** | This shows the length of time since the device has been rebooted. |
| **System Time** | This shows the current system time. |
| **Diagnostic Report** | The **Download** link is for exporting a diagnostic report file required for system investigation. |
| **Remote Assistance** | Click **Turn on** to enable remote assistance. |

The second table shows the MAC address of each LAN/WAN interface connected.

| Important Note |
|---|
| If you encounter issues and would like to contact the Peplink Support Team (http://www.peplink.com/contact/), please download the diagnostic report file and attach it along with a description of your issue. |

### 13.1.2 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 |
|---|---|---|
| DNS | 0 | 51 |
| Facebook | 0 | 1 |
| Google | 0 | 33 |
| Google Ads | 0 | 5 |
| HTTP | 0 | 2 |
| IPsec | 0 | 2 |
| QUIC | 0 | 19 |
| SIP | 0 | 8 |
| SSH | 0 | 3 |
| SSL | 1 | 136 |
| Skype | 0 | 6 |
| Spotify | 0 | 4 |

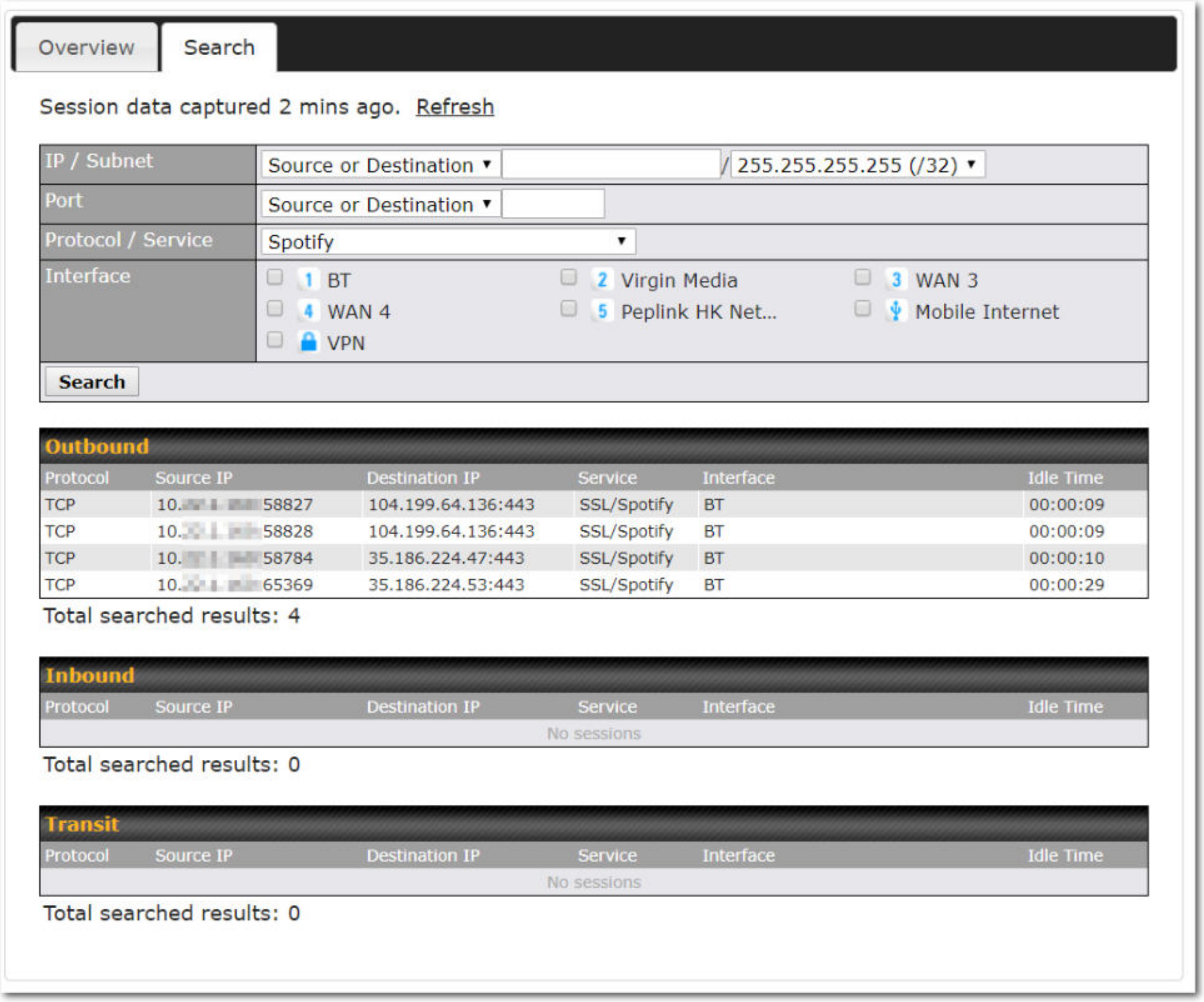
| Interface | Inbound Sessions | Outbound Sessions |
|---|---|---|
| BT | 1 | 360 |
| Virgin Media | 0 | 0 |
| WAN 3 | 0 | 0 |
| WAN 4 | 0 | 6 |
| [redacted] | 0 | 2 |
| [redacted] | 0 | 0 |

**Top Clients**

| Client IP Address | Total Sessions |
|---|---|
| 10.22[redacted] | 116 |
| 10.22[redacted] | 90 |
| 172.1[redacted] | 86 |
| 10.22[redacted] | 83 |
| 172.1[redacted] | 73 |

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. Finally, you can see which clients are initiating the most sessions.

In addition, 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**.



Session data captured 2 mins ago. Refresh

| | |
|---|---|
| IP / Subnet | Source or Destination ▾ / 255.255.255.255 (/32) ▾ |
| Port | Source or Destination ▾ |
| Protocol / Service | Spotify ▾ |
| Interface | □ 1 BT □ 2 Virgin Media □ 3 WAN 3<br>□ 4 WAN 4 □ 5 Peplink HK Net... □ Mobile Internet<br>□ VPN |
| Search | |

**Outbound**

| Protocol | Source IP | Destination IP | Service | Interface | Idle Time |
|---|---|---|---|---|---|
| TCP | 10.[redacted]58827 | 104.199.64.136:443 | SSL/Spotify | BT | 00:00:09 |
| TCP | 10.[redacted]58828 | 104.199.64.136:443 | SSL/Spotify | BT | 00:00:09 |
| TCP | 10.[redacted]58784 | 35.186.224.47:443 | SSL/Spotify | BT | 00:00:10 |
| TCP | 10.[redacted]65369 | 35.186.224.53:443 | SSL/Spotify | BT | 00:00:29 |

Total searched results: 4

**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 | | | |

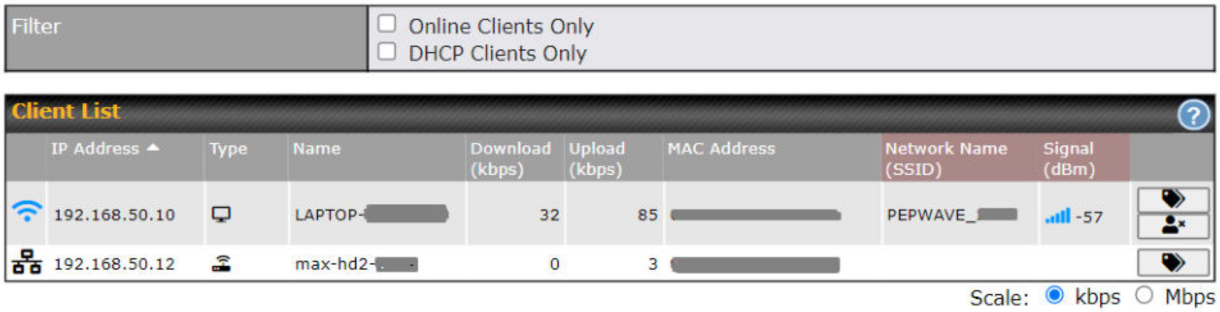
Total searched results: 0

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

### 13.1.3 Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, type, 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. Further update the record after the import by going to **Network>LAN**.



| | |
|---|---|
| Filter | □ Online Clients Only<br>□ DHCP Clients Only |

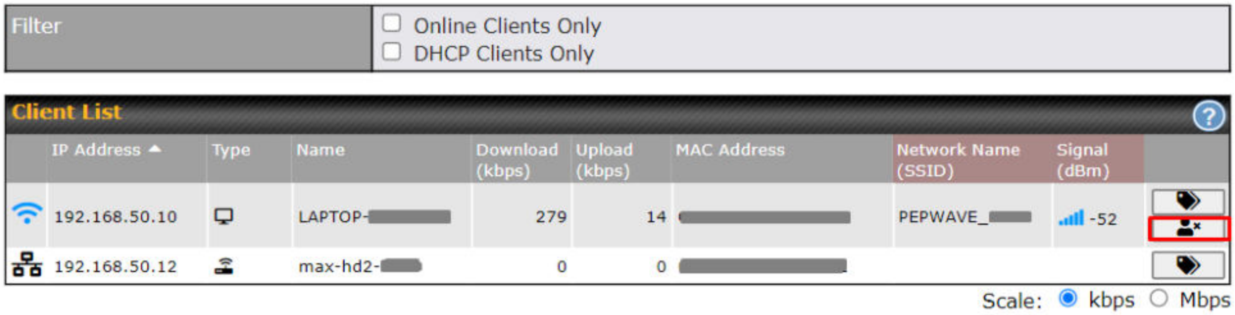
Client List

| | 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 | 🏷<br>👤× |
| 🖧 | 192.168.50.12 | | max-hd2-[redacted] | 0 | 3 | [redacted] | | | 🏷 |

Scale: ● kbps ○ Mbps

If the PPTP server SpeedFusion$^{TM}$, or AP controller 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.



