

User's Guide

TRENDNET[®]



N600 High Power Dual Band PoE Access Point

TEW-753DAP

Table of Contents

Product Overview	1	Setup Wizard.....	12
Package Contents.....	1	Save/ Reload	13
Features	1	Status	14
Front Panel.....	3	System	19
Mounting Holes	3	2.4G Wireless.....	23
Connectors.....	3	5G Wireless.....	33
Product Preset Information	4	Management	42
Mounting Accessories.....	4	Appendix	53
Hardware Installation	5	WDS Frequent Asked Questions	53
Mount on Wall or Ceiling.....	5	Federal Communication Commission Interference Statement.....	54
Mount on T-Bar	5	Europe – EU Declaration of Conformity.....	55
Wireless Performance Considerations.....	6	RoHS	55
Operation Modes	6	Limited Warranty	57
Access Point	6		
Client Bridge	7		
Repeater	7		
Wireless Distribution System.....	8		
System configuration	9		
System Management and Default Settings.....	9		
Log-in System Management for the First Time.....	9		

Product Overview



TEW-753DAP

Package Contents

TEW-753DAP package includes:

- TEW-753DAP
- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1.5 m/5 ft.)
- Power adapter (12 V DC, 1.25 A)
- Installation screws

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Features

TRENDnet's N600 Dual Band PoE Access Point, model TEW-753DAP, is a feature rich business class access point with proven concurrent 300 Mbps dual band wireless technology. A variety of installation scenarios are supported with Access Point, WDS AP, WDS Bridge, and Repeater modes. Save installation time and costs with PoE.

Quick Setup

Get up and running in minutes with the intuitive guided setup

Low Profile

Off white low profile smoke detector shape blends into most environments

Power over Ethernet (PoE)

Save installation time and costs with a PoE (Optional power port for non-PoE installations)

LED Control

Disable diagnostic LEDs to further reduce visual attention

Concurrent Dual Band

Proven concurrent 300 Mbps* dual band wireless n

Gigabit Port

Gigabit port maintains high performance connection to network

Wireless Coverage

Increased coverage with MIMO technology

Backward Compatible

Compatible older wireless g devices

Operation Modes

Independently set each band to Access Point, WDS AP, WDS Bridge, WDS Station, Client Bridge or Repeater mode

IPv6

IPv6 support

AP Scan

Integrated wireless scan function helps optimize wireless setup

SSIDs

Up to 8 SSIDs per band (16 total) with isolation support

Traffic Shaping

Allocate bandwidth to each wireless SSID

System Logs

Eight system log filters aid network troubleshooting

Spanning Tree

Configurable spanning tree controls

SNMP

Extend network monitoring to this device with SNMP support

Encrypted Wireless

Support for encryption up to WPA2

VLAN Management

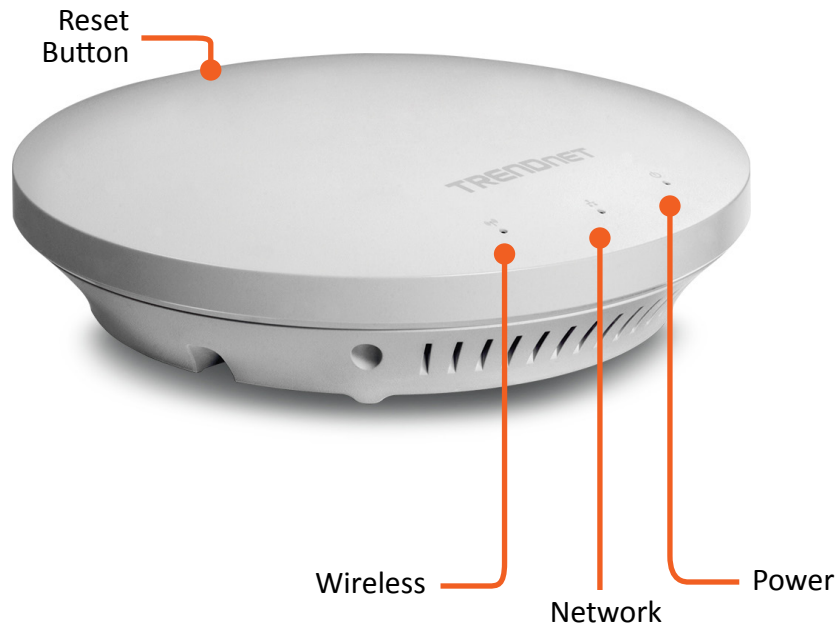
Up to eight SSIDs per band with VLAN management support

Network Access

Create MAC filter tables to reduce network access risk

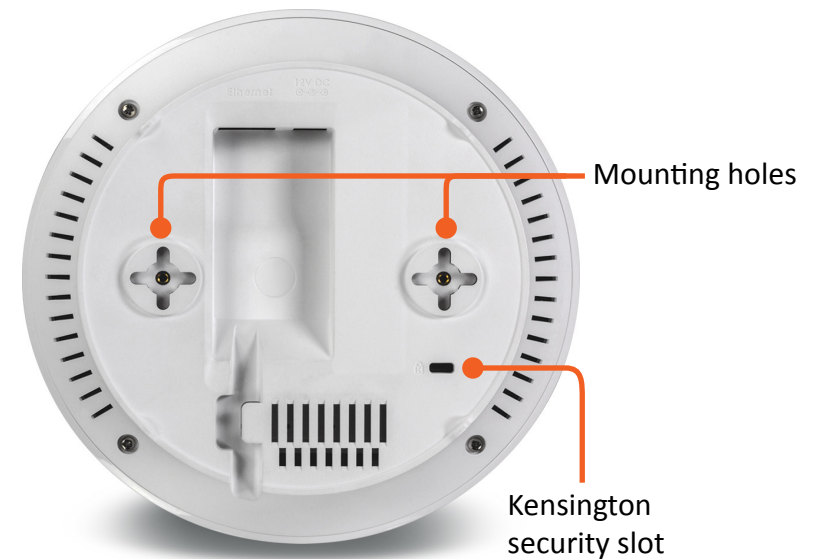
*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Front Panel

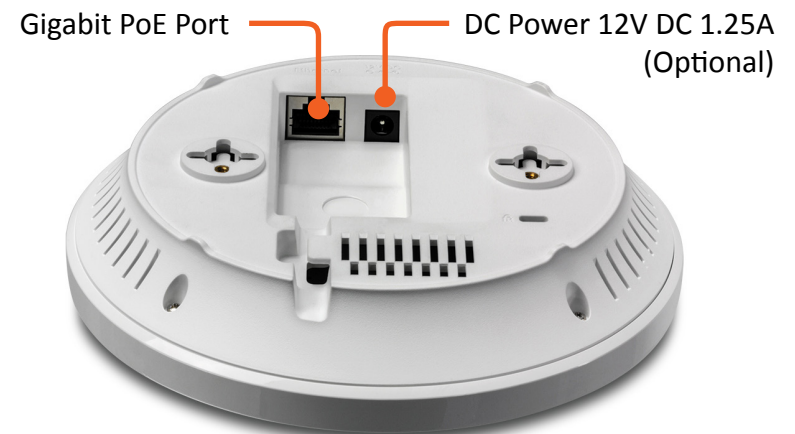


Reset Button	<ul style="list-style-type: none"> • Push and hold for 2 seconds to reset TEW-753DAP • Push and hold for more than 10 seconds to reset configuration to factory default 	
Power LED	OFF	Powered off or LED display is disabled
	ON	Powered on
Network LED Orange: 10/100 Green: Giga bit	OFF	No network connected through Ethernet port (PoE) or LED display has been disabled
	ON	Network connected through Ethernet port (PoE)
	Flashing	Network activities are detected on Ethernet (PoE) port
Wireless LED Orange: 2.4GHz Green: 5GHz	OFF	No wireless network connection or LED display is disabled
	Flashing	Wireless network activities are detected

Mounting Holes

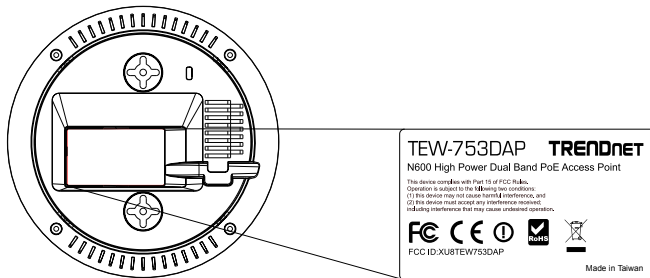


Connectors



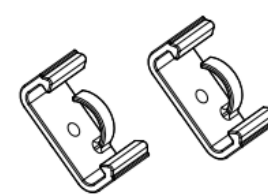
Product Preset Information

There are two preset product labels comes with the package. The first label is located on plastic wrapping of TEW-753DAP. The second label is located on the bottom of the TEW-753DAP. You can find default SSID, wireless key, administrator account, and administrator password there. The default static management IP is 192.168.10.100.

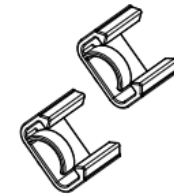


Mounting Accessories

The mounting accessories are provided for easier hardware installation, including two sets of T-Bar clippers, two sets of screws, and a set of spacers.



