

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

^A - Advanced feature. Click the  button on the top right-hand corner to activate.

Important Note

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

Integrated AP	
Wi-Fi Operating Mode	☒ WAN ☐ WAN + AP ☐ AP

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

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

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

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

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

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

This allows users to configure AP Time Settings (both Timezone and NTP) in AP Controller.

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

Controller Management Settings	
Manage Unreachable Action	☐

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

AP Controller Settings	
Client Load Balancing	☐

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

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

Wi-Fi Radio Settings	
Operating Country	United States ▼
Wi-Fi Antenna	☐ Internal ☒ External

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

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

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

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

25 AP Controller Status

25.1 Info

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



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

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

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

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

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

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

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

Controller Management Settings	
Manage Unreachable Action	☐

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

AP Controller Settings	
Client Load Balancing	☐

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

25.2 Access Point

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

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

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

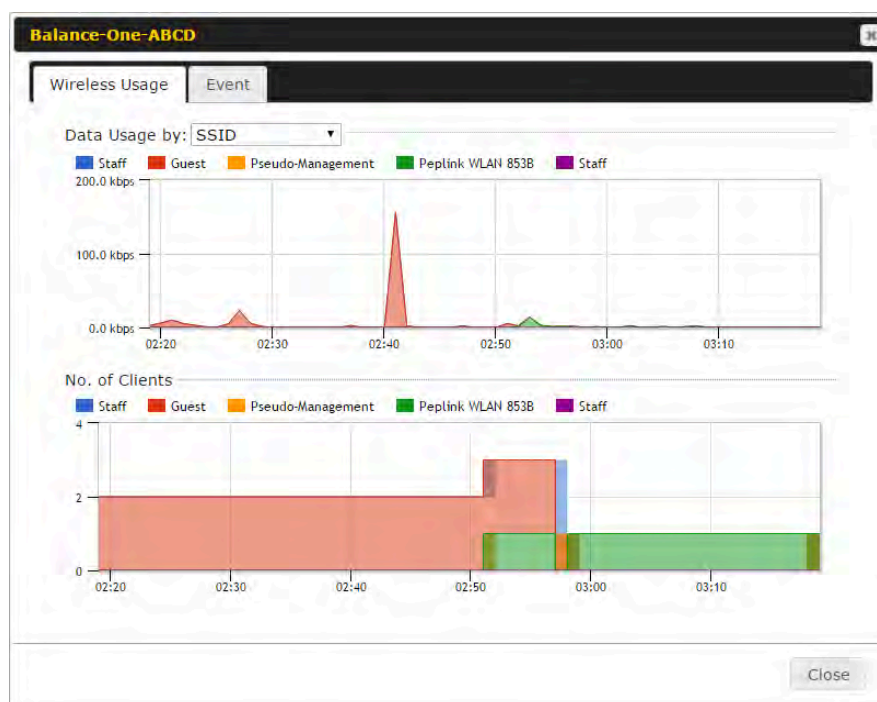
Client List						
MAC Address	IP Address	Type	Signal	SSID	Upload	Download
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB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

Click the icon to configure each client

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

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

Click the icon to see a graph displaying usage:



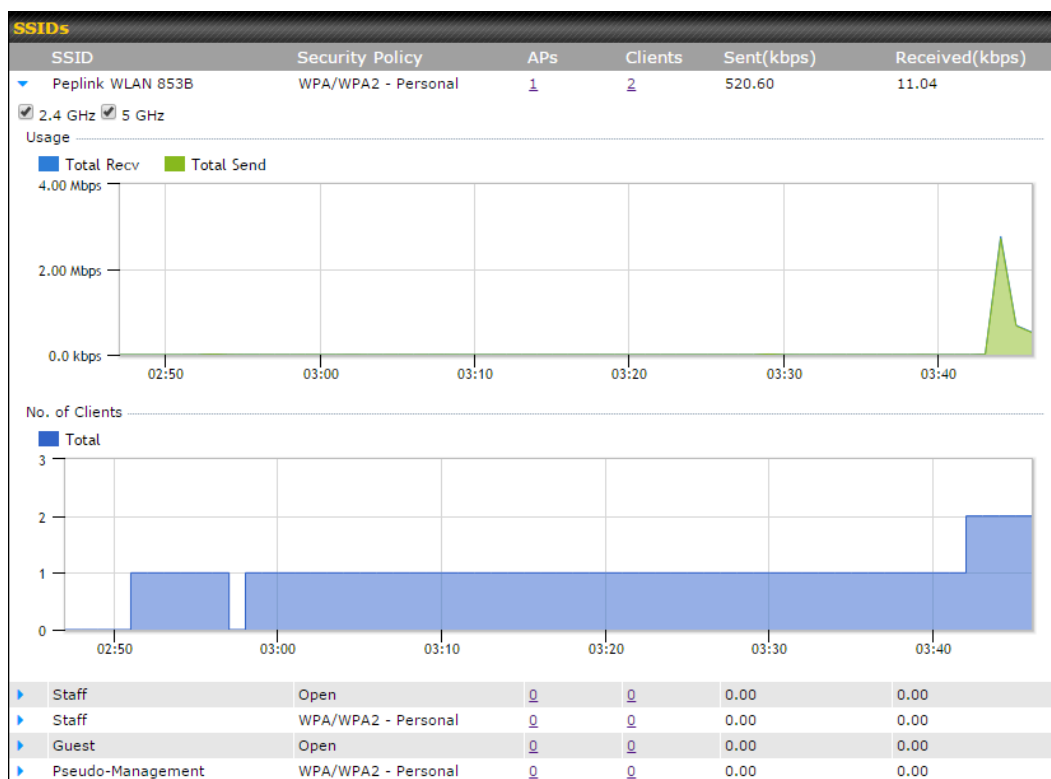
Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate.