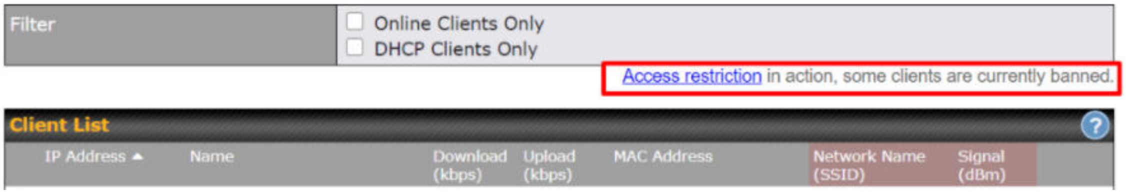
| | |
|---|---|
| Filter | □ Online Clients Only<br>□ DHCP Clients Only |

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 | 🏷<br>👤× |
| 🖧 | 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.



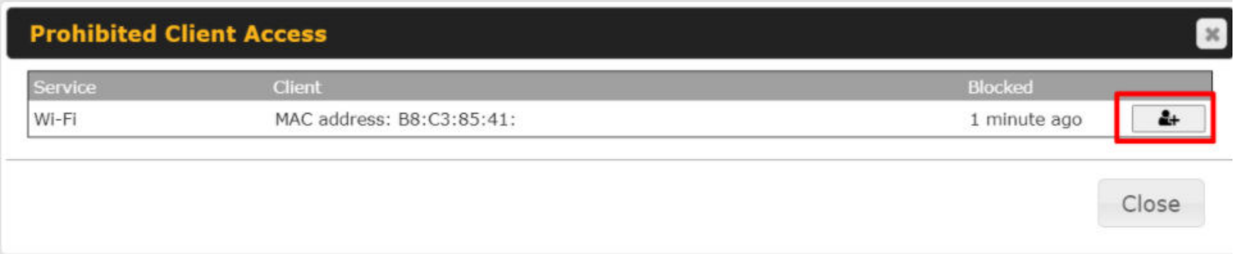
| | |
|---|---|
| Filter | □ Online Clients Only<br>□ DHCP Clients Only |

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) |
|---|---|---|---|---|---|---|

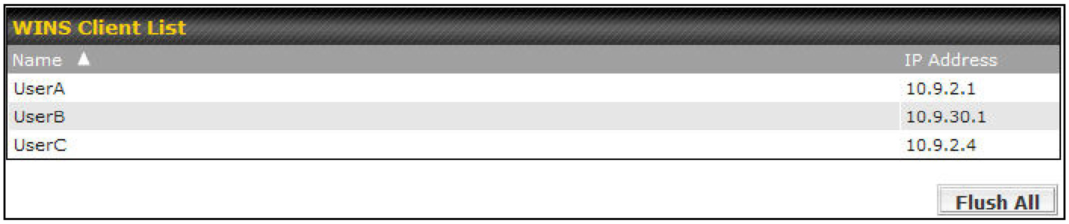
You may also unblock the Wi-Fi or Remote User Access clients when the client devices need to reconnect the network by clicking the button on the right.



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

### 13.1.4 WINS Clients

The WINS client list table is located at **Status>WINS Client**.

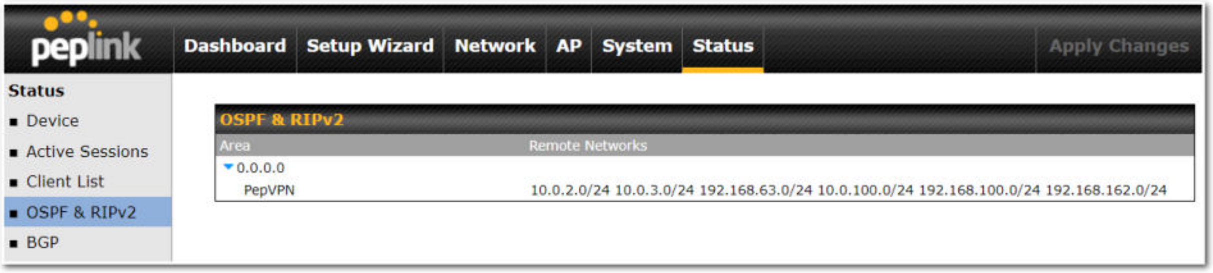


| Name ▲ | IP Address |
|---|---|
| UserA | 10.9.2.1 |
| UserB | 10.9.30.1 |
| UserC | 10.9.2.4 |

The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

### 13.1.5 OSPF & RIPv2

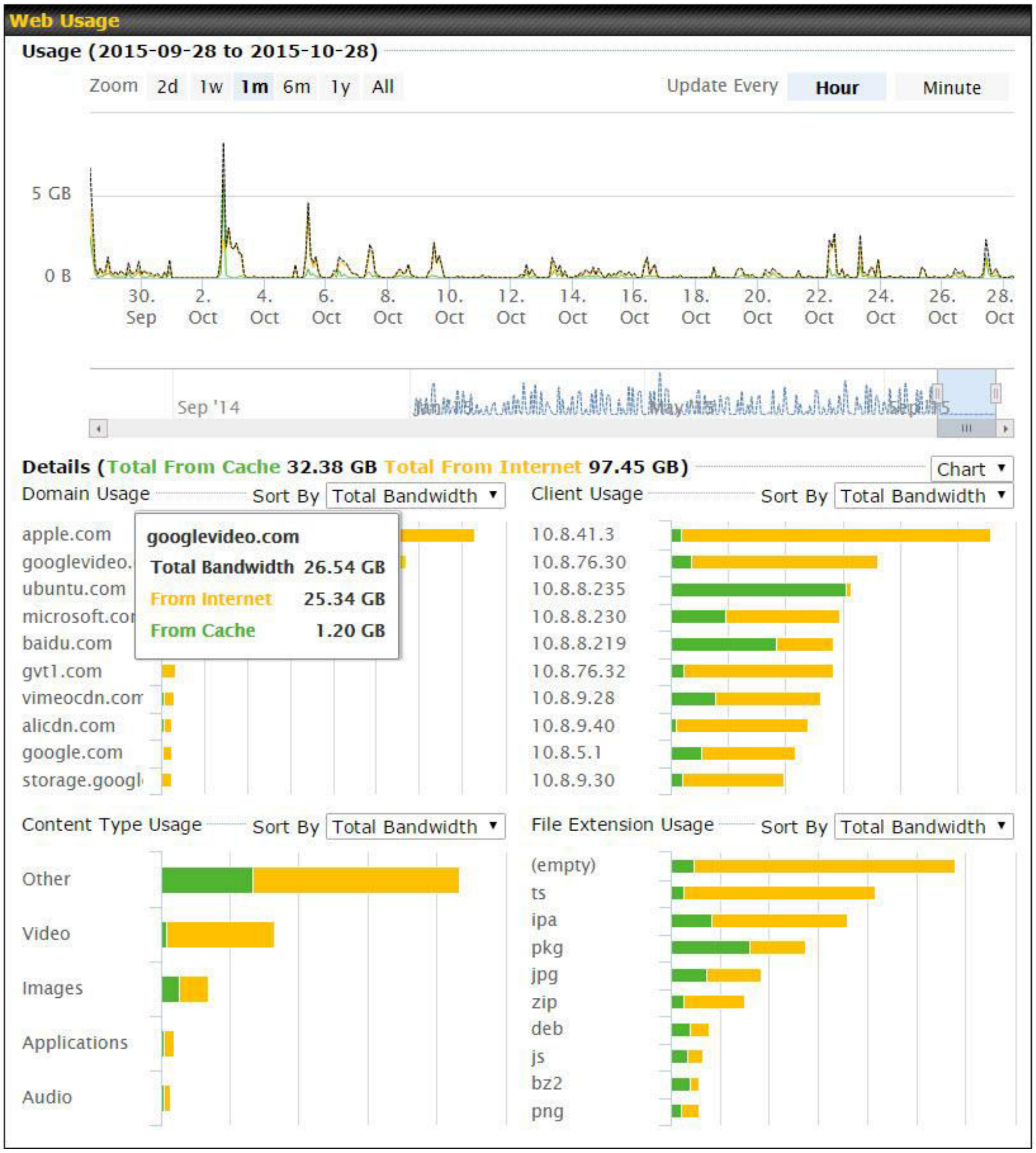
Information on OSPF and RIPv2 routing setup can be found at **Status>OSPF & RIPv2**.



| 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 |

### 13.1.6 MediaFast

To get details on storage and bandwidth usage, select **Status>MediaFast**.