15/16" T-Bar Clips



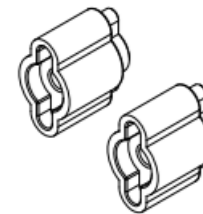
9/16" T-Bar Clips



P2.6 * 10 Screws



P2.6 * 25 Screws

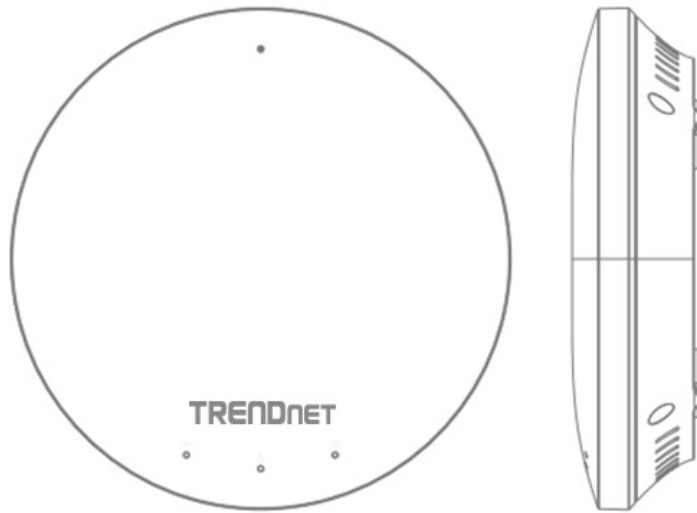


Spacers

Hardware Installation

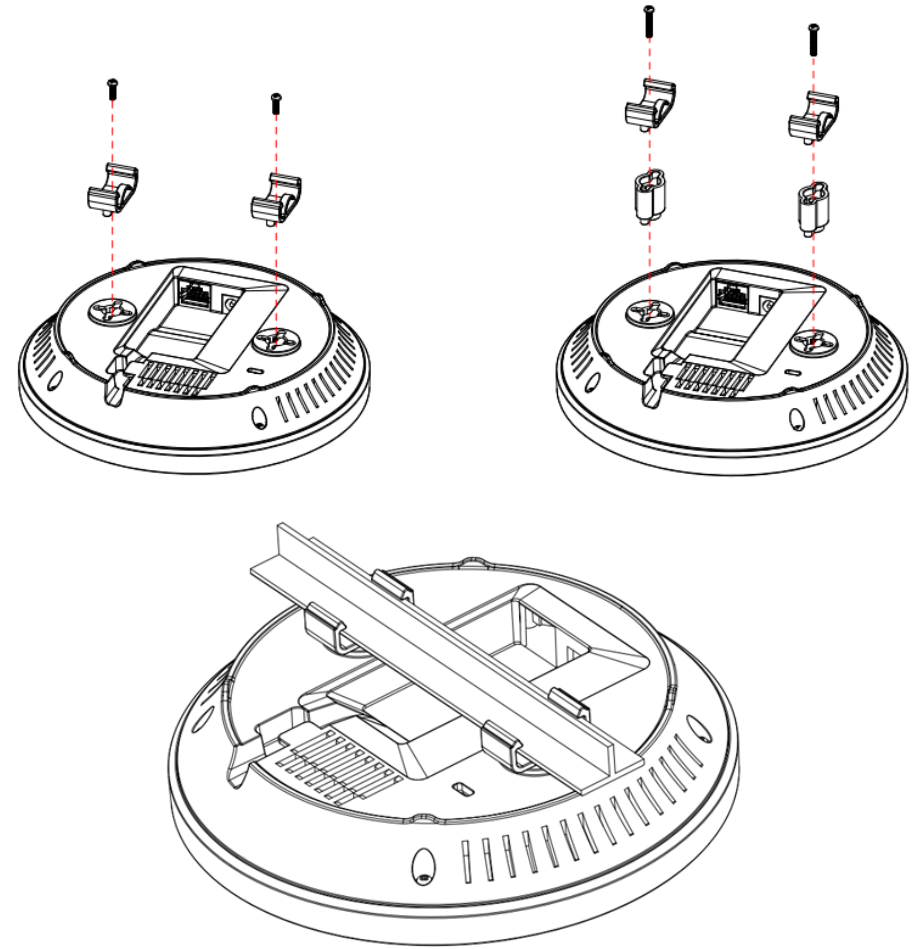
Mount on Wall or Ceiling

Use two P3.5 pan head screws to hold the TEW-753DAP. The distance between mounting points is 2 3/4" (7cm)



Mount on T-Bar

Two additional bronze screw holes are provided for T-Bar mounting. Use two P2.6 screws to secure the TEW-753DAP on T-Bar clip and then clip on the T-Bar.



Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.

Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.

Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.

Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices.

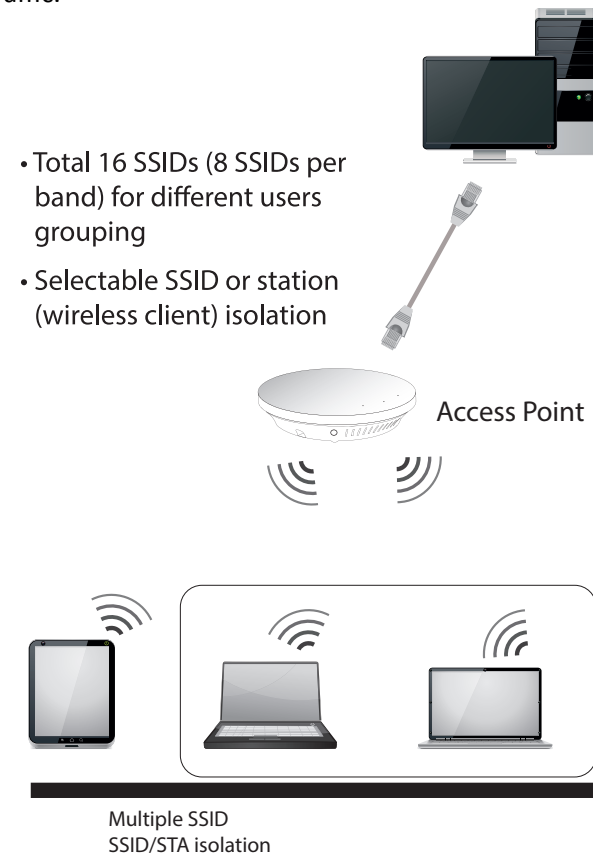
Adjust the wireless power setting on your AP if you have more than one AP covering a large area. Covering only the neighbor hop APs in wireless range is a good design. Covering more than neighbor APs will experience wireless interference and slow down the communication.

Operation Modes

There are four operating modes provided by TEW-753DAP, Access Point, Client Bridge, WDS and Repeater. Configure the TEW-753DAP to different operation mode which service the best in your network.

Access Point

This is the default operation mode. TEW-753DAP service wireless end points in this mode. You can setup local or remote wireless authentication, setup up to 8 sets of SSIDs in 2.4GHz band and 5GHz band, total 16 SSIDs and separate SSID or STA traffic.



Client Bridge

When Client Bridge mode is set to 2.4GHz or 5GHz interface of TEW753DAP, this interface functions as a wireless client connecting to any AP dynamically (channels and encryptions). The interface bridges the traffic to the Ethernet and the other wireless interface.



Repeater

When Repeater Mode is selected, the selected wireless interface functions as a wireless repeater and is able to repeat the wireless signal of an access point. This feature is used to expand your existing wireless network on places your current access point is unable to reach. Make sure all the settings on selected interface of the TEW-753DAP matches the wireless access points you want to repeat in same wireless settings including SSID, channel and wireless encryption settings.



Wireless Distribution System

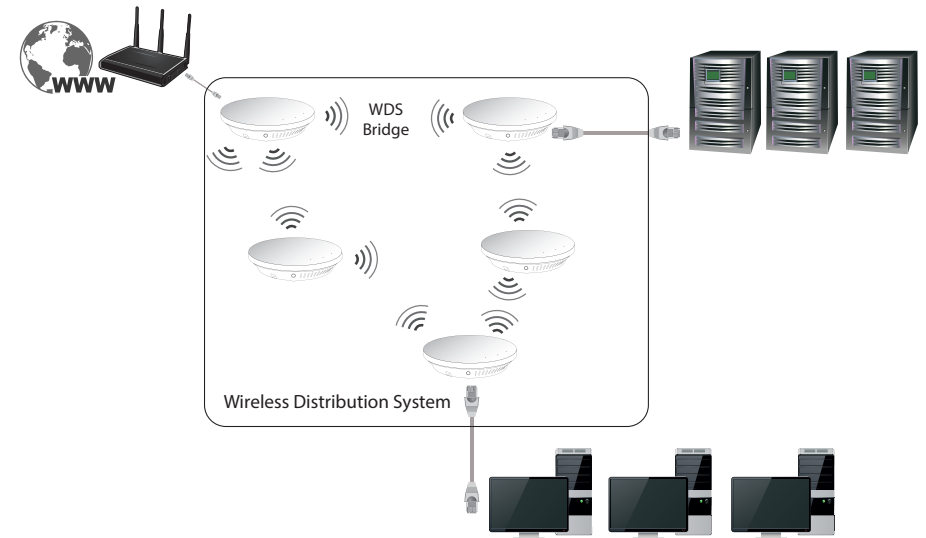


Deploy ONLY multiple TEW-753DAPs in a single DS (distribution system). WDS may not work with other products due to its non-standard nature.

WDS mode is a non-standard extension to the IEEE 802.11 standard to allow transparent Ethernet bridging on the station and to implement seamless hand-over for wireless clients roaming between different access points. Transparent bridge is also one of the requirements to some layer 2 services such as DHCP and 802.1X authentication. Because the WDS implementation differs from product to product, not all WDS-enabled products are interoperable. You have to use multiple TEW-753DAP to build your mesh wireless DS or transparent bridge.

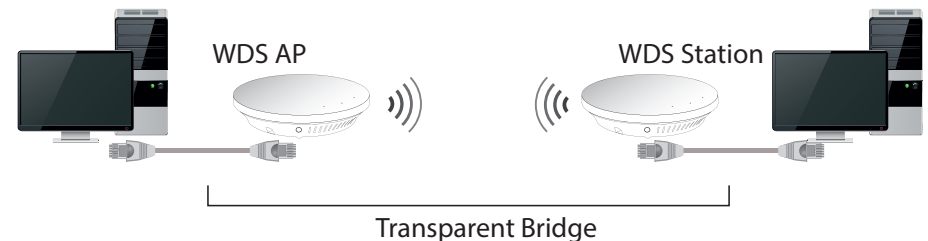
You can setup TEW-753DAP on different WDS modes for your different network planning.

WDS Bridge: In this mode, the selected interface wirelessly communicates to other WDS bridges to make a wireless backbone. You can make a simple mesh network with these WDS bridges. To build a WDS link, you have to list the neighbor's BSSID (the MAC address) as the next hop packet forwarding. Your neighbor, vice versa, has to list your BSSID (the MAC address) as its next hop. Make sure all access points are configured with the same SSID as a single DS (distribution system), wireless channel and wireless encryption settings have to be the same as well.



WDS Access Point: WDS AP is an outlet of a DS. Pairing with a WDS Station you can build a transparent bridge between two DS or from DS to STA. (See more information in "Appendix" on page 53)

WDS Station: Pair with WDS AP, you can build a transparent bridge for layer 2 requirements. (See more information in "Appendix" on page 53)



System configuration

System Management and Default Settings

If you have a brand new out of box TEW-753DAP or if you just reset TEW-753DAP to factory defaults by pressing and holding reset button for over 10 seconds, your TEW-753DAP has following settings:

Management IP : 192.168.10.100

Administrator name : admin

Administrator password : admin

Default SSID : (printed on pre-set label)

Default SSID passphrase : (printed on pre-set label)

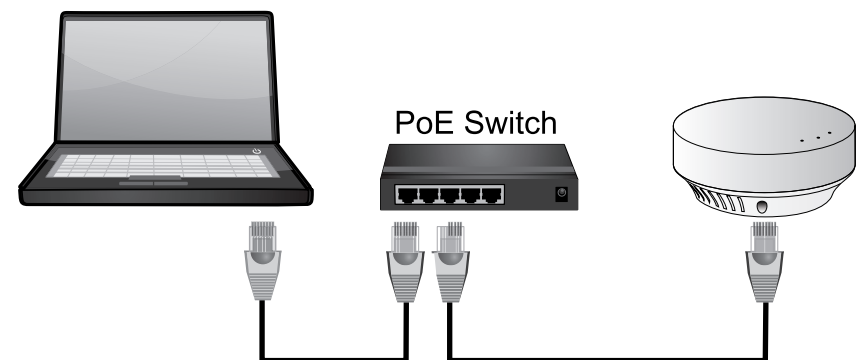
Log-in System Management for the First Time

- 1** Power on your TEW-753DAP by connecting PoE cable to a PoE switch or plug-in the power adapter comes with the package. The power LED will turned on.

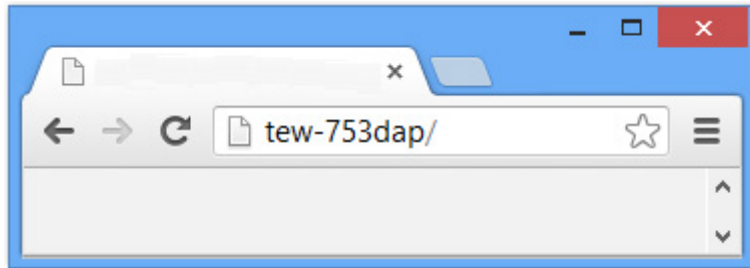
- 2** Search for available wireless connections in your computer's network settings. The default SSID of the TEW-735AP is shown on the preset label. The default wireless security settings are set to WPA2 and the passphrase is printed on the preset label and device label.



Or,
Connect a network cable from your computer to the TEW-753DAP network port.



- 3 Open a web browser and type **http://tew-753DAP** to access web administration page.



If you have a static IP set on your PC, please open a web browser and enter **http://192.168.10.100** The TEW-735AP login page will appear.

 A screenshot of the TEW-753DAP login page. The page title is 'TRENDNET N600 High Power Dual Band PoE Access Point TEW-753DAP'. The main content area is titled 'TEW-753DAP LOGIN' and contains a form with the following fields:

- Username: [text input field]
- Password: [text input field]
- Language: [dropdown menu with 'English' selected]

 A blue 'Login' button is located below the form.