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

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

25.3 Wireless SSID

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



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

25.4 Wireless Client

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

Search Filter

Search Key

Client MAC Address / SSID / AP Serial Number

Maximum Result (1-256)

50

Show Associated Clients Only

☐

Search Result

Search

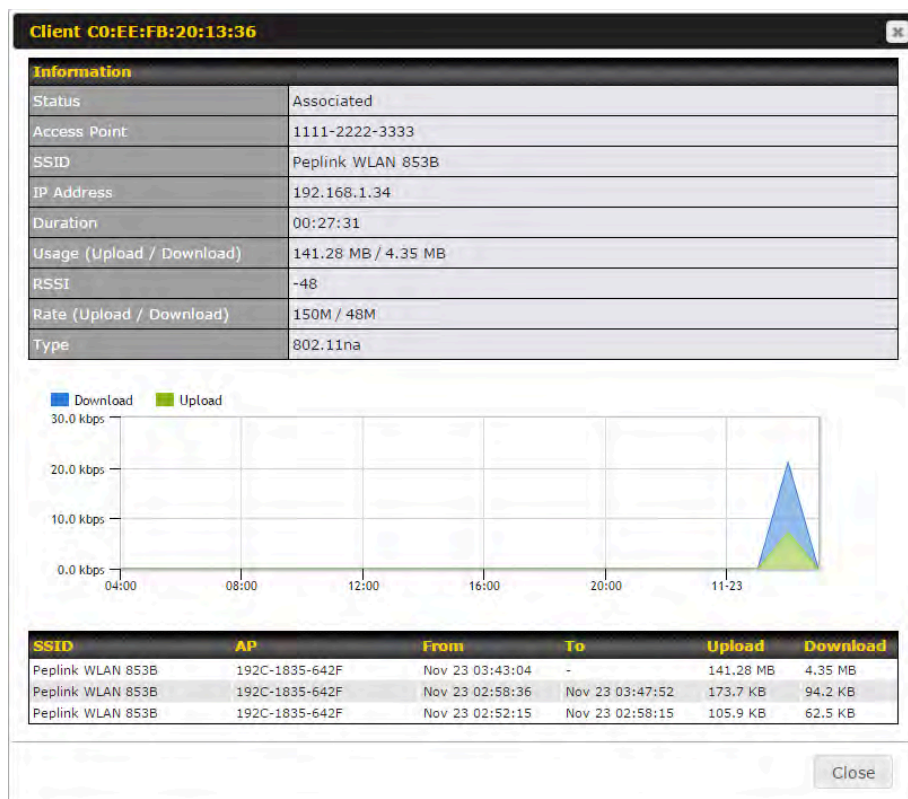
Wireless Clients

Name / MAC Address	IP Address	Type	Mode	RSSI (dBm)	SSID	AP	Duration
HUAWEI Mate 40 P...	-	802.11ng	-	-	-	-	-

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

Client	Upload	Download
No information		

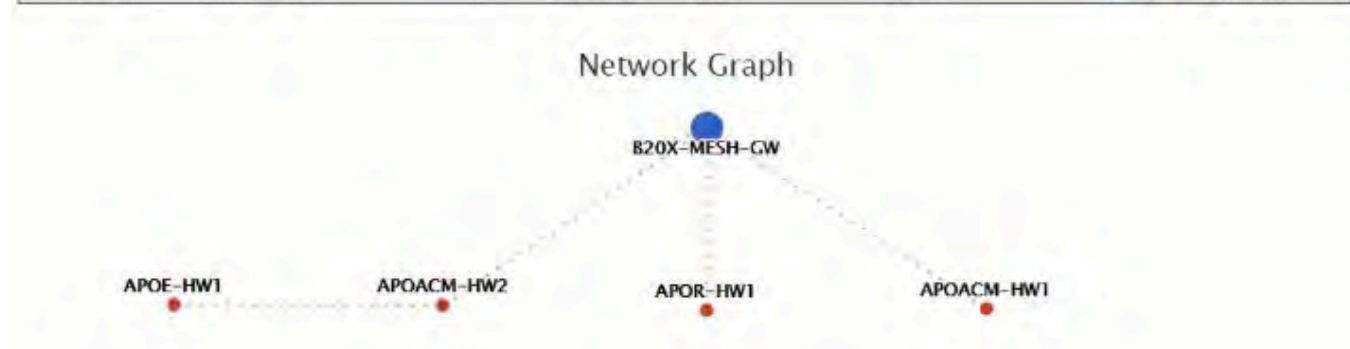
Here, you will be able to see your network's heaviest users as well as search for specific users. Click the ☆ icon to bookmark specific users, and click the 📊 icon for additional details about each user:



25.5 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



25.6 Nearby Device

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

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

Suspected Rogue Devices

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

25.7 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	☐
Search	

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

Events

This event log displays all activity on your AP network, down to the client level. 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.