Web Usage

Usage (2015-09-28 to 2015-10-28)

Zoom 2d 1w **1m** 6m 1y All

Update Every **Hour** Minute

Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)

Chart

Domain Usage Sort By Total Bandwidth

Client Usage Sort By Total Bandwidth

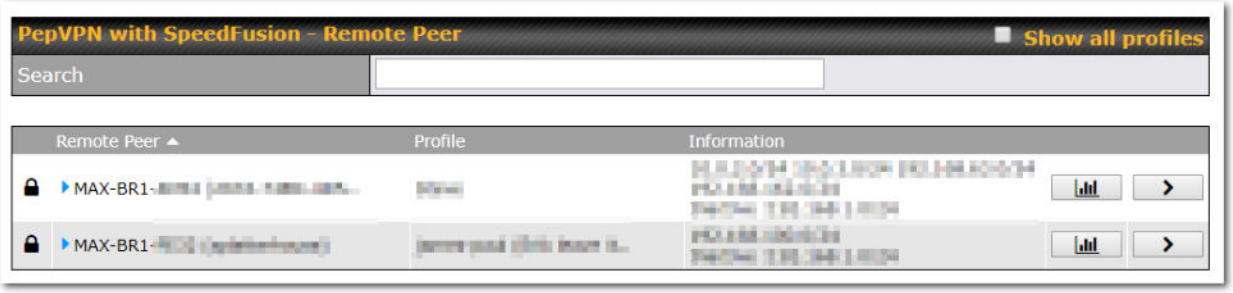
googlevideo.com
Total Bandwidth 26.54 GB
From Internet 25.34 GB
From Cache 1.20 GB

Content Type Usage Sort By Total Bandwidth

File Extension Usage Sort By Total Bandwidth

### 13.1.7 PepVPN / SpeedFusion Status

**PepVPN/SpeedFusion Status** shows the current connection status of each connection profile and is displayed at **Status> PepVPN/SpeedFusion.**

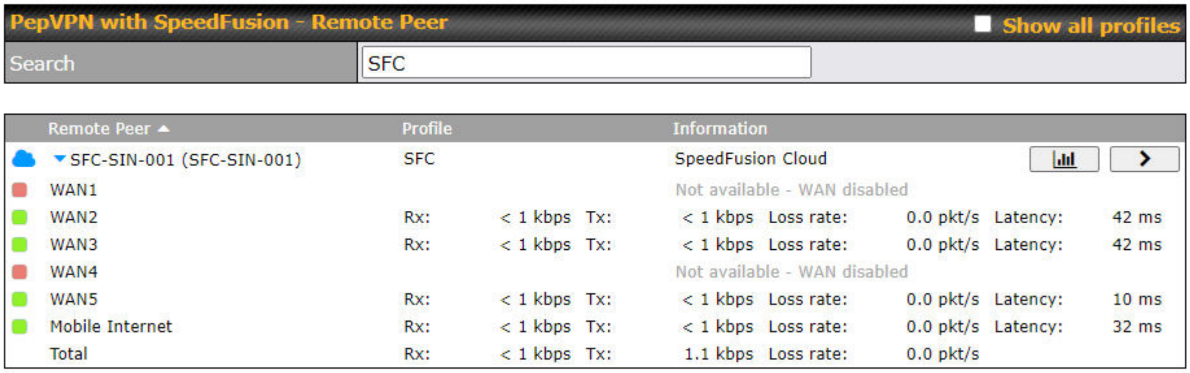


PepVPN with SpeedFusion - Remote Peer ☐ Show all profiles

Search

| | Remote Peer ▲ | Profile | Information | | |
|---|---|---|---|---|---|
| 🔒 | ▸ MAX-BR1-[redacted] | [redacted] | [redacted] | 📊 | > |
| 🔒 | ▸ MAX-BR1-[redacted] | [redacted] | [redacted] | 📊 | > |

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

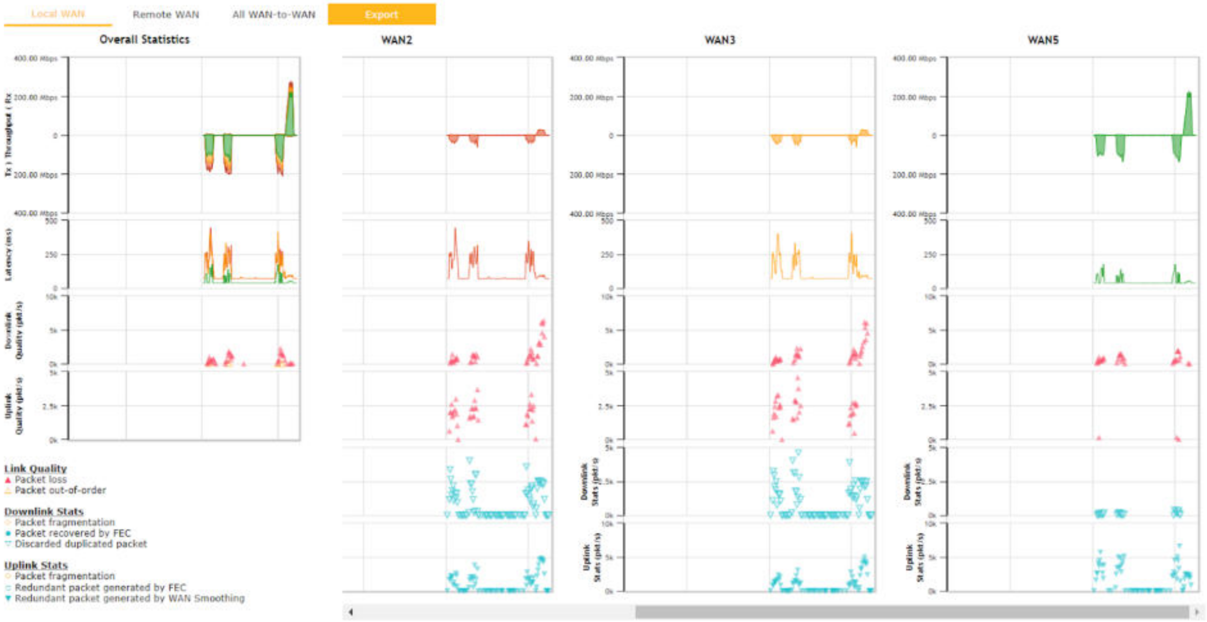


PepVPN with SpeedFusion - Remote Peer ☐ Show all profiles

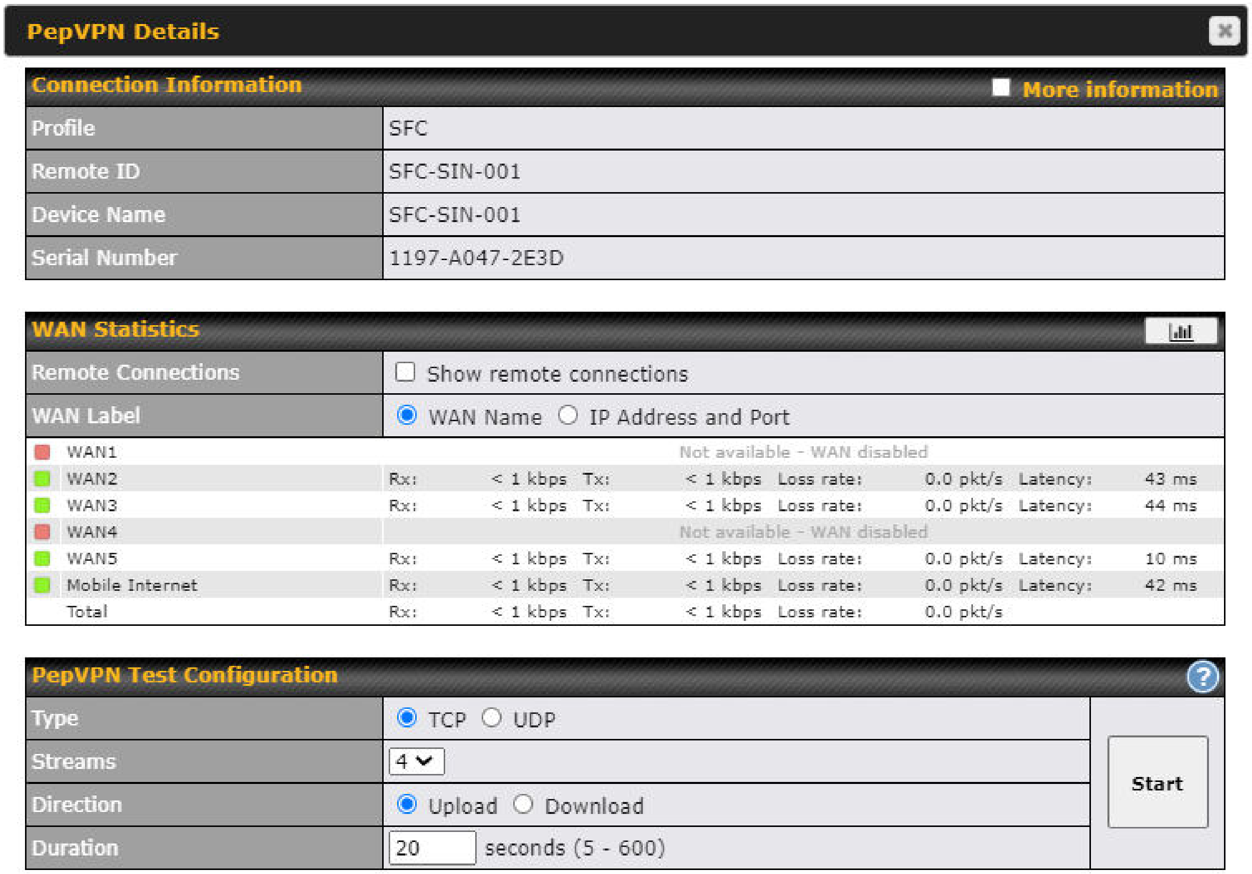
Search SFC

| | Remote Peer ▲ | Profile | | | Information | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ☁ | ▾ SFC-SIN-001 (SFC-SIN-001) | SFC | | | SpeedFusion Cloud | | | | 📊 | > |
| 🟥 | WAN1 | | | | Not available - WAN disabled | | | | | |
| 🟩 | WAN2 | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 42 ms | |
| 🟩 | WAN3 | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 42 ms | |
| 🟥 | WAN4 | | | | Not available - WAN disabled | | | | | |
| 🟩 | WAN5 | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 10 ms | |
| 🟩 | Mobile Internet | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 32 ms | |
| | Total | Rx: | < 1 kbps | Tx: | 1.1 kbps | Loss rate: | 0.0 pkt/s | | | |