Enter administrator login information (The default user name is **admin** and password is **admin**)

* Please reference the troubleshooting section if you cannot access administration web page.

- 4 Change your administration login password away from factory default setting. Click **Next** to continue.

 A screenshot of the 'Login Setting' page in the web administration interface. The page has a sidebar on the left with menu items: 'Save/Reload:0', 'Status', 'System', '2.4G Wireless', '5G Wireless', and 'Management'. The main content area is titled 'Login Setting' and contains the following fields:

- New Name: [text input field with 'admin' entered]
- Old Password: [text input field]
- New Password: [text input field]
- Confirm Password: [text input field]

 A blue 'Next' button is located at the bottom right of the form.

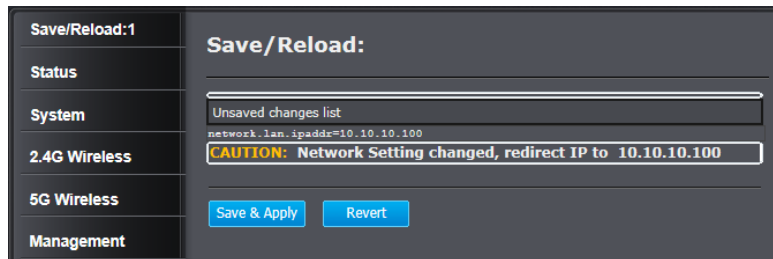
- 5 Change the management IP address for the TEW-753DAP if necessary. Click **Apply**.

 A screenshot of the 'IP Settings' page in the web administration interface. The page has a sidebar on the left with menu items: 'Save/Reload:0', 'Status', 'System', '2.4G Wireless', '5G Wireless', and 'Management'. The main content area is titled 'IP Settings' and contains the following sections:

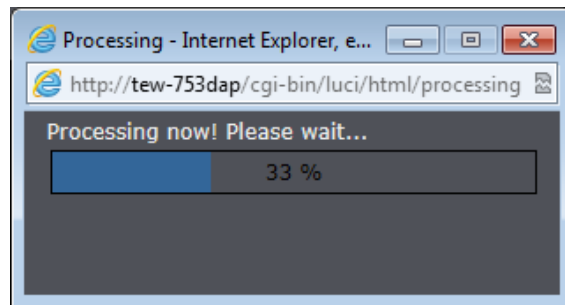
- System Information**
 - IP Network Setting: Obtain an IP address automatically (DHCP) Specify an IP address
 - IP Address: [text input field with '192', '168', '10', '100' entered]
 - IP Subnet Mask: [text input field with '255', '255', '255', '0' entered]
 - Default Gateway: [text input field with '0', '0', '0', '0' entered]
 - Primary DNS: [text input field with '0', '0', '0', '0' entered]
 - Secondary DNS: [text input field with '0', '0', '0', '0' entered]
 - Use Link-Local Address:
 - IPv6 IP Address: [text input field]
 - IPv6 Subnet Prefix Length: [text input field]
 - IPv6 Default Gateway: [text input field]
 - IPv6 Primary DNS: [text input field]
 - IPv6 Secondary DNS: [text input field]

 A blue 'Apply' button is located at the bottom of the form.

6 Click **Save/ Reload** on top of the menu and then click **Save & Apply**.



7 TEW-753DAP will apply password change and then reboot. Login again with your new password.



* Make sure you are still connecting to TEW-753DAP after reboot if you wireless connects to TEW-753DAP.

Setup Wizard

Setup wizard is provided as part of the web configuration utility. It sets up the basic administrator password and management IP address by clicking on the **Wizard** button on the function menu. The following screen will appear.

- 1 Enter your new administrator password and then click **Next** to continue.

The screenshot shows the 'Login Setting' screen. On the left, a sidebar contains the following menu items: 'Save/Reload:0', 'Status', 'System' (selected), 'Wizard' (highlighted), 'Operation Mode', 'IP Settings', and 'Spanning Tree Settings'. The main content area is titled 'Login Setting' and contains a table with the following fields:

New Name	admin
Old Password	
New Password	
Confirm Password	

A blue 'Next' button is located at the bottom right of the form.

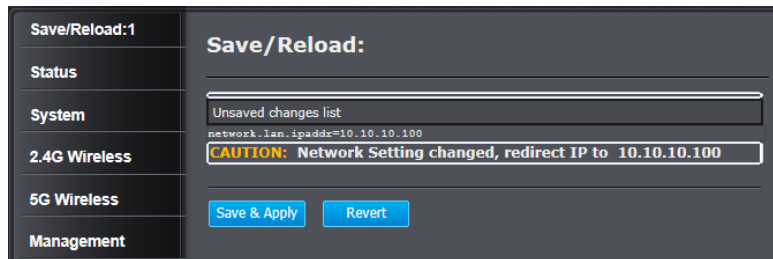
- 2 Enter the management IP address for this TEW-753DAP. The default IP address is 192.168.10.100. Set it up in your network management subnet with a unique IP address. You can leave it set on default IP if you have only one TEW-753DAP on network. Click **Apply**.

The screenshot shows the 'IP Settings' screen. On the left, a sidebar contains the following menu items: 'Save/Reload:0', 'Status', 'System', '2.4G Wireless', '5G Wireless', and 'Management' (selected). The main content area is titled 'IP Settings' and contains a 'System Information' section with the following fields:

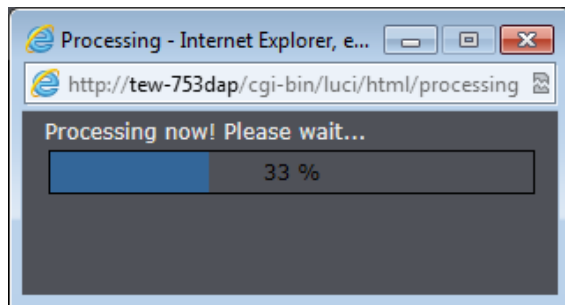
IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input type="radio"/> Specify an IP address
IP Address	192 . 168 . 10 . 100
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0
Use Link-Local Address	<input checked="" type="checkbox"/>
IPv6 IP Address	
IPv6 Subnet Prefix Length	
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	

A blue 'Apply' button is located at the bottom right of the form.

- 3 Click **Save/ Reload** on top of the menu and then click **Save & Apply**.



- 4 TEW-753DAP will apply password change and then reboot. Login again with your new password.



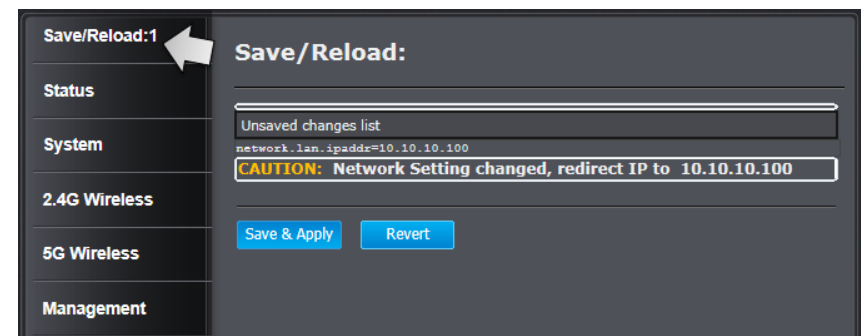
- * Make sure you are still connecting to TEW-753DAP after reboot if you wireless connects to TEW-753DAP.

Save/ Reload

The TEW-753DAP is a commercial grade wireless access point. To make multiple network settings change at the same time and minimum the interruption of production network, all network configurations have to be changed in two stages.

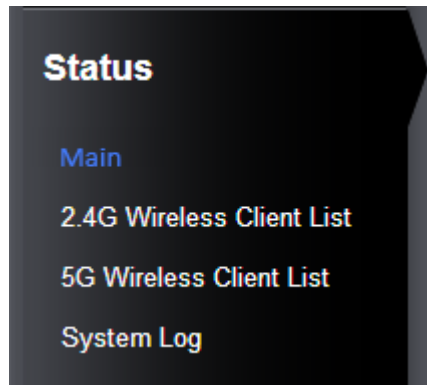
When you change a network setting, the change command will be saved in a queue. When you finish all the setting changes, click **Save/ Reload** on top of the listed menu. Review the list of commands on your change list. Click **Save & Apply** to apply the changes. If you want to cancel the changes, click **Revert**.

The number that follows **Save/ Reload** is a reminder that shows how many changes are in the queue waiting to be applied.



Status

Main status page shows TEW-753DAP's basic information. Click **Status** then click **Main** to show the page.



System Information

Device Name :	Name of this device that is recognized by other network devices such as SNMP.
Ethernet MAC Address :	The MAC address of Ethernet Interface
2.4G Wireless MAC Address :	The MAC address of each individual active SSID.
5G Wireless MAC Address :	The MAC address of each individual active SSID.
Country :	The country in which you are located.
Current Time :	The current is important for schedule control and log accuracy.
Firmware version :	Currently run firmware version
Management VLAN ID :	The VLAN ID assigned to device management network. The default setting is untagged.

Main

System Information

Device Name	TEW-753DAP	
Ethernet MAC Address	D8:EB:97:E8:F7:D6	
2.4G Wireless MAC Address (SSID/MAC)	1	D8:EB:97:E8:F7:D6
	2	N/A
	3	N/A
	4	N/A
	5	N/A
	6	N/A
	7	N/A
	8	N/A
5G Wireless MAC Address (SSID/MAC)	1	D8:EB:97:E8:F7:D7
	2	N/A
	3	N/A
	4	N/A
	5	N/A
	6	N/A
	7	N/A
	8	N/A
Country	United States	
Current Time	Mon Aug 19 12:26:21 UTC 2013	
Firmware Version	2.0.0	
Management VLAN ID	Untagged	

LAN Settings	
IP Address	10.10.10.100
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled
Spanning Tree Protocol	Disabled
IPv6 IP Address	None
IPv6 Link-Local Address	FE80::202:6FFF:FEE8:F7D6
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	427.726 KB (2395 PKts.)
TX(Packets)	1.27593 MB (1522 PKts.)

LAN Settings	
IP Address :	IP address of the TEW-753DAP
Subnet Mask :	Network range of IP address
Default Gateway :	The default route going further from TEW-753DAP subnet.
Primary DNS :	Primary DNS server address
Secondary DNS :	Secondary DNS server address
DHCP Client :	DHCP client status. The IP address was statically set by default.
Spanning Tree Protocol :	Spanning Tree Protocol is enabled or not.
IPv6 IP Address :	The dual-stack IPv6 address of the TEW753DAP.
IPv6 Link-Local Address	IPv6 link local address for auto-configuration
IPv6 Default Gateway	IPv6 default route going further from TEW-753DAP subnet.
IPv6 Primary DNS	Primary IPv6 DNS server address
IPv6 Secondary DNS	Secondary IPv6 DNS server address
RX (packets)	Received packets from Ethernet interface
TX (packets)	Transmitted packets from Ethernet interface

Current Wireless Settings :2.4G	
Operation Mode	Access Point
Wireless Mode	802.11 B/G/N Mixed
Channel Bandwidth	20-40 MHz
Frequency/Channel	2.437 GHz (Channel 6)
Profile Settings (SSID/Security/VID/802.1Q)	1 TRENDnet753_2.4GHz_APS2/WPA2-
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Distance	1 Km
RX(Packets)	0 B (0 PKts.)
TX(Packets)	435.946 KB (1637 PKts.)