26 Toolbox

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

Firmware Packs			
Pack ID	Release Date	Details	Action
1126	2017-08-26		
Check for Updates Manual Upload Default... No default defined.			

Firmware Packs

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

27 Switch

27.1 Switch Controller

Navigate to **Switch Tab > Switch Controller > Controller**.

Switch Controller	
Switch Controller	☒ Enable
Save	

Registered Switches				
Name / Serial Number	Model	IP Address	MAC	
1933- [REDACTED]	24 PoE 2.5G Switch	192.168.52.63	D4:13: [REDACTED]	X

Available Switches				
Name / Serial Number	Model	IP Address	MAC	
1933- [REDACTED]	48 PoE 2.5G Switch	192.168.52.93	D4:13: [REDACTED]	+

X

Switch " " will be registered to this Switch Controller. Are you sure?

☒ Preserve port settings with common VLAN networks on this Switch

OKCancel

Switch Controller

Registered Switches List of registered switches. Press "X" to remove the selected switch from the list.

Available Switches List of available switches connected to the device. Press "+" to register the selected switch to the Registered Switches list.

Note: When option "Preserve port settings with common VLAN networks on this Switch" is tick when register selected switch, the port settings which

VLANs are defined in Switch Controller will be preserved. Else, will be replaced by VLAN 1.

NOTE: PoE 2.5G Switch will only be managed by either InControl or Device switch controller. Do not enable the Switch Controller if the switch needs to be managed by InControl.

27.2 Admin Security

Navigate to **Switch Tab > Switch Controller > Admin Security**.

There are two types of user accounts available for accessing the Web Admin: **admin** and **user**. The **admin** login has full administrative access, while the **user** login 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	
Admin User Name	admin
Admin Password	
Confirm Admin Password	
Read-only User Name	user
Read-only Password	
Confirm Read-only Password	
Web Session Timeout	4 Hours 0 Minutes
Security	HTTPS ▼
Web Admin Port	443

Save

Admin Settings

Admin User Name	Admin User Name is set as <i>admin</i> 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 <i>user</i> by default, but can be changed, if desired.
Read-only Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm Read-only Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to 4 hours .
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: ○ HTTP ○ HTTPS Default will be HTTPS.
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.

27.3 Switch Information

Switch Information	
Device	1933-CF25-5CC4 ▼
Name	-
Serial Number	1933-CF25-5CC4
Model	24 PoE 2.5G Switch
IP Address	192.168.52.63
MAC Address	D4:13:F8:22:A7:A0

Switch Information

Device Drop down list to select Switch to be configured.

Name Name of the switch.(not sure where to define)

Serial Number Selected switch serial number.

Model Selected switch model.

IP Address Uplink IP address of the selected switch.

MAC Address Selected switch MAC address.

27.4 STP

Navigate to **Switch Tab > STP**.

STP Bridge 	
Mode	RSTP
Priority 	32768 (Default) ▼
Hello Time 	2 (Default) ▼ seconds
Forward Delay 	15 (Default) ▼ seconds
Max Age 	20 (Default) ▼ seconds
IEEE 802.1D recommends: $2 \times (\text{Bridge Forward Delay} - 1.0 \text{ seconds}) \geq \text{Bridge Max Age}$ $\text{Bridge Max Age} \geq 2 \times (\text{Bridge Hello Time} + 1.0 \text{ seconds})$	

Save

STP Bridge

Mode RSTP

Priority This field specifies the bridge priority for root switch election. The switch with the lowest bridge priority is elected as the root switch (Default value: 32768).

Hello Time (A) Time between each exchange of bridge protocol data units (BPDU). (Default value: 2 seconds).

Forward Delay (A) Delay used by STP Bridges to transit Root and Designated Ports to Forwarding. (Default value: 15 seconds).

Max Age (A) Maximum age of the information transmitted by the bridge when it is the Root Bridge. (Default value: 20 seconds).

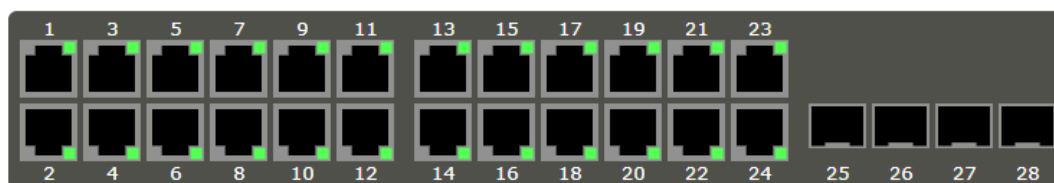
(A) – Advanced feature. Click the  button on the top right-hand corner to activate.

27.5 Switch Ports

Navigate to **Switch Tab > Interfaces > Switch Ports**.

For each port, you can set PoE scheduling, port type (Trunk and Access), as well as the VLAN

which they belong to.