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



When pressing the > button for a PepVPN/SpeedFusion Tunnel Bandwidth Test Tool, the following menu will appear:



**PepVPN Details**

**Connection Information** ☐ More information

| | |
|---|---|
| Profile | SFC |
| Remote ID | SFC-SIN-001 |
| Device Name | SFC-SIN-001 |
| Serial Number | 1197-A047-2E3D |

**WAN Statistics**

| | |
|---|---|
| Remote Connections | ☐ Show remote connections |
| WAN Label | ● WAN Name ○ IP Address and Port |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 🟥 | WAN1 | Not available - WAN disabled | | | | | | | |
| 🟩 | WAN2 | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 43 ms |
| 🟩 | WAN3 | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 44 ms |
| 🟥 | WAN4 | Not available - WAN disabled | | | | | | | |
| 🟩 | WAN5 | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 10 ms |
| 🟩 | Mobile Internet | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | Latency: | 42 ms |
| | Total | Rx: | < 1 kbps | Tx: | < 1 kbps | Loss rate: | 0.0 pkt/s | | |

**PepVPN Test Configuration**

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

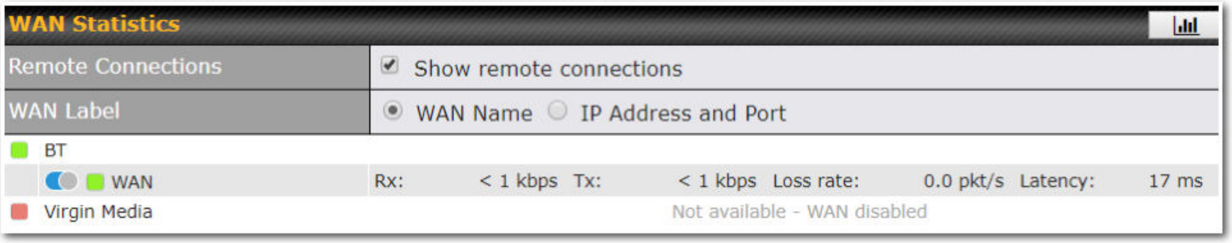
Start

The **connection information** shows the details of the selected PepVPN profile, consisting of the Profile name, **Router ID**, **Router Nam**e and **Serial Number** of the remote router
Advanced features for the PepVPN 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 PepVPN speed between two locations to see if there is interference or network congestion between certain WAN connections.



**WAN Statistics**

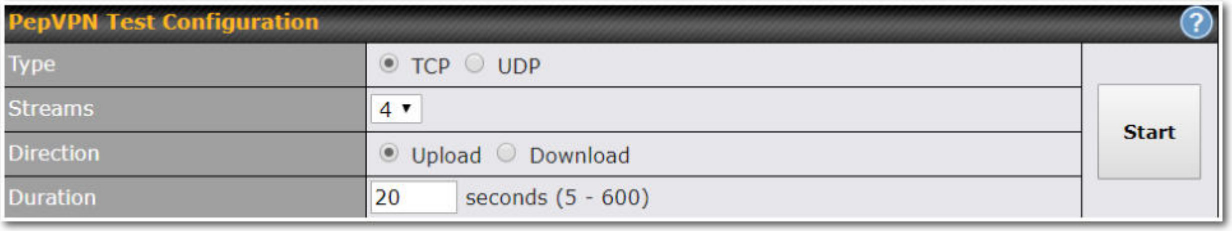
| | |
|---|---|
| Remote Connections | ☑ Show remote connections |
| WAN Label | ● WAN Name ○ IP Address and Port |

🟩 BT

🟩 WAN Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 17 ms

🟥 Virgin Media Not available - WAN disabled

The PepVPN/SpeedFusion 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.



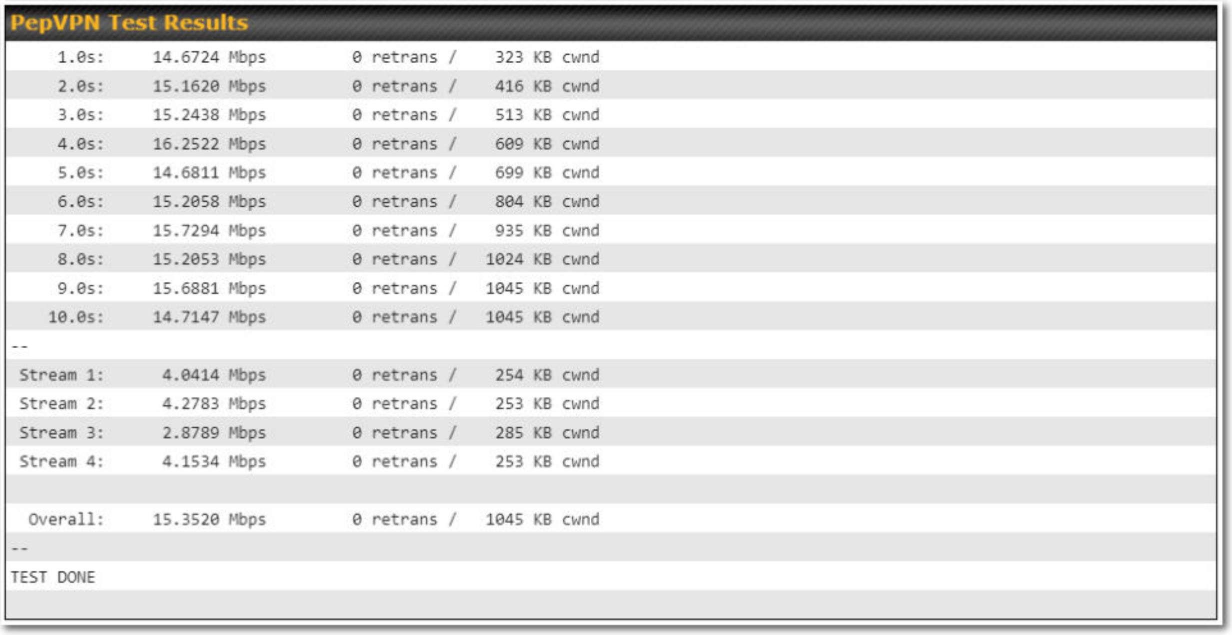
**PepVPN Test Configuration**

| | |
|---|---|
| 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.