Current Wireless Settings :5G	
Operation Mode	Access Point
Wireless Mode	802.11 A/N Mixed
Channel Bandwidth	20-40 MHz
Frequency/Channel	5.785 GHz (Channel 157)
Profile Settings (SSID/Security/VID/802.1Q)	1 TRENDnet753_5GHz_APS2/WPA2-PS
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Distance	1 Km
RX(Packets)	0 B (0 PKts.)
TX(Packets)	308.344 KB (1104 PKts.)
Refresh	

Current Wireless Settings: 2.4GHz

Operation Mode :	Shows which wireless mode the 2.4GHz interface is set to.
Wireless Mode :	Shows which 802.11 wireless mode is set and running on the 2.4GHz interface.
Channel Bandwidth :	Wireless Channel Bandwidth (20 or 40 MHz)
Frequency/ Channel :	Shows which 2.4GHz wireless channel (and frequency) is in use.
Profile Settings :	Briefly shows wireless settings (SSID/ Security/ VID/ 802.1Q) on each SSID.
Distance :	The distance setting for 2.4GHz wireless interface.
RX (packets)	Received packets by 2.4GHz wireless interface
TX (packets)	Transmitted packets from 2.4GHz wireless interface

Current Wireless Settings: 5GHz

Operation Mode :	Shows which wireless mode the 5GHz interface is set to.
Wireless Mode :	Shows which 802.11 wireless mode is set and running on the 5GHz interface.
Channel Bandwidth :	Wireless Channel Bandwidth (20 or 40 MHz)
Frequency/ Channel :	Shows which 5GHz wireless channel (and frequency) is in use.
Profile Settings :	Briefly shows wireless settings (SSID/ Security/ VID/ 802.1q) on each SSID.
Distance :	The distance setting for 5GHz wireless interface.

RX (packets)	Received packets by 5GHz wireless interface
TX (packets)	Transmitted packets from 5GHz wireless interface

Refresh : Click this button to refresh the list

2.4G Wireless Client List

This page shows all wireless clients connected to the 2.4GHz interface.

Save/Reload:0

2.4GHz / Client List

Status

- Main
- 2.4G Wireless Client List
- 5G Wireless Client List
- System Log

System

- 2.4G Wireless
- 5G Wireless
- Management

SSID: #	MAC Address	TX(Bytes)	RX(Bytes)	RSSI(dBm)	Kick and Ban
SSID1: #1	00:17:c4:00:17:c4	90Kb	358Kb	-38	Kick and Ban
SSID8: #1	00:23:6c:00:23:6c	904Kb	571Kb	-22	Kick and Ban

[Refresh](#)

SSID : #	Shows the SSID that clients are associated with and their client number.
MAC Address :	MAC address of wireless client
TX (Bytes) :	Transmitting data statistics
RX (Bytes) :	Receiving data statistics
RSSI (dBm) :	Received Signal Strength Indication: Signal strength of this wireless client
Kick and Ban :	Click this button to send this client to MAC address filter list. Click OK when you see this prompt. (Save/Reload is required to apply change.)

MAC filter deny mode will be enabled. This MAC 00:23:6c:90:23:66 will be added to the deny list.

[OK](#) [Cancel](#)

Refresh : Click this button to refresh the list

5G Wireless Client List

This page shows all wireless clients connected to the 2.4GHz interface.



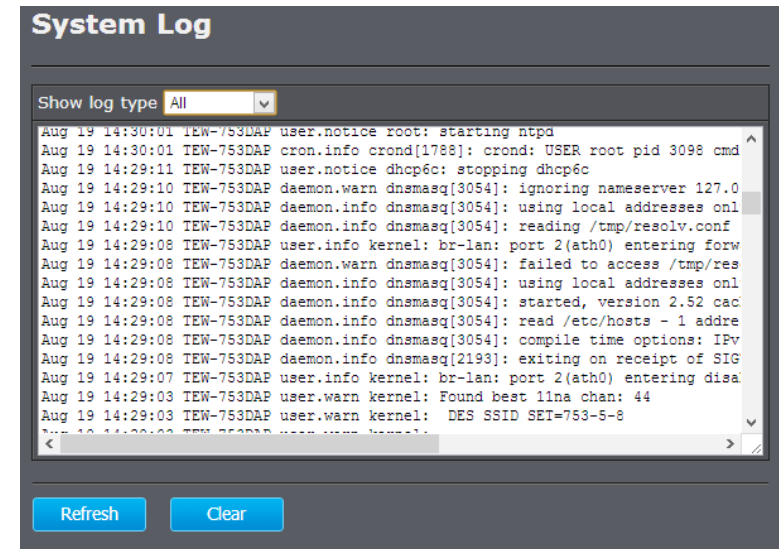
SSID : #	Shows the SSID that clients are associated with and their client number.
MAC Address :	MAC address of wireless client
TX (Bytes) :	Transmitting data statistics
RX (Bytes) :	Receiving data statistics
RSSI(dBm) :	Received Signal Strength Indication: Signal strength of this wireless client
Kick and Ban :	Click this button to send this client to MAC address filter list. Click OK when you see this prompt. (Save/Reload is required to apply change.)

MAC filter deny mode will be enabled. This MAC 00:23:6c:90:23:66 will be added to the deny list.

Refresh : Click this button to refresh the list

System Log

This page allows users to view a running log of the access point's system statistics, events and activities.



- All
- Debug
- Information
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

Choose a filter to quickly find the desired log.

Refresh : Click this button to refresh the log

Clear : Click this button to clear the log

System

Operation Mode

Choose the mode that best suits your network: Access Point, Client Bridge, WDS, and Repeater. Either one of the wireless interfaces can be used in bridge mode (Client Bridge, WDS Bridge, WDS Station, or Repeater), but not both. Select the country in which you are located and then select the operation mode for 2.4GHz and 5GHz wireless configurations. Click Apply to save the change. (**Save/Reload** is required for this change take effect.)

System Properties	
System Properties	
Device Name	"TEW-753DAP"
Operation Mode	2.4G Wireless Configuration
	<input type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> WDS <input type="radio"/> Repeater
	5G Wireless Configuration
	<input type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> WDS <input type="radio"/> Access Point <input type="radio"/> Bridge <input type="radio"/> Station <input type="radio"/> Repeater
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Access Point

This is the default operation mode for both the 2.4GHz and 5GHz wireless interfaces. Wireless clients, known as wireless stations (STAs), can wirelessly associate with these interfaces and connect to the Internet via the Ethernet port.

Client Bridge

The wireless interface works like a wireless station (STA), just like the wireless interface on a regular computer. The interface can connect to an AP dynamically (channels and encryption). The assigned wireless interface bridges the traffic to the Ethernet and the other TEW-753DAP wireless interface.

Repeater

In this mode, the wireless interface repeats wireless signal and packets for backbone communication as well as a client access. This feature is used to expand your existing wireless network to areas that your current access point is unable to reach. Make sure all of the settings of the wireless interface matches to your root or connecting wireless access points, same SSID, channel and wireless encryption settings.

WDS (Wireless Distribution System)

Wireless Distribution System, WDS, creates a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple access points without the need for a wired backbone. TEW-753DAP WDS operation has three sub modes: WDS Access Point, WDS Bridge, or WDS Station

WDS Access Point

The wireless interface connects to other WDS bridge enable devices for backbone communication and provides wireless connection to clients (STAs) at the same time.

WDS Bridge

The wireless interface connects *ONLY* to other WDS bridge enabled devices and local networks (the other wireless interface and Ethernet interface) as a wireless backbone bridge.

WDS Station

The wireless interface connects to other WDS bridge enabled devices for backbone communication and connects to other wireless access points at the same time. Use this mode to pair with the next hop access point as a WDS network outlet.

* Only one bridge can be setup on 2.4GHz or 5GHz band, but not both.

IP Settings

The TEW-753DAP has a static IP (192.168.10.100) set for management purposes. You can change this IP address to fit your network plan or manage multiple TRENDnet access points. You can also set the TEW-753DAP to DHCP client to accept an IP dynamically.

IP Settings	
System Information	
IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input type="radio"/> Specify an IP address
IP Address	10 . 10 . 10 . 100
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0
Use Link-Local Address	<input checked="" type="checkbox"/>
IPv6 IP Address	<input type="text"/>
IPv6 Subnet Prefix Length	<input type="text"/>
IPv6 Default Gateway	<input type="text"/>
IPv6 Primary DNS	<input type="text"/>
IPv6 Secondary DNS	<input type="text"/>
<input type="button" value="Apply"/>	
<input type="button" value="Cancel"/>	

IP Network Setting :	Select "Obtain an IP address automatically (DHCP)" or "Specify an IP address". If you select specify an IP address, you have to enter the following information manually. If DHCP is selected, then the IP address is received automatically from the external DHCP server.
IP Address :	Specify an IP address
IP Subnet Mask :	Specify a subnet mask for the IP address
Default Gateway :	Default route for the TEW-753DAP
Primary DNS :	Primary DNS server address
Secondary DNS :	Secondary DNS server address
Use Link Local Address :	Check this to use link local address
IPv6 IP Address :	Specify an IPv6 dual-stack address
IPv6 Subnet Prefix Length :	Specify a subnet range for the IPv6 address
IPv6 Default Gateway :	Default route for IPv6
IPv6 Primary DNS :	Primary IPv6 DNS server address
IPv6 Secondary DNS :	Secondary IPv6 DNS server address

Spanning Tree

The TEW-753DAP is designed for end point access as well as backbone connection. To avoid network looping, you can enable 802.1d spanning tree protocol.

Spanning Tree Settings

Spanning Tree Status	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Bridge Hello Time	2 <input type="text"/> seconds (1-10)
Bridge Max Age	20 <input type="text"/> seconds (6-40)
Bridge Forward Delay	4 <input type="text"/> seconds (4-30)
Priority	32768 <input type="text"/> (0-65535)

Spanning Tree Status:	Enable or disable 802.1d spanning tree protocol to avoid network looping
Bridge Hello Time :	The time between each bridge protocol data unit (BPDU). Default: 2 sec.
Bridge Max Age :	Maximum time a BPDU kept in bridge. Default: 20 sec.
Bridge Forward Delay :	The time to be spent in listen and learning state. Default: 4 sec.
Priority :	Priority number for root bridge selection. (MAC number is listed on Status > Main page)

Apply : Click this button to apply the change

Cancel : Click this button to cancel the change

Band Steer

In the office, the 2.4GHz is always crowded than 5GHz. There are fewer non-overlapping channels and more legacy devices in 2.4GHz compare to the 5GHz band. The TEW-753DAP is equipped with 2.4GHz and 5GHz wireless interfaces. When your client device can work on both 2.4GHz and 5GHz wireless, Band Steer will choose 5GHz as primary band over 2.4GHz. Traffic will mainly stays on 5GHz in stead of 2.4GHz. To setup band steer, you have to setup the same SSIDs on both the 2.4GHz and the 5GHz interfaces. Then check **Enable** on this page. Then click **Save**.

Band Steer

Band steering alleviates network congestion by directing traffic from the 2.4 GHz band to the 5GHz band.

NOTE:
To enable band steering, you have to setup steering SSID the same in both 2.4GHz and 5GHz.

Band Steering

Enable

Save : Click this button to save the change.
(**Save/Apply is** required to apply changes.)

Cancel : Click this button to cancel the change

2.4G Wireless

Wireless Network

General setups options for your 2.4GHz wireless connection. You can setup up to eight SSIDs for different groups of users.