Port Settings							
ID	Name	Port Type	VLAN Networks	PVID	PoE	RSTP	
1		Trunk	All	Default VLAN - Auto	⚡	✓	
2		Trunk	All	Default VLAN - Auto	⚡	✓	
3		Trunk	All	Default VLAN - Auto	⚡	✓	
4		Trunk	All	Default VLAN - Auto	⚡	✓	
5		Trunk	All	Default VLAN - Auto	⚡	✓	
6		Trunk	All	Default VLAN - Auto	⚡	✓	
7		Trunk	All	Default VLAN - Auto	⚡	✓	
8		Trunk	All	Default VLAN - Auto	⚡	✓	
9		Trunk	All	Default VLAN - Auto	⚡	✓	
10		Trunk	All	Default VLAN - Auto	⚡	✓	
11		Trunk	All	Default VLAN - Auto	⚡	✓	
12		Trunk	All	Default VLAN - Auto	⚡	✓	
13		Trunk	All	Default VLAN - Auto	⚡	✓	
14		Trunk	All	Default VLAN - Auto	⚡	✓	

To configure port, you may click on the port icon or the pen icon from the Port Settings table to show the Port parameters.

Port Settings

1

3

5

7

9

11

13

15

17

19

21

23

2

4

6

8

10

12

14

16

18

20

22

24

25

26

27

28

Port 1

Name	
Enable	☒
PoE Enable	☒
Speed	Auto
Port Type	Trunk
VLAN Networks	All
PVID	☒ Default VLAN
RSTP	☒

Save

Cancel

Port Settings

Name	Set a name for the port
Enable checkbox	Enables / Disables the Port
PoE Enable checkbox	Enables / Disables PoE on the Port
Speed[^]	Set the port speed to Auto, 10 Mbps half/full duplex or 100 Mbps half/full duplex, or 1GB full duplex.
Port Type	Set as Trunk or Access
VLAN Networks	Designate one or more VLANs to be used on this port.

PVID**	Untagged frames received by the port are classified to a VLAN indicated by Port VLAN Identifier (PVID). All frames from the VLAN are untagged on egress.**
---------------	--

RSTP checkbox	Enables or Disables Rapid Spanning Tree Protocol
--------------------------	--

** PVID option is only configurable when Port Type is set to “Trunk”.

^ Configuration options on certain ports are configurable port speeds to 2.5 Gbps. May refer to the datasheet or label below switch ports.

^ Configurable options on SFP+ ports are similar as above, but configurable port speeds are between 100 Mbps Full Duplex up to 10 Gbps Full Duplex.

27.6 LACP (802.3ad) Configuration

LACP is part of the IEEE specification 802.3ad and allows you to bundle several physical ports to form a single logical channel.

Bundling multiple physical ports into a single logical link allows you to increase throughput beyond the limitations of a single connection and provides redundancy in case one link goes down.

Select multiple ports by clicking on them and selecting the **Link Aggregation** checkbox to enable link aggregation for the selected ports.

Port Settings

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

Link Aggregation

☒ Active

Port 21, 22

Name

Enable

☒

PoE Enable

☒

Speed

Auto

Port Type

Trunk

VLAN Networks

All

PVID

☒ Default VLAN

RSTP

Enable

Save

Cancel

28 System Settings

28.1 Admin Security

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

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

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

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

configuration is located at **System > Admin Security**.

Admin Settings

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

LAN Connection Access Settings

Allowed LAN Networks	☒ Any ☐ Allow this network only
----------------------	--

WAN Connection Access Settings

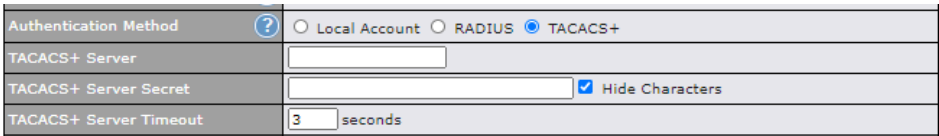
Allowed Source IP Subnets	☒ Any ☐ Allow access from the following IP subnets only									
Allowed WAN IP Address(es)	<table> <thead> <tr> <th>Connection / IP Address(es)</th> <th>All</th> <th>Clear</th> </tr> </thead> <tbody> <tr><td>☐ WAN</td></tr> <tr><td>☐ Cellular</td></tr> <tr><td>☐ Wi-Fi WAN on 2.4 GHz</td></tr> <tr><td>☐ Wi-Fi WAN on 5 GHz</td></tr> <tr><td>☐ VLAN WAN 1</td></tr> <tr><td>☐ OpenVPN WAN 1</td></tr> </tbody> </table>	Connection / IP Address(es)	All	Clear	☐ WAN	☐ Cellular	☐ Wi-Fi WAN on 2.4 GHz	☐ Wi-Fi WAN on 5 GHz	☐ VLAN WAN 1	☐ OpenVPN WAN 1
Connection / IP Address(es)	All	Clear								
☐ WAN										
☐ Cellular										
☐ Wi-Fi WAN on 2.4 GHz										
☐ Wi-Fi WAN on 5 GHz										
☐ VLAN WAN 1										
☐ OpenVPN WAN 1										