**PepVPN Test Results**

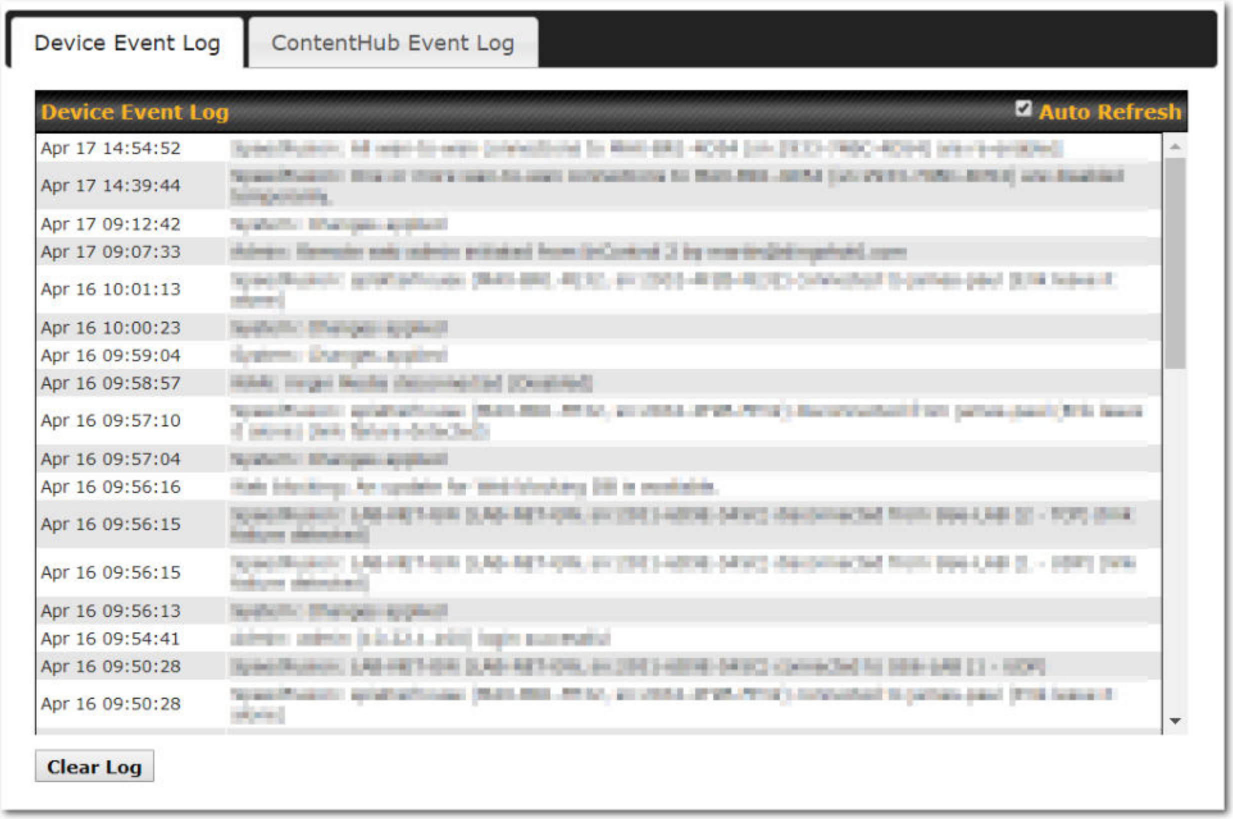
```
     1.0s:     14.6724 Mbps        0 retrans /    323 KB cwnd
     2.0s:     15.1620 Mbps        0 retrans /    416 KB cwnd
     3.0s:     15.2438 Mbps        0 retrans /    513 KB cwnd
     4.0s:     16.2522 Mbps        0 retrans /    609 KB cwnd
     5.0s:     14.6811 Mbps        0 retrans /    699 KB cwnd
     6.0s:     15.2058 Mbps        0 retrans /    804 KB cwnd
     7.0s:     15.7294 Mbps        0 retrans /    935 KB cwnd
     8.0s:     15.2053 Mbps        0 retrans /   1024 KB cwnd
     9.0s:     15.6881 Mbps        0 retrans /   1045 KB cwnd
    10.0s:     14.7147 Mbps        0 retrans /   1045 KB cwnd
--
 Stream 1:      4.0414 Mbps        0 retrans /    254 KB cwnd
 Stream 2:      4.2783 Mbps        0 retrans /    253 KB cwnd
 Stream 3:      2.8789 Mbps        0 retrans /    285 KB cwnd
 Stream 4:      4.1534 Mbps        0 retrans /    253 KB cwnd

  Overall:     15.3520 Mbps        0 retrans /   1045 KB cwnd
--
TEST DONE
```

### 13.1.8 Event Log

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

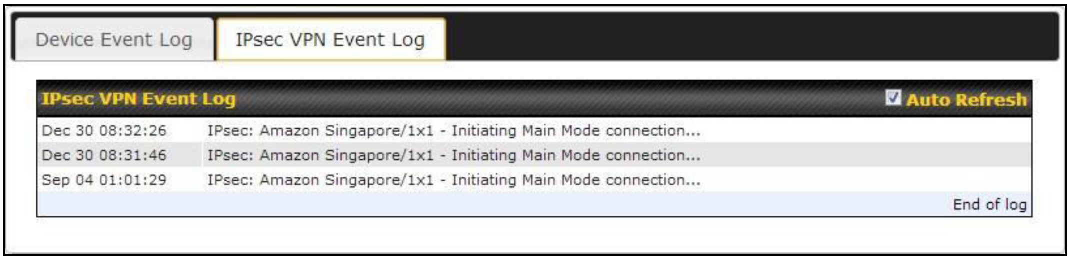
## Device Event Log



```
Apr 17 14:54:52   [illegible]
Apr 17 14:39:44   [illegible]
Apr 17 09:12:42   [illegible]
Apr 17 09:07:33   [illegible]
Apr 16 10:01:13   [illegible]
Apr 16 10:00:23   [illegible]
Apr 16 09:59:04   [illegible]
Apr 16 09:58:57   [illegible]
Apr 16 09:57:10   [illegible]
Apr 16 09:57:04   [illegible]
Apr 16 09:56:16   [illegible]
Apr 16 09:56:15   [illegible]
Apr 16 09:56:15   [illegible]
Apr 16 09:56:13   [illegible]
Apr 16 09:54:41   [illegible]
Apr 16 09:50:28   [illegible]
Apr 16 09:50:28   [illegible]
```

The log section displays a list of events that have taken place on the Peplink Balance unit. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

## IPsec Event Log

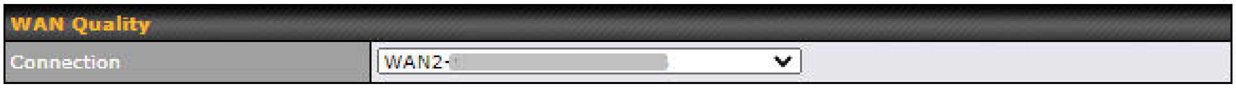


```
Dec 30 08:32:26   IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
Dec 30 08:31:46   IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
Sep 04 01:01:29   IPsec: Amazon Singapore/1x1 - Initiating Main Mode connection...
                                                                         End of log
```

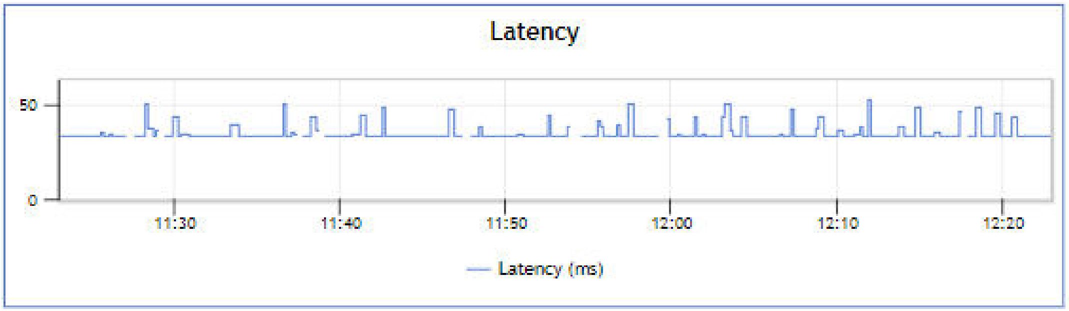
This section displays a list of events that have taken place within an IPsec VPN connection.

Check the box next to **Auto Refresh** and the log will be refreshed automatically.
For an AP event log, navigate to **AP > Info**.

## 13.2 WAN Quality



| WAN Quality | |
|---|---|
| Connection | WAN2-[redacted] |



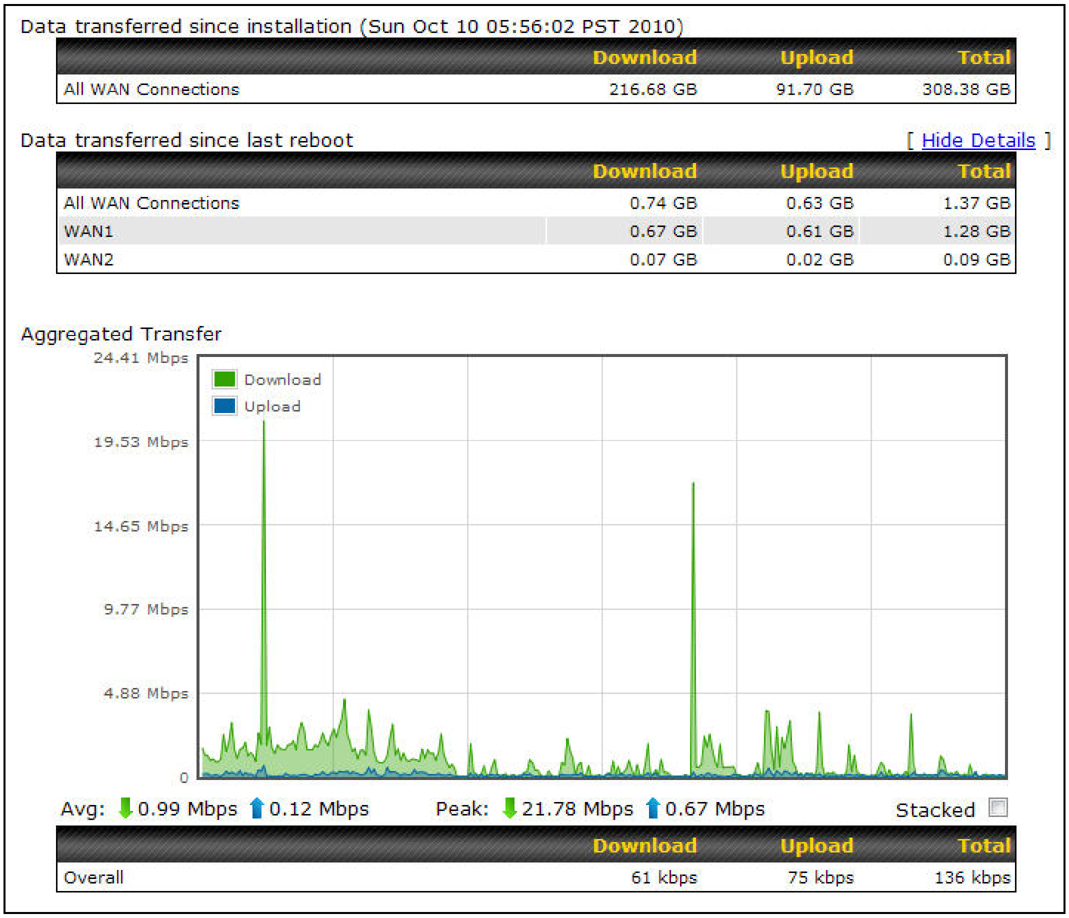
The **Status > WAN Quality** allows to show detailed information about each connected WAN connection.