2.4GHz / Wireless Network

Wireless Mode	802.11 B/G/N Mixed			
Channel HT Mode	20/40MHz			
Extension Channel	Upper Channel			
Channel / Frequency	Ch1-2.412GHz	<input checked="" type="checkbox"/> Auto		
AP Detection	Scan			

Current Profiles				
SSID	Security	VID	Enable	Edit
TRENDnet753_2.4GHz_5RL2	WPA2-PSK AES	1	<input checked="" type="checkbox"/>	Edit
	None	2	<input type="checkbox"/>	Edit
	None	3	<input type="checkbox"/>	Edit
	None	4	<input type="checkbox"/>	Edit
	None	5	<input type="checkbox"/>	Edit
	None	6	<input type="checkbox"/>	Edit
	None	7	<input type="checkbox"/>	Edit
	None	8	<input type="checkbox"/>	Edit

Apply
Cancel

Network Mode : 802.11 B/G/N Mixed 802.11 B/G/N Mixed 802.11 B 802.11 B/G Mixed 802.11 G 802.11 N only	Choose between N only, G only, B only, B/G mixed, or B/G/N mixed mode. The rule of the thumb is to choose single mode if your devices all work in the same mode. Mixed mode increases compatibility, but sometimes lowers the data speed.
Channel HT Mode : 20/40MHz 40MHz 20/40MHz 20MHz	The latest 802.11 protocol can combine channels for better wireless performance. You can choose fixed 20MHz or 40MHz, or automatically select 20MHz or 40MHz channels.
Extension Channel : Upper Channel Lower Channel Upper Channel	When you choose manual channel selection and 20/40MHz or 40MHz in channel HT mode, you can choose which neighbor channel you want to combine, upper channel or lower channel.
Channel / Frequency : Ch1-2.412GHz Ch1-2.412GHz Ch2-2.417GHz Ch3-2.422GHz Ch4-2.427GHz Ch5-2.432GHz Ch6-2.437GHz Ch7-2.442GHz Ch8-2.447GHz Ch9-2.452GHz Ch10-2.457GHz Ch11-2.462GHz	If you want to setup fixed channel, choose a channel number to switch your radio frequency. Otherwise, check auto to select the channel automatically which is selected by default. (When you choose 20/40MHZ or 40MHz channel HT mode, the channel selection list is shorter. Four marginal channels are reserved for channel expansion.)

Current Profile

SSID (1 - 8) :	The wireless network name setup for this SSID.
Security :	Wireless security type setup for this SSID.
VID :	VLAN id for this SSID
Enable :	Check this box to enable this SSID
Edit :	Click Edit to change the settings for this SSID

(**Save/Apply** is required to apply changes.)

AP Detection

Before you setup your TEW-753DAP wireless settings, you may want to know what signal are currently broadcasting. Click Scan to do a site survey and list the running access points around you.

2.4GHz / Site Survey						
2.4GHz Site Survey Infrastructure <input checked="" type="checkbox"/> Ad_hoc <input type="checkbox"/>						
BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:14:D1:C5:7D:44	TrendnetSkyN	1	-77 dBm	11g/n	WPA2-PSK	
00:14:D1:BE:07:74	WalkingDead	1	-70 dBm	11g/n	WPA2-PSK	
00:14:D1:AA:1C:80	MII	1	-85 dBm	11g/n	WPA/WPA2-PSK	

[Go Back](#)

BSSID :	Basic SSID. This is strictly unique SSID to identify a wireless access point, WAP. It is also the MAC address of the wireless interface.
SSID :	Service Set Identifier. This SSID is human readable and performs as ESSID to setup wireless groups.
Channel :	2.4GHz wireless channel number
Signal Level :	The signal strength from the access point.
Type :	The 802.11 wireless mode this access point provides.
Security :	Which wireless security was set to use.
Mode:	This wireless source works on infrastructure mode or ad hoc mode.

Go Back : Click this button to go back

SSID Settings

Click **Edit** one the SSID you want to edit. The following setup window will appear.

Wireless Settings

SSID :	Select the human readable SSID to be easily identified. You can choose any combination with 1 to 32 letters .
Suppressed SSID :	Check this box to suppress SSID broadcasting. Your wireless network name is broadcast to anyone within wireless signal range. When this is box is checked, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
Station Separation :	If you enable station separation, wireless clients (a.k.a. STAs) associated with this SSID cannot communicate to each other directly even if they are in the same wireless group.

Wireless Security

Security Mode :	(SSID 1 Only) Choose between Disabled, WEP, WPA-PSK, WPA2-PSK or WPA-PSK Mixed for your wireless security.
Security Mode :	(SSID 2-8) Choose between Disabled, WPA-PSK, WPA2-PSK or WPA-PSK mixed, WPA, WPA2 or WPA Mixed for your wireless security.

WEP (Wired Equivalent Privacy)

This is a minimum and legacy type of wireless security. Only SSID 1 can be set with WEP wireless security mode.

Wireless Security	
Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	<input type="text"/>
Key2	<input type="text"/>
Key3	<input type="text"/>
Key4	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Key Type :	Select your key format to be in hexadecimal or ASCII codes. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.
Key Length :	Select a 64-bit, 128-bit, or 152-bit WEP key length from the drop-down list
Default Key :	You may choose one of your four different WEP keys from below
Key 1-4 :	You can enter four different WEP keys

Auth Type :	Select Open System or Shared Key.
Open System	Open System allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption.
Shared Key	Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

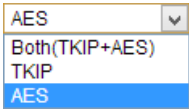
Save: Click this button to save the changes

Cancel: Click this button to cancel the change

WPA-PSK, WPA2-PSK, Mixed WPA-PSK

This group of wireless security settings use the preshared key, PSK, stored on you TEW-753DAP to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed

Wireless Security	
Security Mode	WPA-PSK Mixed ▾
Encryption	Both(TKIP+AES) ▾
Passphrase (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Encryption : 	Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
Passphrase :	The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or hexadecimal numbers at both ends of the wireless connections. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client
Group Key Update Interval :	Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead.(Default: 3600 seconds/ 1 hour)

WPA, WPA2, Mixed WPA

This group of wireless security settings uses remote key services, RADIUS, to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed

Wireless Security	
Security Mode	WPA Mixed
Encryption	Both(TKIP+AES)
Radius Server	. . .
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Disable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

WPA Type :	Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
RADIUS Server :	IP address of RADIUS server
RADIUS Port :	RADIUS service port number. Default: 1812
RADIUS Secret:	RADIUS service shared secret to authenticate this credential agent.
Group Key Update Interval :	Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead. (default: 3600 seconds/ 1 hour)
Radius Accounting :	Enable or disable RADIUS accounting service

Apply : Click this button to apply the changes

Cancel : Click this button to cancel the change

MAC Filter

Set up a list of clients and policies that allow only the clients on the list to associate with this AP or to reject clients on the list from associating with this AP. Set up the list with MAC addresses. A MAC address is a unique ID assigned by the manufacturer of the network adapter. Enter a MAC address and click **Add** to add it to the list. Click **Delete** to remove an entry. Select your **ACL Mode** and then click **Apply**. (You can also go to the wireless client list and click **Kick and Ban** to add a client to the list.)

2.4GHz / Wireless MAC Filter

CAUTION: When WPS is enabled, Wireless MAC Filter cannot be applied to the first SSID.

ACL Mode **Deny MAC in the List**

_____ : _____ : _____ : _____ : _____ : _____ **Add**

#	MAC Address	
1	12:34:56:78:90:12	Delete

Apply

ACL (Access Control List) Mode : Choose “Disabled” to disable the MAC filter.

Disabled

Disabled

Deny MAC in the List

Allow MAC in the List

Choose “Deny MAC in the List” to allow clients that aren’t on the list to associate with the TEW-753DAP’s 2.4GHz wireless interface.

Choose “Allow MAC in the List” to deny clients that aren’t on the list to associate with the TEW-753DAP’s 2.4GHz wireless interface.

2.4GHz / Client List

SSID:#	MAC Address	TX(Bytes)	RX(Bytes)	RSSI(dBm)	Kick and Ban
SSID1:#1	00:17:c4:00:17:c4	90kb	358kb	-38	Kick and Ban
SSID8:#1	00:23:6c:00:23:6c	904kb	571kb	-22	Kick and Ban

Refresh

Click **Kick and Ban** in the wireless client list to add a MAC entry to the MAC filter list.

Wireless Advanced Settings

Fine tune your wireless settings on this page.

2.4GHz / Wireless Advanced Settings

Data Rate:

Transmit Power:

RTS/CTS Threshold (1 - 2346): bytes

Distance (1-30km): km

Aggregation: Enable Disable
 Frames Bytes(Max)

WMM Parameters

AC	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3.008ms
AC_VO	2	3	2	1.504ms

Client limit

Frequency	Enable	Max Client
2.4G	<input checked="" type="checkbox"/>	<input type="text" value="127"/>

<p>Data Rate :</p> <ul style="list-style-type: none"> MCS0 MCS1 MCS2 MCS3 MCS4 MCS5 MCS6 MCS7 MCS8 MCS9 MCS10 MCS11 MCS12 MCS13 MCS14 MCS15 Auto 	<p>Choose a fixed data rate for 802.11b and g mode and MCS number for 802.11n, or choose Auto for automatic rate adapting. The default setting is Auto.</p>
--	---

<p>Transmit Power :</p> <ul style="list-style-type: none"> 18 dBm 11 dBm 12 dBm 13 dBm 14 dBm 15 dBm 16 dBm 17 dBm 18 dBm 	<p>Wireless signal transmission power. Setting transmission power to an appropriate value can make your multiple AP deployment easier. The default value is 18 dBm. Valid settings are between 11 and 18 (both FCC and CE).</p>
<p>RTS/CTS Threshold :</p>	<p>Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and to prevent hidden nodes from degrading the performance. Specify a value between 1 and 2346. The default value is 2346</p>
<p>Distance :</p>	<p>Set the distance between the TEW-753DAP and other access points or wireless clients. Low speed/ long range settings may be a priority for longer range connections. Valid settings are between 1 and 30. The default value is 1 Km.</p>
<p>Aggregation :</p>	<p>Combine short packets and send them together. Enabling packet aggregation will increase data throughput. However, it may cause jitters or delays in real-time communication.</p>

WMM Parameters				
AC	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3.008ms
AC_VO	2	3	2	1.504ms

WMM Parameters

AC :	Access Category: best effort (AC_BE), background (AC_BK), video (AC_VI), and voice (AC_VO)
CWmin :	Minimum contention window
CWmax :	Maximum contention window
AIFSN :	The Arbitration Inter-Frame Spacing Number specifies a wait time for data frames
TXOP Limit :	Transmission Opportunity Limit : The limit of the interval of time between the access point having the right to initiate transmissions and the transmission start time.

Client limit		
Frequency	Enable	Max Client
2.4G	<input checked="" type="checkbox"/>	127
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Client Limit

Frequency :	Limit the number of clients connected to the 2.4GHz interface
Enable :	Check this box to enable maximum client limitation
Max Client :	The maximum number of clients that can connect to the TEW-753DAP's 2.4GHz interface is 127. The valid numbers are from 1 to 127. The default value is 127.

WPS

WPS is one way to connect a wireless client to the TEW-753DAP. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both the wireless client and the TEW-753DAP, and WPS will do the rest for you.

Only the first SSID (SSID 1) supports WPS pairing. There are two types of WPS: WPS via Push Button and WPS via PIN code are supported. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start WPS pairing, and click the **Start to Process** button in this page under **WPS via Push Button** to start WPS pairing.

If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the access point.

WPS is disabled by default. To enable it, you have to click **Enable** and then Apply. Go **Save/Apply** to apply the changes. Then come back to this page to start your WPS session.