Save

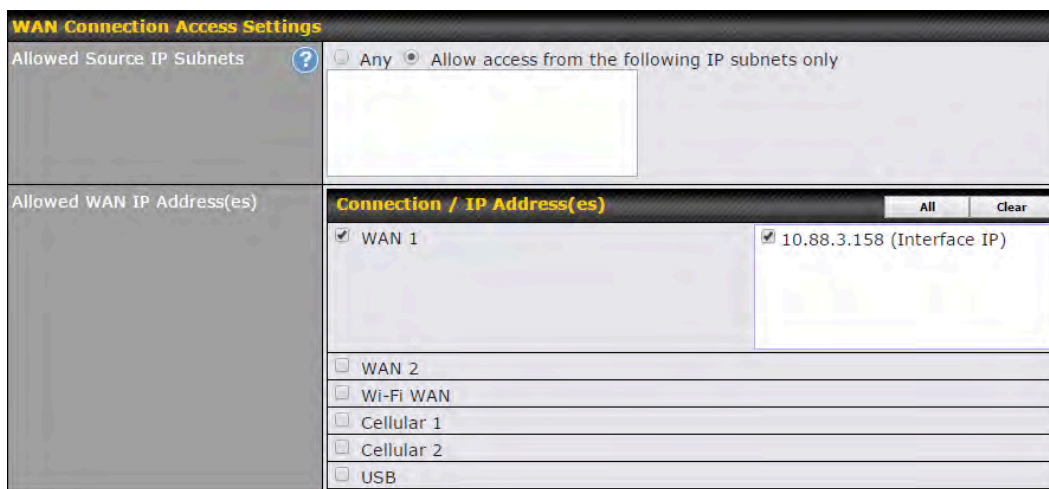
Admin Settings

Device Name This field allows you to define a name for this Peplink router. By default, **Device**

	Name is set as MAX_XXXX , where XXXX refers to the last 4 digits of the unit's serial number.																																							
Admin User Name	Admin User Name is set as <i>admin</i> 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 <i>user</i> by default, but can be changed, if desired.																																							
Read-only Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.																																							
Confirm Read-only Password	This field allows you to verify and confirm the new user password.																																							
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Peplink router terminates its access to the web admin interface. By default, it is set to 4 hours .																																							
Authentication Method	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.																																							
	Available options: - Local Account - RADIUS (Secondary is optional as a backup)																																							
	<table><tr><th colspan="3">RADIUS Settings</th></tr><tr><th></th><th>Primary</th><th>Secondary</th></tr><tr><td>Authentication Protocol</td><td colspan="2">MS-CHAP v2 ▾</td></tr><tr><td>Authentication Profile</td><td>▾</td><td>▾</td></tr><tr><td>Authentication Host</td><td></td><td></td></tr><tr><td>Authentication Port</td><td>1812</td><td>1812</td></tr><tr><td>Authentication Secret</td><td> ☒ Hide Characters</td><td> ☒ Hide Characters</td></tr><tr><td>Accounting Profile</td><td>▾</td><td>▾</td></tr><tr><td>Accounting Host</td><td></td><td></td></tr><tr><td>Accounting Port</td><td>1813</td><td>1813</td></tr><tr><td>Accounting Secret</td><td> ☒ Hide Characters</td><td> ☒ Hide Characters</td></tr><tr><td>Authentication Timeout</td><td colspan="2">3 seconds</td></tr><tr><td>Source Network Address</td><td colspan="2">VLAN 21 (21) ▾</td></tr></table>	RADIUS Settings				Primary	Secondary	Authentication Protocol	MS-CHAP v2 ▾		Authentication Profile	▾	▾	Authentication Host			Authentication Port	1812	1812	Authentication Secret	 ☒ Hide Characters	 ☒ Hide Characters	Accounting Profile	▾	▾	Accounting Host			Accounting Port	1813	1813	Accounting Secret	 ☒ Hide Characters	 ☒ Hide Characters	Authentication Timeout	3 seconds		Source Network Address	VLAN 21 (21) ▾	
RADIUS Settings																																								
	Primary	Secondary																																						
Authentication Protocol	MS-CHAP v2 ▾																																							
Authentication Profile	▾	▾																																						
Authentication Host																																								
Authentication Port	1812	1812																																						
Authentication Secret	 ☒ Hide Characters	 ☒ Hide Characters																																						
Accounting Profile	▾	▾																																						
Accounting Host																																								
Accounting Port	1813	1813																																						
Accounting Secret	 ☒ Hide Characters	 ☒ Hide Characters																																						
Authentication Timeout	3 seconds																																							
Source Network Address	VLAN 21 (21) ▾																																							

	Authentication Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .
	Authentication Host	This specifies the IP address or hostname of the RADIUS server host.
	Authentication Port	This setting specifies the UDP destination port for authentication requests.
	Authentication Secret	This field is for entering the secret key for accessing the RADIUS server.
	Accounting Host	This specifies the IP address or hostname of the RADIUS server host.
	Accounting Port	This setting specifies the UDP destination port for accounting requests.
	Accounting Secret	This field is for entering the secret key for accessing the accounting server.
	Authentication Timeout	This option specifies the time value for authentication timeout
TACACS+		
 The screenshot shows a configuration interface for TACACS+. It includes a 'Authentication Method' section with radio buttons for 'Local Account', 'RADIUS', and 'TACACS+' (which is selected). Below this are fields for 'TACACS+ Server', 'TACACS+ Server Secret' (with a 'Hide Characters' checkbox), and 'TACACS+ Server Timeout' (set to 3 seconds).		
	TACACS+ Server	This specifies the access address of the external TACACS+ server.
	TACACS+ Server Secret	This field is for entering the secret key for accessing the RADIUS server.
	TACACS+ Server Timeout	This option specifies the time value for TACACS+ timeout
CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to Section 31.5 .	
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.	