## 13.3 Usage Reports

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

### 13.3.1 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 (Sun Oct 10 05:56:02 PST 2010)

| | Download | Upload | Total |
|---|---|---|---|
| All WAN Connections | 216.68 GB | 91.70 GB | 308.38 GB |

Data transferred since last reboot [ Hide Details ]

| | Download | Upload | Total |
|---|---|---|---|
| All WAN Connections | 0.74 GB | 0.63 GB | 1.37 GB |
| WAN1 | 0.67 GB | 0.61 GB | 1.28 GB |
| WAN2 | 0.07 GB | 0.02 GB | 0.09 GB |

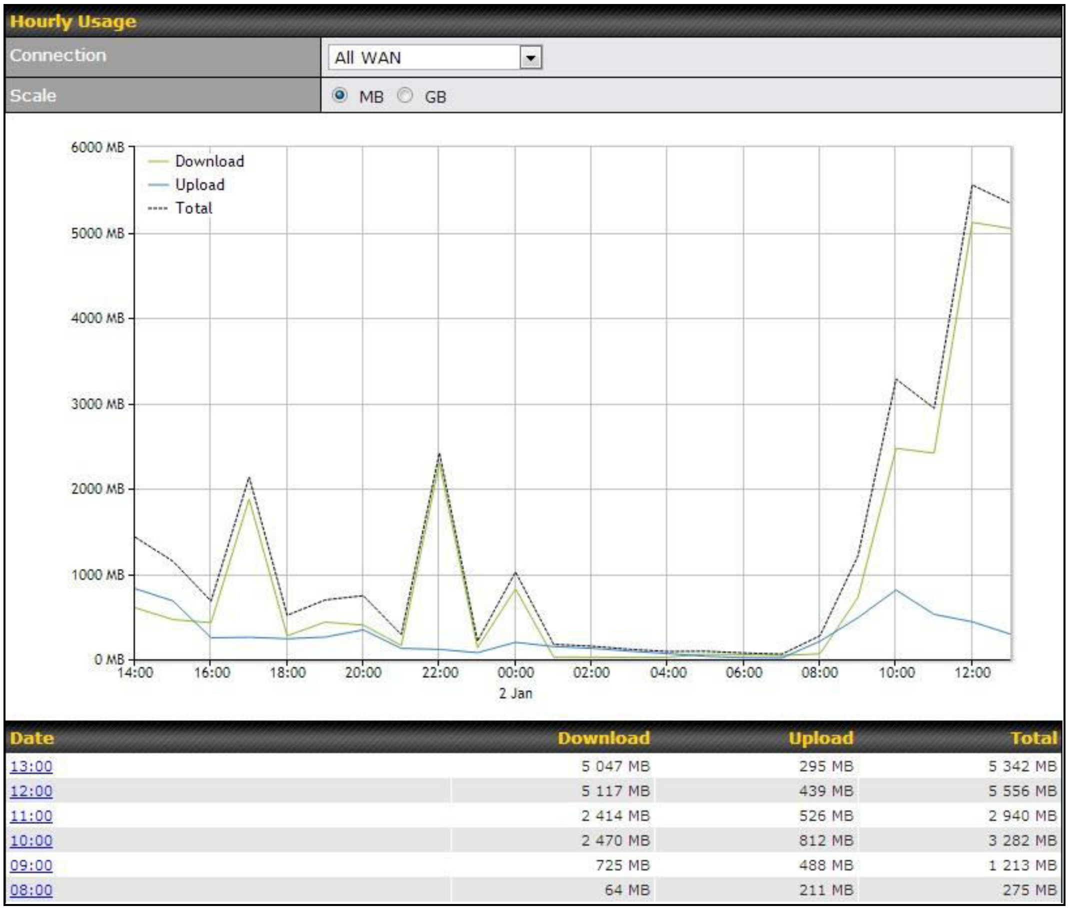
Aggregated Transfer

Avg: ⬇ 0.99 Mbps ⬆ 0.12 Mbps Peak: ⬇ 21.78 Mbps ⬆ 0.67 Mbps Stacked □

| | Download | Upload | Total |
|---|---|---|---|
| Overall | 61 kbps | 75 kbps | 136 kbps |

### 13.3.2 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 |
| Scale | ● MB ○ GB |

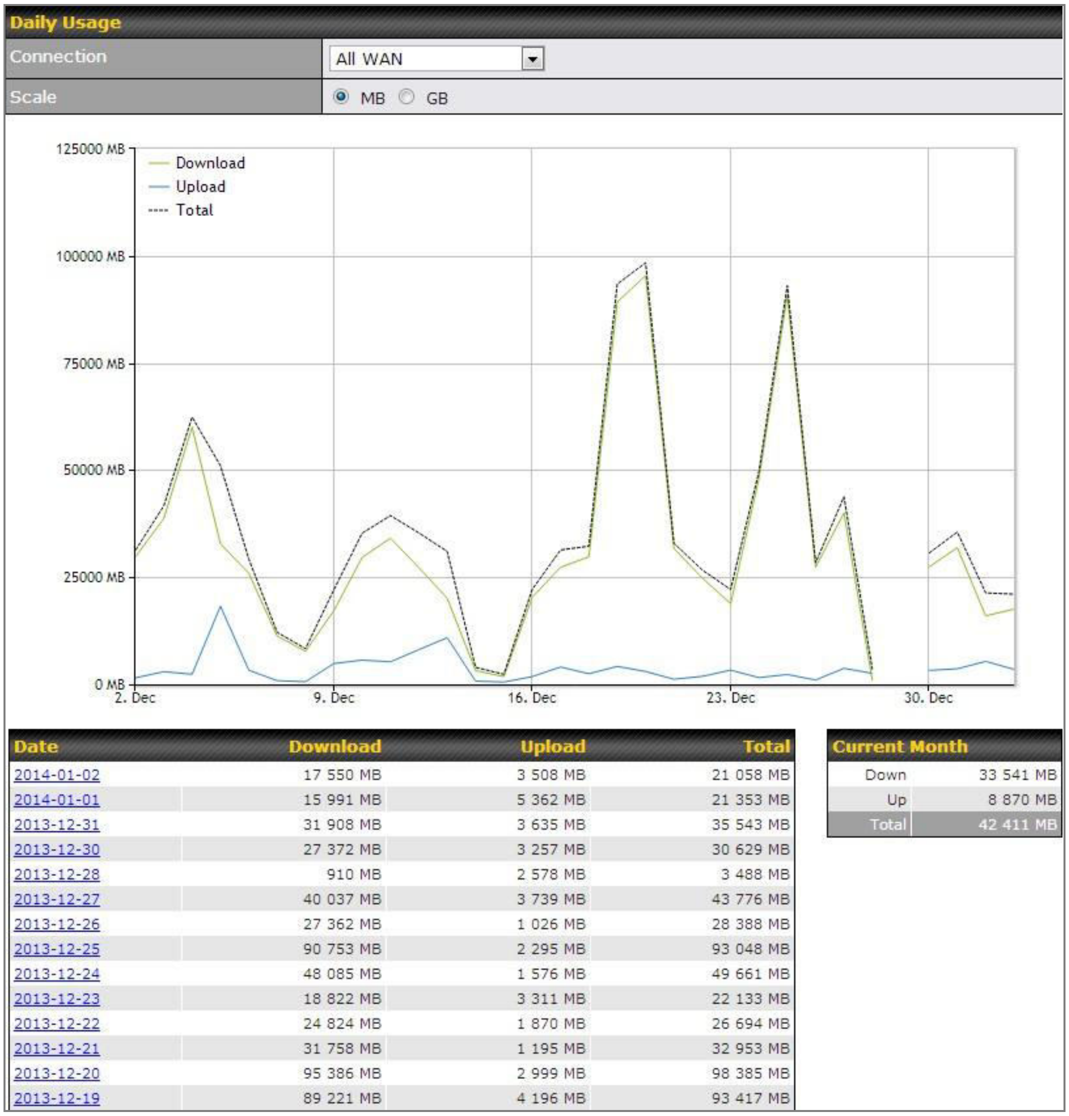
| Date | Download | Upload | Total |
|---|---|---|---|
| 13:00 | 5 047 MB | 295 MB | 5 342 MB |
| 12:00 | 5 117 MB | 439 MB | 5 556 MB |
| 11:00 | 2 414 MB | 526 MB | 2 940 MB |
| 10:00 | 2 470 MB | 812 MB | 3 282 MB |
| 09:00 | 725 MB | 488 MB | 1 213 MB |
| 08:00 | 64 MB | 211 MB | 275 MB |

### 13.3.3 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 as shown in **Section 13.4,** 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**).