2.4GHz / WPS Setting

WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS current status	Configured <input type="button" value="Release Configuration"/>
Self Pin Code	35525646
SSID	TRENDnet753_2.4GHz_5RL2
Authentication Mode	WPA2-PSK AES
Passphrase Key	<input type="checkbox"/> *****
WPS Via Push Button	<input type="button" value="Start to Process"/>
WPS Via Pin	<input type="text"/> <input type="button" value="Start to Process"/>

WPS :	Enable the WPS feature
WPS Current Status :	Displays the current status of the WPS configuration. Press Release Configuration to release previous settings.
Self Pin Code :	Displays PIN code of TEW-753DAP
SSID :	Displays the SSID for WPS pairing. Only the first SSID (SSID 1) can proceed with WPS pairing.
Authentication Mode :	Displays the authentication mode of SSID 1
Passphrase Key :	Current passphrase. Click the check box to reveal the passphrase.
WPS Via Push Button :	Click on the Start to Process button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click the OK button in the dialog box
WPS via PIN :	Specify a PIN, a unique number that can be used to add the router to an existing network or to create a new network. Then click the Start to Process button

5G Wireless

Wireless Network

General setups for your 5GHz wireless connection. You can setup up to eight SSIDs for different groups of users.

5GHz / Wireless Network

Wireless Mode	802.11 A/N Mixed			
Channel HT Mode	20/40MHz			
Extension Channel	Upper Channel			
Channel / Frequency	Ch36-5180GHz	<input checked="" type="checkbox"/> Auto		
AP Detection	Scan			

Current Profiles

SSID	Security	VID	Enable	Edit
TRENDnet753_5GHz_5RL2	WPA2-PSK AES	51	<input checked="" type="checkbox"/>	Edit
	None	52	<input type="checkbox"/>	Edit
	None	53	<input type="checkbox"/>	Edit
	None	54	<input type="checkbox"/>	Edit
	None	55	<input type="checkbox"/>	Edit
	None	56	<input type="checkbox"/>	Edit
	None	57	<input type="checkbox"/>	Edit
	None	58	<input type="checkbox"/>	Edit

Apply
Cancel

Network Mode : <div style="border: 1px solid #ccc; padding: 2px; margin: 2px;"> 802.11 A/N Mixed 802.11 A/N Mixed 802.11 A 802.11 N only </div>	Choose between N only, a only, or A/N mixed mode. The rule of the thumb is to choose single mode if your devices all work in the same mode. Mixed mode increases compatibility, but sometimes lowers the data speed.
Channel HT Mode : <div style="border: 1px solid #ccc; padding: 2px; margin: 2px;"> 20/40MHz 40MHz 20/40MHz 20MHz </div>	The latest 802.11 protocol can combine channel for better wireless performance. You can choose fixed 20MHz or 40MHz, or automatically select 20MHz or 40MHz channels.
Extension Channel :	Not applicable in 5GHz wireless
Channel / Frequency : <div style="border: 1px solid #ccc; padding: 2px; margin: 2px;"> Ch36-5180GHz Ch36-5180GHz Ch40-5200GHz Ch44-5220GHz Ch48-5240GHz Ch149-5745GHz Ch153-5765GHz Ch157-5785GHz Ch161-5805GHz </div>	If you want to setup fixed channel, choose a channel number to switch your radio frequency. Otherwise, check auto to select the channel automatically, which is selected by default.

Current Profile

SSID (9 - 16) :	The wireless network name setup for this SSID.
Security :	Wireless security type setup for this SSID.
VID :	VLAN id for this SSID
Enable :	Check this box to enable this SSID
Edit :	Click Edit to change the settings for this SSID

(Save/Apply is required to apply changes.)

AP Detection

Before you setup your TEW-753DAP wireless settings, you may want to know what signals are currently broadcasting. Click Scan to do a site survey and list the running access points around you.

5GHz / Site Survey

5GHz Site Survey :Infrastructure :Ad_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:14:D1:9B:B3:78	Wally World_5GHz	36	-58 dBm	11a/n	2-PSK	
00:14:D1:9C:70:34	692gr_5-it	48	-59 dBm	11a/n	2-PSK	
00:14:D1:A3:FA:F5	TRENDnet812ac9821	149	-66 dBm	11a/n	WPA2-	

[Go Back](#)

BSSID :	Basic SSID. This is a strictly unique SSID to identify a wireless access point, WAP. It is also the MAC address of the wireless interface.
SSID :	Service Set Identifier. This SSID is human readable and performs as ESSID to setup wireless groups.
Channel :	5GHz wireless channel number
Signal Level :	The signal strength from the access point.
Type :	The 802.11 wireless mode this access point provides.
Security :	Which wireless security was set to use.
Mode:	This wireless source works on infrastructure mode or ad hoc mode.

Go Back : Click this button to go back

SSID Settings

Click **Edit** for the SSID you want to edit. The following setup window will appear.

5GHz / SSID Profile

Wireless Setting

SSID: (1 to 32 characters)

Suppressed SSID:

Station Separation: Enable Disable

Wireless Security

Security Mode: ▼

Encryption: ▼

Passphrase: (8 to 63 characters) or (64 Hexadecimal characters)

Group Key Update Interval: seconds(30~3600, 0: disabled)

Wireless Security

<p>Security Mode :</p> <div style="border: 1px solid black; padding: 2px;"> <p style="margin: 0;">WPA2-PSK ▼</p> <p style="margin: 0;">Disabled</p> <p style="margin: 0;">WPA-PSK</p> <p style="margin: 0;">WPA2-PSK</p> <p style="margin: 0;">WPA-PSK Mixed</p> <p style="margin: 0;">WPA</p> <p style="margin: 0;">WPA2</p> <p style="margin: 0; background-color: #007bff; color: white;">WPA Mixed</p> </div>	<p>Choose between Disabled, WPA-PSK, WPA2-PSK or WPA-PSK mixed, WPA, WPA2 or WPA Mixed for your wireless security.</p>
--	--

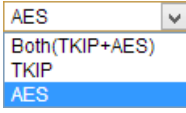
Wireless Settings

SSID :	Select the human readable SSID to be easily identified. You can choose any combination with 1 to 32 letters .
Suppressed SSID :	Check this box to suppress SSID broadcasting. Your wireless network name is broadcast to anyone within wireless signal range. When this is box is checked, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
Station Separation :	If you enable station separation, wireless clients (a.k.a. STAs) associated with this SSID cannot communicate to each other directly, even if they are in the same wireless group.

WPA-PSK, WPA2-PSK, Mixed WPA-PSK

This group of wireless security settings use the preshared key, PSK, stored on you TEW-753DAP to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed

Wireless Security	
Security Mode	WPA-PSK Mixed
Encryption	Both(TKIP+AES)
Passphrase (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Encryption : 	Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
Passphrase :	The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or hexadecimal numbers at both ends of the wireless connections. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client
Group Key Update Interval :	Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead.(default: 3600 seconds/ 1 hour)

WPA, WPA2, Mixed WPA

This group of wireless security use remote key services, RADIUS, to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed

Wireless Security	
Security Mode	WPA Mixed
Encryption	Both(TKIP+AES)
Radius Server	
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Disable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

WPA Type :	Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
RADIUS Server :	IP address of RADIUS server
RADIUS Port :	RADIUS service port number. Default: 1812
RADIUS Secret:	RADIUS service shared secret to authenticate this credential agent.
Group Key Update Interval :	Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead. (default: 3600 seconds/ 1 hour)
Radius Accounting :	Enable or disable RADIUS accounting service

Apply : Click this button to apply the changes

Cancel : Click this button to cancel the change

Wireless MAC Filter

Set up a list of clients and policies that allow only the clients on the list to associate with this AP or to reject clients on the list from associating with this AP. Set up the list with MAC addresses. A MAC address is a unique ID assigned by the manufacturer of the network adapter. Enter a MAC address and click **Add** to add it to the list. Click **Delete** to remove an entry. Select your **ACL Mode** and then click **Apply**. (You can also go to the wireless client list and click **Kick and Ban** to add a client to the list.)

ACL (Access Control List) Mode :

Choose "Disabled" to disable the MAC filter.

Choose "Deny MAC in the List" to allow clients that aren't on the list to associate with the TEW-753DAP's 5GHz wireless interface.

Choose "Allow MAC in the List" to deny clients that aren't on the list from associating with the TEW-753DAP's 5GHz wireless interface.

SSID:#	MAC Address	TX(Bytes)	RX(Bytes)	RSSI(dBm)	Kick and Ban
SSID1:#1	00:17:c4:00:17:c4	90Kb	358Kb	-38	Kick and Ban
SSID8:#1	00:23:6c:00:23:6c	904Kb	571Kb	-22	Kick and Ban

Click **Kick and Ban** in the wireless client list to add a MAC entry to MAC filter list.

Wireless Advanced Settings

Fine tune your wireless settings on this page.

5GHz / Wireless Advanced Settings

Data Rate	Auto			
Transmit Power	18 dBm			
RTS/CTS Threshold (1 - 2346)	2346	bytes		
Distance (1-30km)	1	km		
Aggregation:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable 32 Frames 50000 Bytes(Max)			

WMM Parameters				
AC	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3.008ms
AC_VO	2	3	2	1.504ms

Client limit		
Frequency	Enable	Max Client
5G	<input checked="" type="checkbox"/>	127

Apply
Cancel

<p>Data Rate :</p> <div style="border: 1px solid #ccc; padding: 2px;"> Auto ▼ MCS0 MCS1 MCS2 MCS3 MCS4 MCS5 MCS6 MCS7 MCS8 MCS9 MCS10 MCS11 MCS12 MCS13 MCS14 MCS15 Auto </div> <p>6Mbps 9Mbps 12Mbps 18Mbps 24Mbps 36Mbps 48Mbps 54Mbps</p>	<p>Select different 802.11n Modulation and Coding Scheme (MCS) against particular wireless noise or select auto for the TEW-753DAP to select MCSs dynamically. Or, choose the speed you want in 802.11a mode.</p>
<p>Transmit Power :</p> <div style="border: 1px solid #ccc; padding: 2px;"> 18 dBm ▼ 11 dBm 12 dBm 13 dBm 14 dBm 15 dBm 16 dBm 17 dBm 18 dBm </div>	<p>Wireless signal transmission power. Setting transmission power to an appropriate value can make your multiple AP deployment easier. The default value is 18 dBm. Valid settings are between 11 and 18 (both FCC and CE).</p>

RTS/CTS Threshold :	Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and to prevent hidden nodes from degrading the performance. Specify a value between 1 and 2346. The default value is 2346
Distance :	Set the distance between the TEW-753DAP and other access points or wireless clients. Low speed/ long range settings may be a priority for longer range connection. Valid settings are between 1 and 30. The default value is 1 Km.
Aggregation :	Combine short packets and send them together. Enabling packet aggregation will increase data throughput. However, it may cause jitters or delays in real-time communication.

WMM Parameters				
AC	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3.008ms
AC_VO	2	3	2	1.504ms

WMM Parameters

AC :	Access Category: best effort (AC_BE), background (AC_BK), video (AC_VI), and voice (AC_VO)
CWmin :	Minimum contention window
CWmax :	Maximum contention window
AIFSN :	The Arbitration Inter-Frame Spacing Number specifies a wait time for data frames

TXOP Limit :	Transmission Opportunity Limit : The limit of the interval of time between the access point having the right to initiate transmissions and the transmission start time.
---------------------	---

Client limit	Frequency	Enable	Max Client
	5G	<input checked="" type="checkbox"/>	127

Apply Cancel

Client Limit

Frequency :	Limit the number of clients connected to the 5GHz interface
Enable :	Check this box to enable maximum client limitation
Max Client :	The maximum number of clients that can connect to the TEW-753DAP's 5GHz interface is 127. The valid numbers are from 1 to 127. The default value is 127.

WPS

WPS is one way to connect a wireless client to the TEW-753DAP. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both the wireless client and the TEW-753DAP, and WPS will do the rest for you.

Only the first SSID (SSID 9) supports WPS pairing. There are two types of WPS: WPS via Push Button and WPS via PIN code are supported. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start WPS pairing, and click the **Start to Process** button in this page under **WPS via Push Button** to start WPS pairing.

If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the access point.