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



WAN Connection Access Settings

Allowed Source IP Subnets

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

The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., 192.168.0.0), and *m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, 192.168.0.0/24).

To define multiple subnets, separate each IP subnet one in a line. For example:

- 192.168.0.0/24
- 10.8.0.0/16

Allowed WAN IP Address(es)

This is to choose which WAN IP address(es) the web server should listen on.

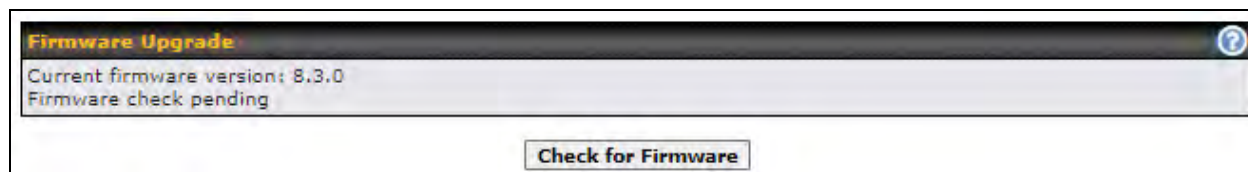
28.2 Firmware

Web admin interface : automatically check for updates

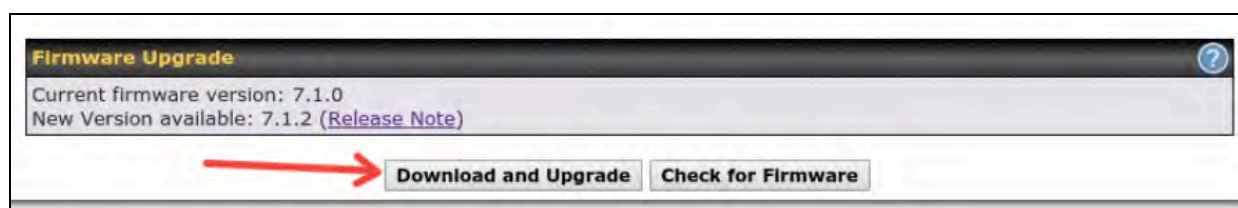
Upgrading firmware can be done in one of three ways.

Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

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



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



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.

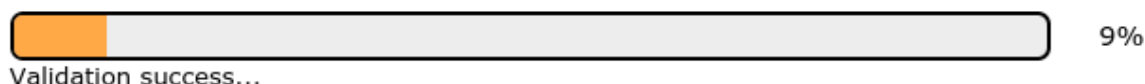
The router will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



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.



**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/Peplink GA firmware can be found [here](#). Navigate to the relevant product line (ie. Balance, Max, FusionHub, 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 ▼ Search:						
Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual	
Balance 1350	HW2	7.1.2	Download	PDF	PDF	
Balance 1350	HW1	6.3.4	Download	PDF	PDF	
Balance 20	HW1-6	7.1.2	Download	PDF	PDF	
Balance 210	HW4	7.1.2	Download	PDF	PDF	

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

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

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

Manual Firmware Upgrade

Firmware Image

Choose File

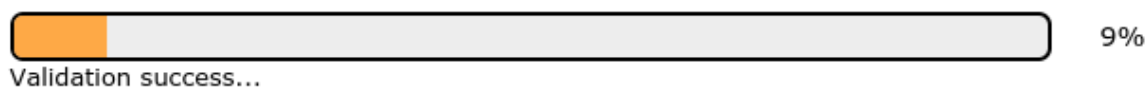
No file chosen

Manual Upgrade

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

Firmware Upgrade

It may take up to 8 minutes.



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

The InControl method

[Described in this knowledgebase article on our forum.](#)

28.3 Time

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

Time Settings

Time Zone	(UTC) Coordinated Universal Time Show all
Time Sync	Time Server
Time Server	0.pepwave.pool.ntp.org time.google.com
Time Server Source Network Address	Untagged LAN (1)

Save

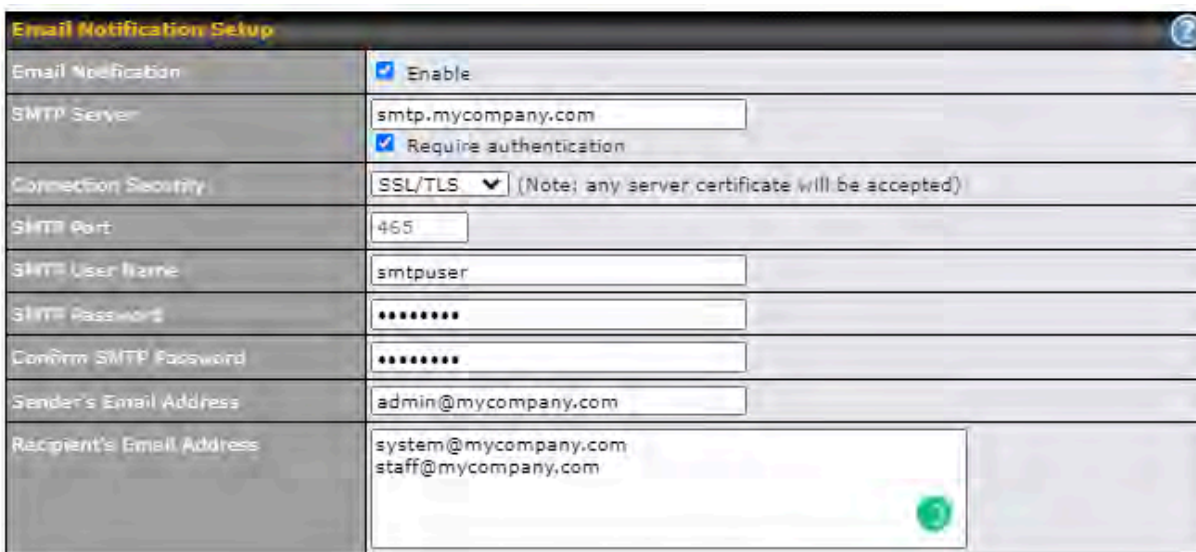
Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The Time Zone value affects the time stamps in the Peplink router's event log and e-mail notifications. Check Show all to show all time zone options.
Time Sync	This field allows to select your time sync mode, the available options are: • Time Server • GPS • GPS with Time Server as fallback
Time Server	This setting specifies the NTP network time server to be utilized by the router. NOTE: Multiple NTP servers can be added starting from firmware version 8.5.3.
Time Server Source Network Address	This setting is to specific which VLAN network will be used for NTP traffic.

28.4 Schedule

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

Name	Time	Used by
No schedule profiles defined		
New Schedule		

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



Test Email Notification Save

Email Notification Settings

Email Notification	This setting specifies whether or not to enable email notification. If Enable is checked, the Peplink router will send email messages to system administrators when the WAN status changes or when new firmware is available. If Enable is not checked, email notification is disabled and the Peplink router will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check Require authentication .
Connection Security	This setting specifies via a drop-down menu one of the following valid Connection Security: • None • STARTTLS • SSL/TLS
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to 25 . If Connection Security is selected " STARTTLS ", the default port number will be set to 587 . If Connection Security is selected " SSL/TLS ", the default port number will be set to 465 . You may customize the port number by editing this field.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication is checked in the SMTP Server setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.

Sender's Email Address	This setting specifies the email address the Peplink router will use to send reports.
Recipient's Email Address	This setting specifies the email address(es) to which the Peplink router will send email notifications. For multiple recipients, separate each email addresses using the enter key.

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

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

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

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

Email Notification Setup ?	
Email Notification	☒ Enable
SMTP Server	 ☒ Require authentication
Connection Security	SSL/TLS ▼ (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	
SMTP Password	
Confirm SMTP Password	
Sender's Email Address	
Recipient's Email Address	

Test Email Notification **Save**

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
<- 220 smtp.gmail.com ESMTP h11sm3907691pjpg.46 - gsmt
-> 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 AGdwc2dhbjk0QGdtYVlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

28.6 Event Log

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

Send Events to Remote Syslog Server	
Remote Syslog	☐
Remote Syslog Host	
Port:	514
Source Network Address	Untagged LAN ▼
Push Events to Mobile Devices	
Push Events	☐
URL Logging	
Enable	☐
Session Logging	
Enable	☐
Save	

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

Session Logging This setting is to enable event logging at the specified log server.

Session Logging Host This setting specifies the IP address or hostname of the Session log server.



For more information on the Router Utility, go to:
www.peplink.com/products/router-utility

28.7 SNMP

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

SNMP Settings	
SNMP Device Name	MAX_TST_3D88
Location	
SNMP Port	161 Default
SNMPv1	☐ Enable
SNMPv2c	☐ Enable
SNMPv3	☐ Enable
SNMP Trap	☒ Enable
SNMP Trap Community	
SNMP Trap Server	
SNMP Trap Port	162
SNMP Trap Server Heartbeat	☐
Save	