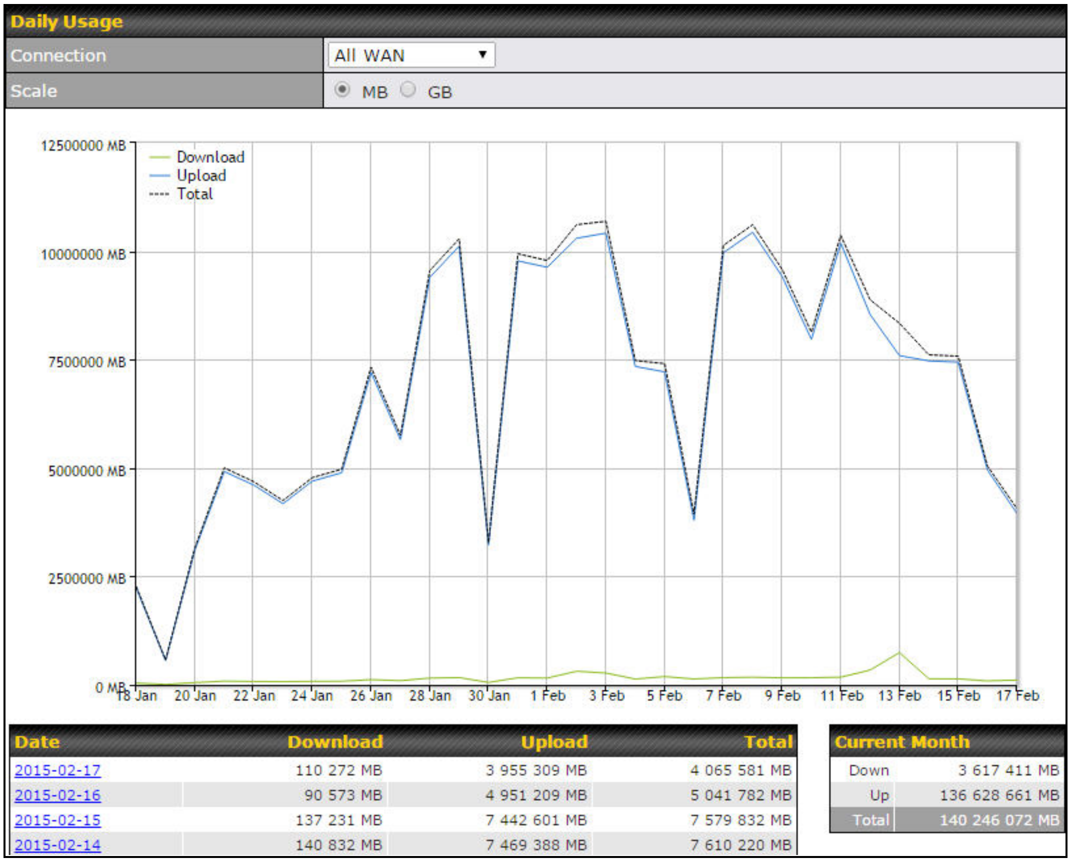
**Daily Usage**

| | |
|---|---|
| Connection | All WAN ▾ |
| Scale | ● MB ○ GB |

| Date | Download | Upload | Total |
|---|---|---|---|
| 2014-01-02 | 17 550 MB | 3 508 MB | 21 058 MB |
| 2014-01-01 | 15 991 MB | 5 362 MB | 21 353 MB |
| 2013-12-31 | 31 908 MB | 3 635 MB | 35 543 MB |
| 2013-12-30 | 27 372 MB | 3 257 MB | 30 629 MB |
| 2013-12-28 | 910 MB | 2 578 MB | 3 488 MB |
| 2013-12-27 | 40 037 MB | 3 739 MB | 43 776 MB |
| 2013-12-26 | 27 362 MB | 1 026 MB | 28 388 MB |
| 2013-12-25 | 90 753 MB | 2 295 MB | 93 048 MB |
| 2013-12-24 | 48 085 MB | 1 576 MB | 49 661 MB |
| 2013-12-23 | 18 822 MB | 3 311 MB | 22 133 MB |
| 2013-12-22 | 24 824 MB | 1 870 MB | 26 694 MB |
| 2013-12-21 | 31 758 MB | 1 195 MB | 32 953 MB |
| 2013-12-20 | 95 386 MB | 2 999 MB | 98 385 MB |
| 2013-12-19 | 89 221 MB | 4 196 MB | 93 417 MB |

| Current Month | |
|---|---|
| Down | 33 541 MB |
| Up | 8 870 MB |
| Total | 42 411 MB |

Status



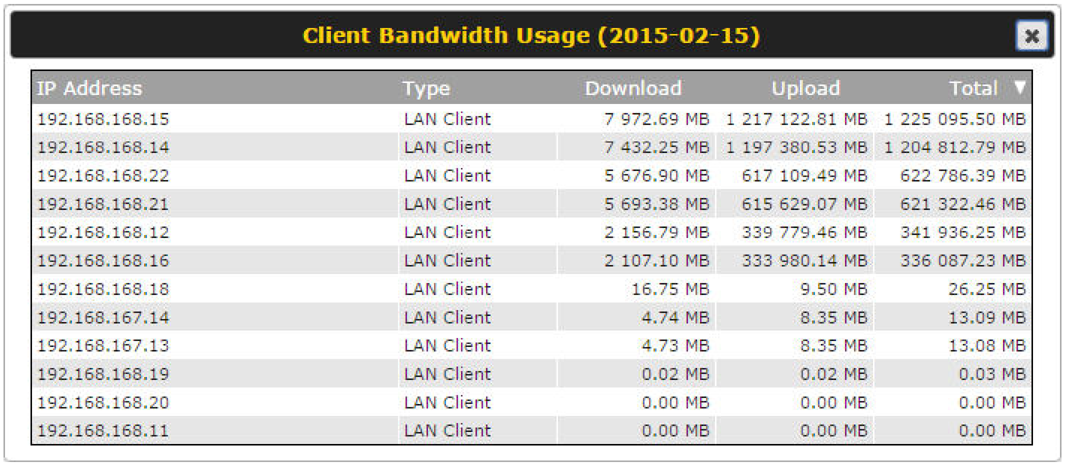
**Daily Usage**

| | |
|---|---|
| Connection | All WAN ▾ |
| Scale | ● MB ○ GB |

| Date | Download | Upload | Total |
|---|---|---|---|
| 2015-02-17 | 110 272 MB | 3 955 309 MB | 4 065 581 MB |
| 2015-02-16 | 90 573 MB | 4 951 209 MB | 5 041 782 MB |
| 2015-02-15 | 137 231 MB | 7 442 601 MB | 7 579 832 MB |
| 2015-02-14 | 140 832 MB | 7 469 388 MB | 7 610 220 MB |

| Current Month | |
|---|---|
| Down | 3 617 411 MB |
| Up | 136 628 661 MB |
| Total | 140 246 072 MB |

Click on a specific date to receive a breakdown of all client usage for that date.



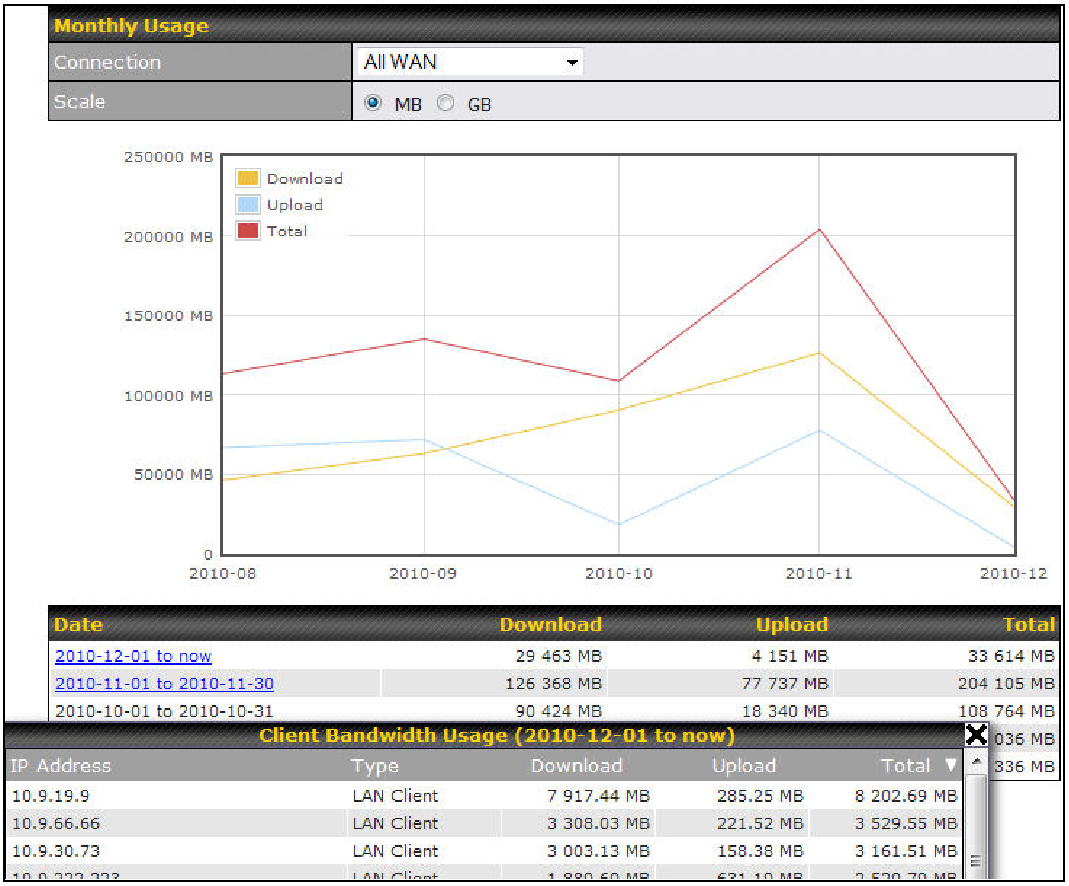
**Client Bandwidth Usage (2015-02-15)**

| IP Address | Type | Download | Upload | Total ▼ |
|---|---|---|---|---|
| 192.168.168.15 | LAN Client | 7 972.69 MB | 1 217 122.81 MB | 1 225 095.50 MB |
| 192.168.168.14 | LAN Client | 7 432.25 MB | 1 197 380.53 MB | 1 204 812.79 MB |
| 192.168.168.22 | LAN Client | 5 676.90 MB | 617 109.49 MB | 622 786.39 MB |
| 192.168.168.21 | LAN Client | 5 693.38 MB | 615 629.07 MB | 621 322.46 MB |
| 192.168.168.12 | LAN Client | 2 156.79 MB | 339 779.46 MB | 341 936.25 MB |
| 192.168.168.16 | LAN Client | 2 107.10 MB | 333 980.14 MB | 336 087.23 MB |
| 192.168.168.18 | LAN Client | 16.75 MB | 9.50 MB | 26.25 MB |
| 192.168.167.14 | LAN Client | 4.74 MB | 8.35 MB | 13.09 MB |
| 192.168.167.13 | LAN Client | 4.73 MB | 8.35 MB | 13.08 MB |
| 192.168.168.19 | LAN Client | 0.02 MB | 0.02 MB | 0.03 MB |
| 192.168.168.20 | LAN Client | 0.00 MB | 0.00 MB | 0.00 MB |
| 192.168.168.11 | LAN Client | 0.00 MB | 0.00 MB | 0.00 MB |

### 13.3.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled **Bandwidth Monitoring** feature as shown in **Section 13.4**, 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 |
|---|---|---|---|
| 2010-12-01 to now | 29 463 MB | 4 151 MB | 33 614 MB |
| 2010-11-01 to 2010-11-30 | 126 368 MB | 77 737 MB | 204 105 MB |
| 2010-10-01 to 2010-10-31 | 90 424 MB | 18 340 MB | 108 764 MB |
| | | | 036 MB |
| | | | 336 MB |

**Client Bandwidth Usage (2010-12-01 to now)**

| IP Address | Type | Download | Upload | Total ▼ |
|---|---|---|---|---|
| 10.9.19.9 | LAN Client | 7 917.44 MB | 285.25 MB | 8 202.69 MB |
| 10.9.66.66 | LAN Client | 3 308.03 MB | 221.52 MB | 3 529.55 MB |
| 10.9.30.73 | LAN Client | 3 003.13 MB | 158.38 MB | 3 161.51 MB |

Click on a specific month to receive a breakdown of all client usage for that month.

# Appendix

## Appendix A. Restoration of Factory Defaults

To restore the factory default settings on a Peplink Balance unit, perform the following:

**For Balance models with a reset button:**

1. Locate the reset button on the Peplink Balance unit.
2. With a paperclip, press and keep the reset button pressed.

Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

Hold for approximately 20 seconds for factory reset (Note: The LED status light blinks in RED 3 times and release the button, all WAN/LAN port lights start blinking)

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

**For Balance/MediaFast models with an LCD menu:**

- Use the buttons on the front panel to control the LCD menu to go to **Maintenance**>**Factory Defaults**, and then choose **Yes** to confirm.

Afterwards, 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. |

## Appendix B. Routing under DHCP, Static IP, and PPPoE

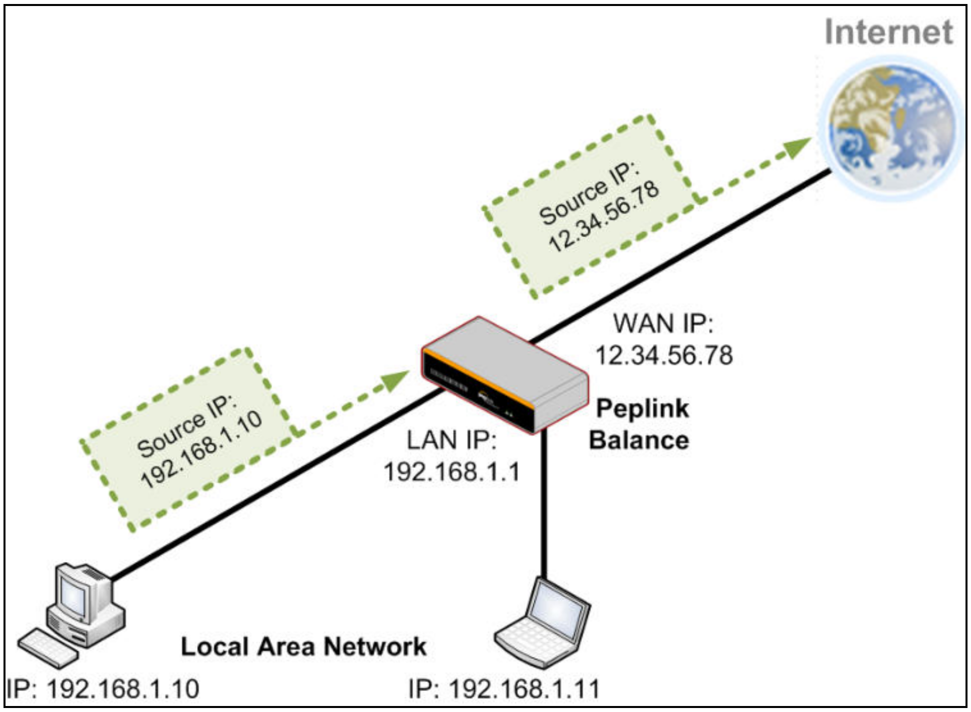
The information in this appendix applies only to situations where the Peplink Balance operates a WAN connection under DHCP, Static IP, or PPPoE.

### B.1 Routing Via Network Address Translation (NAT)

When the Peplink Balance is operating under NAT mode, the source IP addresses of outgoing IP packets are translated to the WAN IP address of the Peplink Balance. With NAT, all LAN devices share the same WAN IP address to access the Internet (i.e., the WAN IP address of the Peplink Balance).

Operating the Peplink Balance in NAT mode requires only one WAN (Internet) IP address. In addition, operating in NAT mode also has security advantages because LAN devices are hidden behind the Peplink Balance. They are not directly accessible from the Internet and hence less vulnerable to attacks.

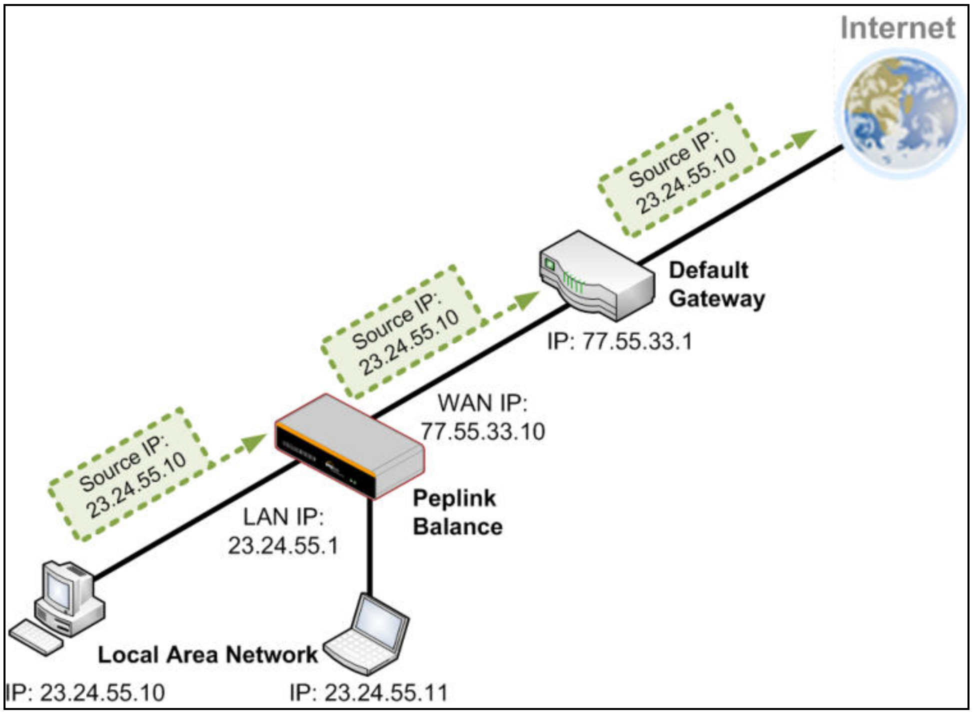
The following figure shows the packet flow in NAT mode:



## B.2 Routing Via IP Forwarding

When the Peplink Balance is operating under IP forwarding mode, the IP addresses of IP packets are unchanged; the Peplink Balance forwards both inbound and outbound IP packets without changing their IP addresses.

The following figure shows the packet flow in IP forwarding mode:


Internet
Source IP: 23.24.55.10
Default Gateway
IP: 77.55.33.1
Source IP: 23.24.55.10
WAN IP: 77.55.33.10
Source IP: 23.24.55.10
Peplink Balance
LAN IP: 23.24.55.1
Local Area Network
IP: 23.24.55.10
IP: 23.24.55.11

# Appendix C. 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.