WPS is disabled by default. To enable it, you have to click **Enable** and then Apply. Go to **Save/Apply** to apply the changes. Then come back to this page to start your WPS session.

WPS :	Enable the WPS feature
WPS Current Status :	Displays the current status of the WPS configuration. Press Release Configuration to release previous settings.
Self Pin Code :	Displays PIN code of TEW-753DAP

SSID :	Displays the SSID for WPS pairing. Only the first SSID (SSID 9) can proceed with WPS pairing.
Authentication Mode :	Displays the authentication mode of SSID 9
Passphrase Key :	Current passphrase. Click the check box to reveal the passphrase.
WPS Via Push Button :	Click on the Start to Process button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click the OK button in the dialog box
WPS via PIN :	Specify a PIN, a unique number that can be used to add the router to an existing network or to create a new network. Then click the Start to Process button

Management

Administration

Change the password required to log into the access point's web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive. Enter your password and system information and then click **Apply** to save the change.

New Name: The new administrator login name

Old Password: Enter the current password for authentication allowing new password change.

New Password: Enter your new password here.

Confirm Password: Type your new password again for verification purposes

Management VLAN Settings

This feature is only available under Access Point or WDS AP mode and allows users to configure the 802.1q VLAN settings to for all wireless clients. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Enter the VLAN ID you want to tag to clients associated with specific SSIDs. Different SSIDs should be set with different VLAN IDs. Enable Virtual LAN service and click **Apply** to save the changes.

LAN VLAN MGMT is a special VLAN to manage the TEW-753DAP. Enabling management VLAN tagging will keep all services, for example DHCP server and client, in this VLAN.

Management VLAN Settings

2.4G Current Profiles				
SSID	Security	Isolation	VID	Enable
TRENDnet753_2.4GHz_5RL2	WPA2-PSK AES	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>
	None	<input type="checkbox"/>	2	<input type="checkbox"/>
	None	<input type="checkbox"/>	3	<input type="checkbox"/>
	None	<input type="checkbox"/>	4	<input type="checkbox"/>
	None	<input type="checkbox"/>	5	<input type="checkbox"/>
	None	<input type="checkbox"/>	6	<input type="checkbox"/>
	None	<input type="checkbox"/>	7	<input type="checkbox"/>
	None	<input type="checkbox"/>	8	<input type="checkbox"/>

5G Current Profiles				
SSID	Security	Isolation	VID	Enable
TRENDnet753_5GHz_5RL2	WPA2-PSK AES	<input type="checkbox"/>	51	<input checked="" type="checkbox"/>
	None	<input type="checkbox"/>	52	<input type="checkbox"/>
	None	<input type="checkbox"/>	53	<input type="checkbox"/>
	None	<input type="checkbox"/>	54	<input type="checkbox"/>
	None	<input type="checkbox"/>	55	<input type="checkbox"/>
	None	<input type="checkbox"/>	56	<input type="checkbox"/>
	None	<input type="checkbox"/>	57	<input type="checkbox"/>
	None	<input type="checkbox"/>	58	<input type="checkbox"/>

CAUTION: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID

No VLAN tag
 Specified VLAN ID
 (must be in the range 1 ~ 4094.)

Accept Cancel

2.4G / 5G Current Profiles

SSID (1 - 16) :	Showing the human readable SSID
Security :	Wireless security set to the SSID
Isolation :	Packets are not tagged with a VLAN ID by default. Checking this box will tag the VLAN ID to the packets going through this SSID. Packets with different VLAN ID are recognized as if they are in the different network.
VID :	Virtual LAN ID
Enable :	Redundant control to enable or disable the particular SSID.

Management VLAN ID

No VLAN Tag :	Management VLAN packets are not tagged by default.
Specified VLAN ID :	Select this if you want to separate the management VLAN. Enabling tagging will redirect all services, including web management and DHCP, to a specific VLAN, specified in VLAN ID field. (1 ~ 4094)

Apply : Click this button to apply the changes.
(Save/Apply is required to apply changes.)

Cancel : Click this button to cancel the change.

Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

Wireless Traffic Shaping	
Enable Traffic Shaping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Incoming Traffic Limit	10000 kbit/s (512-99999999)
2.4G Setting	
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %
SSID #1 : TRENDnet753_2.4GHz_5RL2	10 %
SSID #2 : (Off)	10 %
SSID #3 : (Off)	10 %
SSID #4 : (Off)	10 %
SSID #5 : (Off)	10 %
SSID #6 : (Off)	10 %
SSID #7 : (Off)	10 %
SSID #8 : (Off)	10 %
5G Setting	
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %
SSID #1 : TRENDnet753_5GHz_5RL2	10 %
SSID #2 : (Off)	10 %
SSID #3 : (Off)	10 %
SSID #4 : (Off)	10 %
SSID #5 : (Off)	10 %
SSID #6 : (Off)	10 %
SSID #7 : (Off)	10 %
SSID #8 : (Off)	10 %
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Enable Traffic Shaping :	Choose to enable or disable the traffic shaping feature
Incoming Traffic Limit :	Set the traffic limitation going through Ethernet port. The default value is 10Mbps (10,000). The number can be set from 512 to 99,999,999. The traffic will be limited by this value and physical speed whichever is lower. (The TEW-753DAP Ethernet port is capable of 1Gbps, 1,000,000 kbps.)

2.4GHz / 5GHz Settings

Outgoing Traffic Limit :	Set the traffic limitation going through the wireless interface. The default value is 180Mbps (180,000). The number can be set from 512 to 99,999,999. The traffic will be limited by this value and physical speed whichever is lower. (The TEW-753DAP wireless interfaces are capable of 300 Mbps, 300,000 kbps for 2.4GHz and 5GHz respectively.)
Total Percentage :	This value adds up all numbers in following 8 SSID percentage settings. This value may exceed 100, up to 800. The traffic limit of this wireless interface is calculated as: Outgoing Traffic Limit * Total Percentage.
SSID (1 - 8) :	Set the number you want to shape your traffic for clients connects to specific SSIDs by increasing or decreasing the value. The default value is 10 (%). The number can be set from 0 to 100. The traffic limit of this SSID is calculated as: Outgoing Traffic Limit * Total Percentage.

Apply : Click this button to apply the changes. (Save/Apply is required to apply changes.)

Cancel : Click this button to cancel the change

SNMP Settings

SNMP Settings allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

SNMP Settings

SNMP	<input type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read/Write)	<input type="text" value="private"/>
Trap Destination Address	<input type="text"/>
Trap Destination Community Name	<input type="text" value="public"/>
SNMPv3	<input type="radio"/> v3Enable <input type="radio"/> v3Disable
User Name	<input type="text" value="admin"/>
Auth Protocol	<input type="text" value="MD5"/>
Auth Key (8-32 Characters)	<input type="text" value="12345678"/>
Priv Protocol	<input type="text" value="DES"/>
Priv Key (8-32 Characters)	<input type="text" value="12345678"/>
Engine ID	<input type="text"/>

SNMP :	Choose to enable or disable the SNMP feature
Contact :	Specify the contact details of the TEW-753DAP
Location :	Specify the location of the TEW-753DAP
Community Name (Read Only) :	Specify the password for access the SNMP community for read only access
Community Name (Read/Write) :	Specify the password for access to the SNMP community with read/write access
Trap Destination Address :	Specify the IP address for the SNMP trap community
Trap Destination Community Name :	Specify the name of SNMP trap community

SNMP v3 :	Select enable or disable SNMP v3 protocol
User Name :	SNMP v3 manager user name
Auth Protocol :	Choose the authentication method to verify the source of information: MD5, SHA, or None. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> MD5 ▼ MD5 SHA None </div>
Auth Key :	Specify the authentication key between 8 to 32 letters.
SNMP Manager IP :	Specify the SNMP manager IP address
Priv Protocol :	Choose the privacy key to encrypt SNMP messages: DES or None. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> DES ▼ DES None </div>
Priv Key :	Specify the privacy key between 8 to 32 letters.
Engine ID :	SNMPv3 engine ID

Save/Apply : Click this button to apply the changes.

Cancel : Click this button to cancel the change.

Backup / Restore Settings

This page allows you to save the current configurations. Click **Backup** to save your current configuration.

To load previously saved configurations, click **Choose File** to find the configuration file and then click **Restore**. The configuration file is encrypted with an **Encryption Key**. Enter your encryption key and then click Save to save the key to the TEW-753DAP. The new configuration file will be saved and encrypted with this new key.

In case you want to reset TEW-753DAP's configurations back to factory defaults, click **Factory Default** in this page. All configurations will be set back to their original default settings.

Firmware Upgrade

TRENDnet may periodically release firmware upgrades that might add features or fix problems associated with your TRENDnet model and version. To find out if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link.

<http://www.trendnet.com/downloads/>

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.
3. Log into the TEW-753DAP
4. Click on **Management** and then **Firmware Upgrade**
5. Click **Choose File** and navigate to the folder on your computer in which the unzipped firmware file (.bin) is.
6. Located and select it the firmware file.
7. Click **Upload**.

Time Settings

The accuracy of the system clock is important for scheduling and accurate logging. You can synchronize the system time with your computer, or automatically check the time accuracy with a network time server (NTP server).

Time Settings

Time

Manually Set Date and Time

2013 / 08 / 20 10 : 40 [Synchronize with PC](#)

Automatically Get Date and Time

Time Zone: UTC+00:00 Gambia, Liberia, Morocco

User defined NTP Server: 209.81.9.7

Enable Daylight Saving

Start

Time: January 1st Sun 12 am

End

Time: January 1st Mon 12 am

[Save/Apply](#) [Cancel](#)

Manually Set Date and Time

Choose this option to manually set your system clock. You can enter the time manually or you can copy the time from your computer by clicking **Synchronize with PC**. Click **Save/Apply** to change the system clock.

Automatically Get Date and Time

Choose this selection to get the time from a network time server automatically. Select the **Time Zone** of the country or region you are currently in. The TEW-753DAP will set its time based on your selection.

If you have a preferred NTP server, check the **User defined NTP Server** and Enter the NTP server IP address. Otherwise, leave it unchecked to use the TEW-753DAP's default NTP server.

Check **Enable Daylight Saving** if your time zone has daylight savings. Enter the start time and end time of daylight savings.

When you finish your settings, click **Save/Apply** to change the system clock.

Schedule

Service schedule can be set up daily or weekly for power saving and security reasons. You can setup up to 50 schedule entries. Click **Add** to add a schedule entry. Select an entry and then click **Delete Selected** to delete the entries. Click **Reset** to remove the selections. Click **Delete All** to remove all entries. After schedule editing, click **Apply** to save your schedule. Check **Enabled Schedule Table** to make AP services work with the schedule.

Schedule

Wifi Schedule:

Schedule Name:

Service: Reboot
 Wireless Active (2.4GHz)
 Wireless Active (5GHz)
 Wireless Active (Both)

Day: Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time of day: :

Schedule Table				
#	Name	Service	Schedule	Select
1	a1	Wireless Active (2.4GHz)	ALL Time- - Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>
2	b	Wireless Active (2.4GHz)	ALL Time- - Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>

Schedule Table				
#	Name	Service	Schedule	Select
1	a1	Wireless Active (2.4GHz)	ALL Time- - Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>
2	b	Wireless Active (2.4GHz)	ALL Time- - Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>

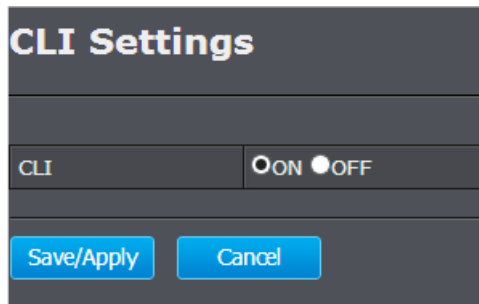
Delete Selected :	Delete selected schedule
Delete All :	Click this button to clear the list
Reset :	Reset previous selections

Apply : Click this button to apply the changes.