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

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

SNMP Settings

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

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

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

SNMP Community

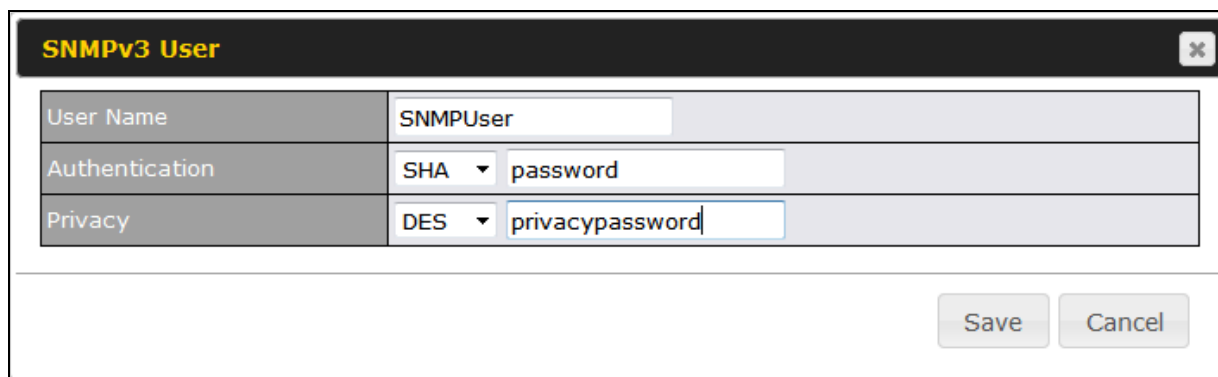
Community Name	My Company	
Allowed Network	192.168.1.25	/ 255.255.255.0 (/24) ▼

Save

Cancel

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:



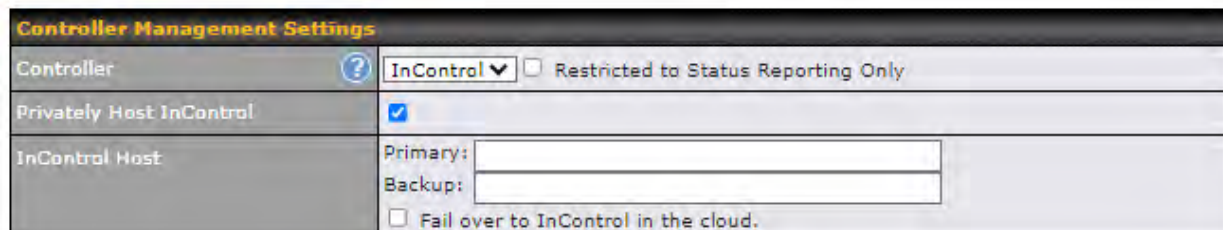
The screenshot shows a window titled "SNMPv3 User" with a close button (X) in the top right corner. It contains three rows of configuration fields:

User Name	SNMPUser
Authentication	SHA password
Privacy	DES privacypassword

At the bottom right, there are two buttons: "Save" and "Cancel".

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

28.8 InControl



The screenshot shows a window titled "Controller Management Settings" with a help icon (?) in the top left corner. It contains the following configuration fields:

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

InControl is a cloud-based service which allows you to manage all of your Peplink devices with

one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

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

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

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

28.9 Configuration

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

Restore Configuration to Factory Settings
?

Restore Factory Settings

Download Active Configurations
?

Download

Upload Configurations
?

Configuration File
Browse...
No file selected.

Upload

Upload Configurations from High Availability Pair
?

Configuration File
Browse...
No file selected.

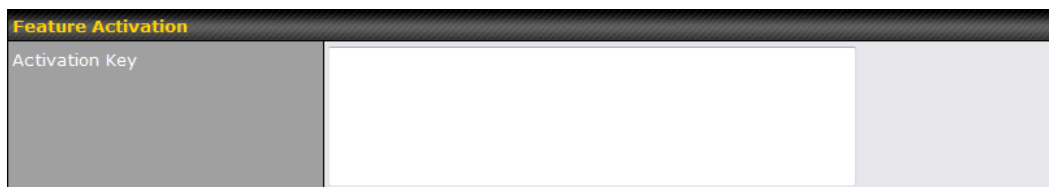
Upload

Configuration	
Restore	The Restore Factory Settings button is to reset the configuration to factory

Configuration to Factory Settings	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, a Peplink router can quickly load the configuration of its HA counterpart. To do so, click the Upload button. After loading the settings, configure the LAN IP address of the Peplink router so that it is different from the HA counterpart.

28.10 Feature Add-ons

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

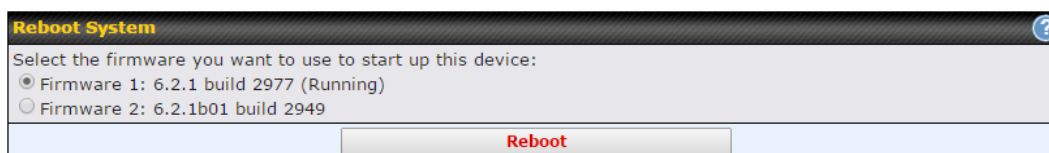


The image shows a web form titled "Feature Activation". It contains a single input field labeled "Activation Key" with a light gray background and a white border. To the right of the input field is a light gray rectangular area, likely a button or a placeholder for another field.

28.11 Reboot

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

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



The image shows a web form titled "Reboot System" with a blue question mark icon in the top right corner. The form contains a text label "Select the firmware you want to use to start up this device:" followed by two radio button options: "Firmware 1: 6.2.1 build 2977 (Running)" and "Firmware 2: 6.2.1b01 build 2949". Below these options is a red "Reboot" button.

29 Tools

29.1 Ping

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

Ping

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

Start

Stop

Results

Clear Log

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

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

Tip

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