Cancel : Click this button to cancel the change.

CLI Settings

To enable the Command Line Interface for batch management or advanced configuration, select CLI ON and then click **Save/Apply**.



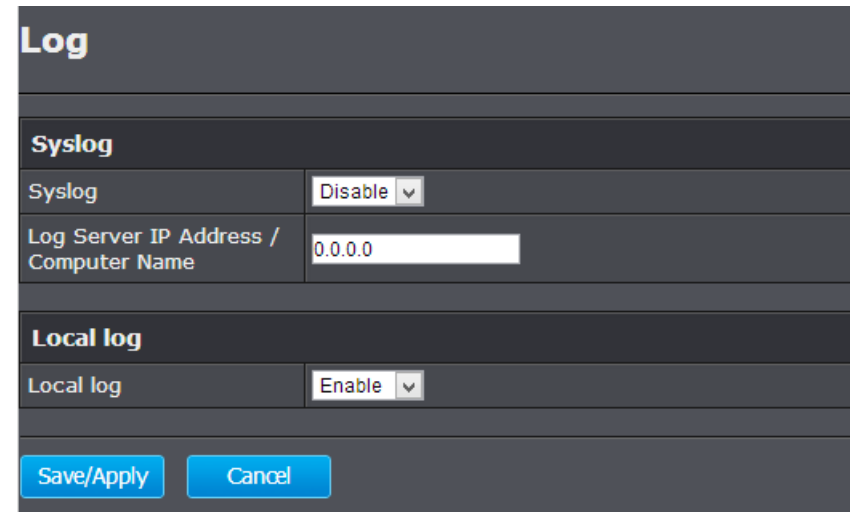
The image shows a configuration window titled "CLI Settings". It has a dark grey background. At the top, the title "CLI Settings" is in white. Below the title, there is a section for "CLI" with two radio buttons: "ON" (which is selected) and "OFF". At the bottom of the window, there are two blue buttons: "Save/Apply" and "Cancel".

Access the CLI interface using SSH with the administrator user name and password. For example (in Linux):

```
$ ssh admin@192.168.10.100
The authenticity of host '192.168.10.100
(192.168.10.100)' can't be established.
RSA key fingerprint is b2:41:6e:0f:4b:2a:f3:03:18:60:
0b:c4:eb:74:9d:9c.
Are you sure you want to continue connecting (yes/
no)? yes
admin@192.168.10.100's password:
*** Hi admin, welcome to use cli(V-1.7.6) ***
----- Commands Help -----
  stat -- Status
  sys  -- System
wless2 -- 2.4G-Wireless
wless5 -- 5G-Wireless
  mgmt -- Management
  tree -- Tree
  help -- Help
  reboot -- Reboot
tew-753dap>
```

Log

To keep your system operating history, you can setup local and remote loggings.



The image shows a configuration window titled "Log". It has a dark grey background. The title "Log" is in white. Below the title, there are two sections: "Syslog" and "Local log". In the "Syslog" section, there is a "Syslog" dropdown menu set to "Disable" and a "Log Server IP Address / Computer Name" text input field containing "0.0.0.0". In the "Local log" section, there is a "Local log" dropdown menu set to "Enable". At the bottom of the window, there are two blue buttons: "Save/Apply" and "Cancel".

Syslog

Select **Enable** from the drop down list and then enter the log server IP address or URL. Then click **Save/Apply** to save the log to the log server.

Local Log

Select **Enable** from the drop down list and then click **Save/Apply** to save the log locally. You can view the log in **Status > System Log**

Diagnosis

There are 3 network tools you can use on the TEW-753DAP: ping, traceroute, and speed test.

Diagnostics

Ping Test Parameters

Target IP / Domain Name	<input style="width: 80%;" type="text"/>
Ping Packet Size	<input style="width: 40%;" type="text" value="64"/> bytes
Number of Pings	<input style="width: 40%;" type="text" value="4"/>

[Start Ping](#)

Traceroute Test Parameters

Traceroute target	<input style="width: 80%;" type="text"/>
-------------------	--

[Start Traceroute](#)

Speed Test

Target Address	<input style="width: 80%;" type="text"/>
Time period	<input style="width: 40%;" type="text" value="20"/> Sec
Check Interval	<input style="width: 40%;" type="text" value="5"/> Sec

[Start Speed Test](#)

IPv4 Port	<input style="width: 80%;" type="text" value="5001"/>
IPv6 Port	<input style="width: 80%;" type="text" value="5002"/>

PING

Enter the **Target IP / Domain Name**, **Ping Packet Size** and **Number of Pings** and then click **Start Ping** to start the PING tool.

Diagnostics Results

```
PING trendnet.com (192.168.1.249): 64 data bytes
72 bytes from 192.168.1.249: seq=0 ttl=127 time=1.368 ms
72 bytes from 192.168.1.249: seq=1 ttl=127 time=1.036 ms
72 bytes from 192.168.1.249: seq=2 ttl=127 time=1.063 ms
72 bytes from 192.168.1.249: seq=3 ttl=127 time=1.048 ms

--- trendnet.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.036/1.128/1.368 ms
```

[Go Back](#)

Traceroute

Enter the **Traceroute Target** and then click **Start Traceroute** to start the Traceroute tool.

Diagnostics Results

```
traceroute to trendnet.com (192.168.1.249), 30 hops max, 38 byte packets
 1  10.10.10.254 (10.10.10.254)  1.192 ms  0.558 ms  0.033 ms
 2  192.168.1.249 (192.168.1.249)  0.953 ms  1.443 ms  0.822 ms
```

[Go Back](#)

Speed Test

Setup an iperf server. Enter the server address as the **Target Address, Time Period, Check Interval** and then click **Start Speed Test** to start the speed test tool. The default IPv4 test port is 5001 and the IPv6 test port is 5002.

Diagnostics Results

```

-----
Client connecting to 10.10.10.2, TCP port 5001
TCP window size: 16.0 KByte (default)
-----
[ 6] local 10.10.10.100 port 40886 connected with 10.10.10.2 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 6]  0.0- 5.0 sec  5.88 MBytes 9.86 Mbits/sec
[ 6]  5.0-10.0 sec  5.63 MBytes 9.44 Mbits/sec
[ 6] 10.0-15.0 sec  5.75 MBytes 9.65 Mbits/sec
[ 6] 15.0-20.0 sec  5.63 MBytes 9.44 Mbits/sec
[ 6]  0.0-20.0 sec 22.9 MBytes 9.61 Mbits/sec

```

Go Back

Device Discovery

The TEW-753DAP can discover other TEW-753DAPs on neighboring wired or wireless network.

Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version

Refresh

Device Name :	Device name of neighbor TEW-753DAP.
Operation Mode :	Which operation mode the neighbor TEW-753DAP is running.
IP Address :	IP address of neighbor TEW-753DAP
System MAC Address :	System MAC address (LAN/ 2.4GHz wireless interface MAC address) of neighbor TEW-753DAP.
Firmware Version :	Firmware version the neighbor TEW-753DAP is running.

Refresh : Click this button to discover the neighboring devices.

LED Control

All LED indicators are turned on by default. You can turn any one of them or all of them on or off. Click the LED you want to turn on or off and then click **Save/Apply** to save and apply the changes.

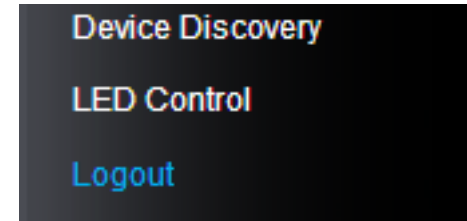
LED Control	
Power LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF
LAN LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF
2.4GHz LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF
5GHz LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF

Save/Apply Cancel

Power LED	OFF	Powered off or LED display is disabled
	ON	Powered on
Network LED Orange: 10/100 Green: Giga bit	OFF	No network connection detected through Ethernet port (PoE) or LED display has been disabled
	ON	Network connected through Ethernet port (PoE)
	Flashing	Network activities are detected on Ethernet (PoE) port
Wireless LED Orange: 2.4GHz Green: 5GHz	OFF	No wireless network connection or LED display is disabled
	Flashing	Wireless network activities are detected

Logout

Logout from the management page. The TEW-753DAP allows only one management login at the same time. If you want to access the TEW-753DAP from different computer, remember to logout of the web management page first.



Appendix

WDS Frequent Asked Questions

What is WDS?

WDS stands for Wireless Distribution System, a non-standard extension to the IEEE 802.11 standard to allow transparent Ethernet bridging on the station and to implement seamless hand-over for wireless clients roaming between different access points.

Should I use WDS or not?

WDS links create transparent bridges facilitate layer 2 seamless communication. You don't have to use WDS if you don't need layer 2 services passing through TEW-753DAP, such as MAC filtering, and 802.1X authentication. You can simply use AP, Client Bridge, and Repeater mode to fit most of your network plan.

What problem WDS is resolving?

The 802.11 standard only uses three MAC addresses for frames transmitted between the Access Point and the Station. Frames transmitted from the station to the AP don't include the Ethernet source MAC address of the requesting host and response frames are missing the destination Ethernet MAC to address the target host behind the client bridge.

WDS AP and WDS Station uses the 4 MAC address including complete source, destination, WDS AP, and WDS Station addresses. Data frame arriving WDS AP or WDS Station will be translated back to 802.3 data frame with real source address instead of WDS AP or WDS Station address. The 4 addresses design keeps the original data frame intact bridging to the other side transparently.

What should I have to build WDS network?

You have to use multiple TEW-753DAPs to build WDS AP - WDS Station pair or WDS bridge mesh groups. Different model with same or different brand name may NOT work together because of the different WDS implementation details.

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC.. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC:

EN 60950-1:2006+A11:2009+A1:2010+A12:2011
IEC 60950-1:2005 (2nd Edition) Am 1:2009
Safety of Information Technology Equipment

EN50385 : 2002

Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)

EN 300 328 V1.7.1

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.9.2

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.2.1

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance WLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.










In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.










This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

**RoHS**

This product is RoHS compliant.



 Český [Czech]	TRENDnet tímto prohlašuje, že tento TEW-753DAP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
 Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-753DAP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.
 Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-753DAP in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG und 2009/125/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-753DAP vastavust direktiivi 1999/5/EÜ, 2006/95/EÜ ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, TRENDnet, declares that this TEW-753DAP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2006/95/EC, and 2009/125/EC.
 Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-753DAP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, 2009/125/CE y.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TRENDnet ΔΗΛΩΝΕΙ ΟΤΙ ΤΕW-753DAP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK, 2006/95/EK, 2009/125/EK κ.α.
 Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-753DAP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE, 2006/95/CE, 2009/125/CE et.
 Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-753DAP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
 Latvīski [Latvian]	Ar šo TRENDnet deklarē, ka TEW-753DAP atbilst Direktīvas 1999/5/EK, 2006/95/EK, un 2009/125/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
 Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-753DAP atitinka esminius reikalavimus ir kitas 1999/5/EB, 2006/95/EB ir 2009/125/EB Direktyvos nuostatas.

 Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-753DAP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.
 Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-753DAP jikkonforma mal-ftigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/KE, 2006/95/KE, u 2009/125/KE.
 Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-753DAP megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-753DAP jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.
 Português [Portuguese]	TRENDnet declara que este TEW-753DAP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
 Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-753DAP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES, a 2009/125/ES.
 Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TEW-753DAP spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EF.
 Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-753DAP tyyppinen laite on direktiivin 1999/5/EY, 2006/95/EY ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-753DAP står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG, 2006/95/EG och 2009/125/EG.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

- TEW-753DAP – 3 Years Warranty
- AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME

FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.



Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA