User's Guide

TRENDnet®

Wireless LAN Controller

TEW-WLC100

Contents

Product Overview

TEW-WLC100

Package Contents

In addition to your controller, the package includes:

- Quick Installation Guide
- CD-ROM (User's Guide)
- Power adapter (12V DC, 1A)
- Rack mount kit

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 Wireless LAN Controller, model TEW-WLC100, lets you easily setup and manage access points across your network from a single interface. Intelligent radio resource manamagement ensures your mobile wifi clients have optimal roaming conditions when wirelessly transitioning between access points within the network. Simultaneously manage up to 32 access points, perform batch firmware upgrades, and monitor network connection status.

Centralized AP Management

Easily manage up to 32 access points (AP) across your wireless network

Intelligent Radio Resource Management

Intelligent radio resource manamagement ensures your mobile wifi clients have optimal roaming conditions when wirelessly transitioning between access points within the network

Access Point Monitoring

View the status of online users or network devices

Simultaneously Upgrade Firmware

Select multiple access points to upgrade firmware at the same time

Rack Mount Design

Standard 19" 1U design (brackets included)

Product Hardware Features

Front View

Rear View

1 LED indicators
2 USB port
3 Reset button
4 Gigabit ports
5 Power switch
6 Power port

- **Reset Button –** Press and hold this button for 10 seconds and release to reset the controller to factory defaults. The ports LEDs will turn off to indicate that the reset was initiated.

- **Gigabit Ports (1-5) –** Connect to your LAN network and connect additional network devices.

- **Power Port** – Connect the included power adapter to your controller power port and then to an available power outlet.
  Note: *Use only the adapter that came with your controller.*

- **On/Off Power Switch** – Push the controller On/Off push button to turn your controller "On" (Inner position) or "Off" (Outer position).

- ***USB Port –** Reserved for firmware upgrade, backup/restore configuration functions.
  ****Note:*** *Functionality is not available in initial shipping firmware will be added in future firmware upgrade.*

- **Security Slot –** Can be used to with third party lock to physically secure your controller to a specific location.

LED Indicators

- **POWER/SYSTEM LED**

On	:	When the System LED is on, the device is receiving power.
Off	:	When the System turns off, the power adapter is not connected or the device is not receiving power.

- **LAN LED**

On (Green)	:	Indicates that a network device (router, switch, access point, computer, etc.) has been physically connected to one of the five Gigabit ports (1-5).
Off	:	Indicates no physical Ethernet connection or no network devices physically connected to any of the Gigabit ports (1-5).

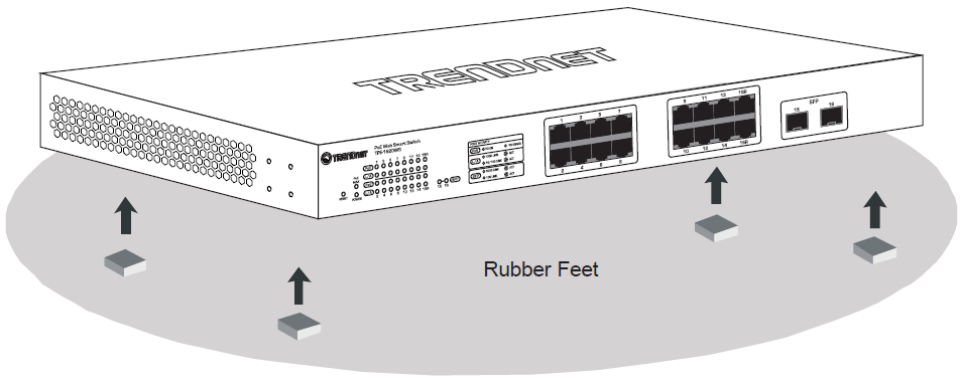
Controller Installation

Desktop Hardware Installation

The site where you install the hub stack may greatly affect its performance. When installing, consider the following pointers:

Note: *The controller model may be different than the one shown in the example illustrations.*

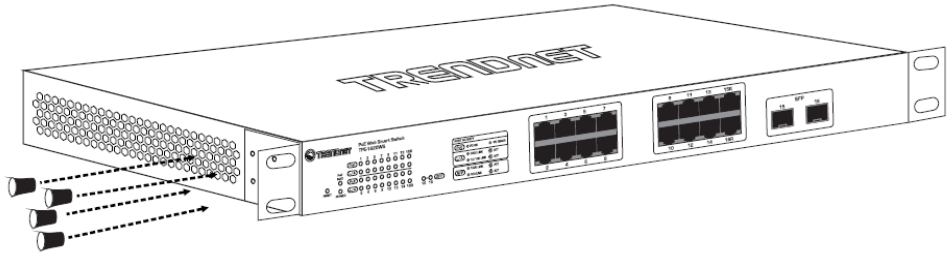
- Install the controller in a fairly cool and dry place.
- Install the Controller in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 10cm of space at the front and rear of the hub for ventilation.
- Install the Controller on a sturdy, level surface that can support its weight, or in an EIA standard-size equipment rack. For information on rack installation, see the next section, Rack Mounting.
- When installing the Controller on a level surface, attach the rubber feet to the bottom of each device. The rubber feet cushion the hub and protect the hub case from scratching.



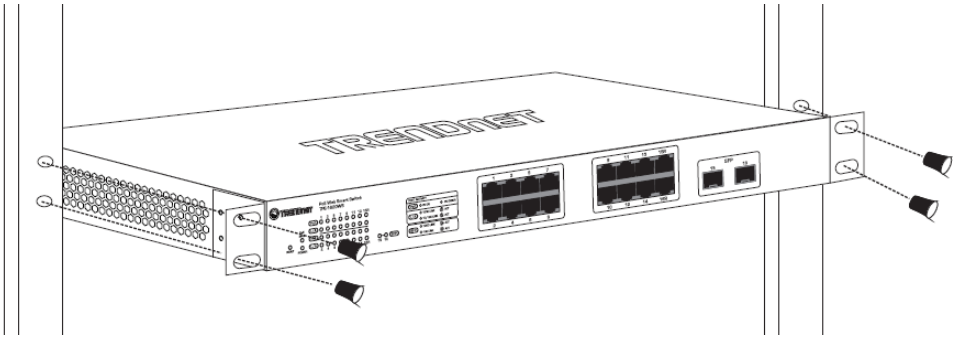
Rack Mount Hardware Installation

The controller can be mounted in an EIA standard-size, 19-inch rack, which can be placed in a wiring closet with other equipment. Attach the mounting brackets at the controller's front panel (one on each side), and secure them with the provided screws.

Note: *The controller model may be different than the one shown in the example illustrations.*



Then, use screws provided with the equipment rack to mount each controller in the rack.



Basic Installation

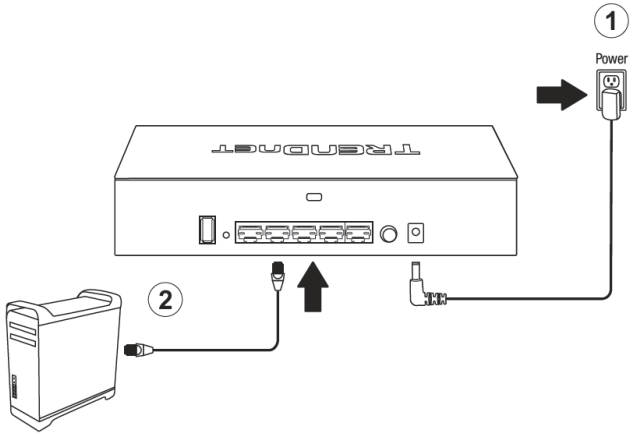
Access Point Compatibility

Before you proceed, please ensure you are using one of the access point models in the list and the firmware version your access points has been upgraded accordingly to the versions indicated in the list below. Please reset all access point to the factory default configuration. Also, make sure your network is using a DHCP server to distribute IP addresses to the access points. By default, TRENDnet access point models listed below will obtain an IP address automatically through DHCP or otherwise default back to 192.168.10.100 / 255.255.255.0 if a DHCP server is not available on your network. Each access point must be assigned ma unique IP address on the same network.

Access Point Model	Description	Firmware Version
TEW-755AP	N300 PoE Access Point	1.02 or above
TEW-821DAP	AC1200 Dual Band PoE Access Point	1.04 or above

You can download the access point firmware from http://www.trendnet.com/support which include instructions on how to upgrade the firmware.

Hardware Installation and Configuration



3. Assign a static IP address to your computer's network adapter in the subnet of 192.168.10.x (e.g. 192.168.10.25) and a subnet mask of 255.255.255.0.

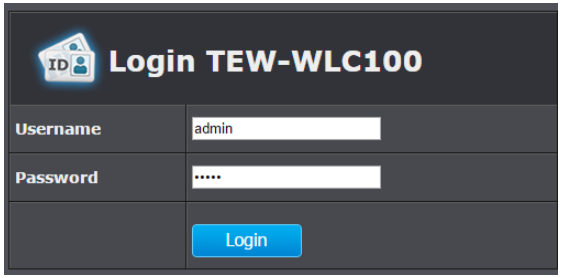
4. Open your web browser, and type the IP address of the controller in the address bar, and then press **Enter**. The default IP address is **192.168.10.200**.

5. Enter the User Name and Password, and then click **Login.** By default:

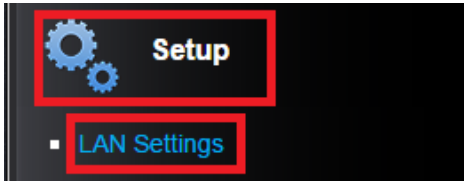
User Name: **admin**

Password: **admin**

Note: *User name and password are case sensitive.*

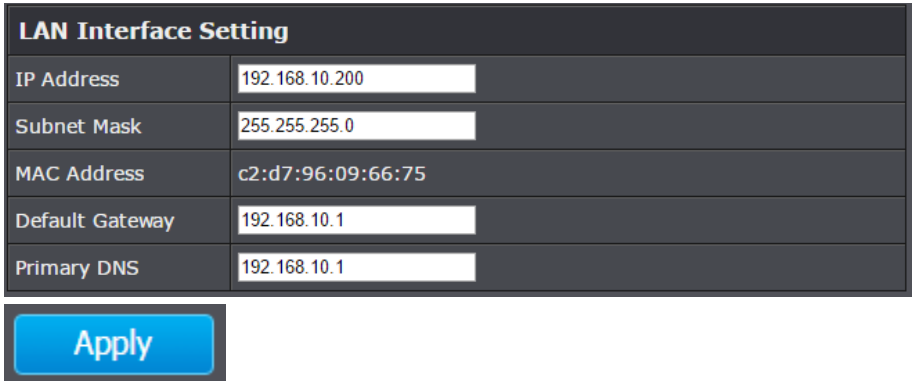


6. Click **Advanced**, click on **Setup,** and then click **LAN Settings**.

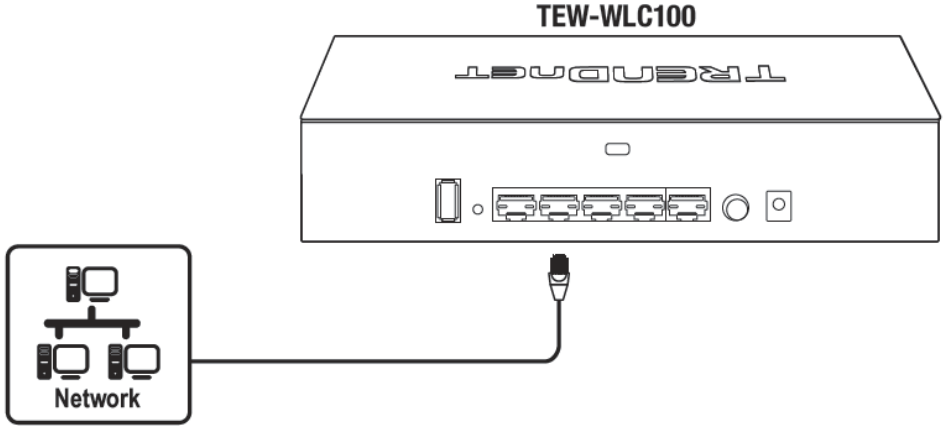


7. Configure the controller IP address settings to be within your network subnet, then click **Apply.**

Note: *You may need to modify the static IP address settings of your computer's network adapter to IP address settings within your subnet in order to regain access to the controller. The Default Gateway and DNS IP settings must be assigned to ensure the wireless controller is able to check for available online firmware upgrades*



8. Using an Ethernet cable, connect one of the five Gigabit Ethernet ports located on the back of the wireless controller to your network (e.g. router, switch, etc.)

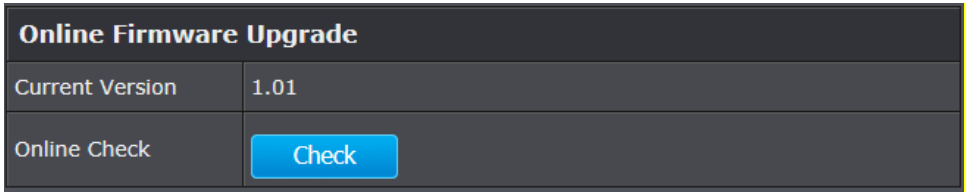


9. Access the wireless controller management page using the newly assigned IP address.

Note: *You may need to revert to your computer's original IP address settings before you can access the wireless controller with the new IP address settings.*

10. Click **Advanced**, click **Setup**, then click on **Firmware**.

11. Click **Check** to check for available online firmware upgrades.

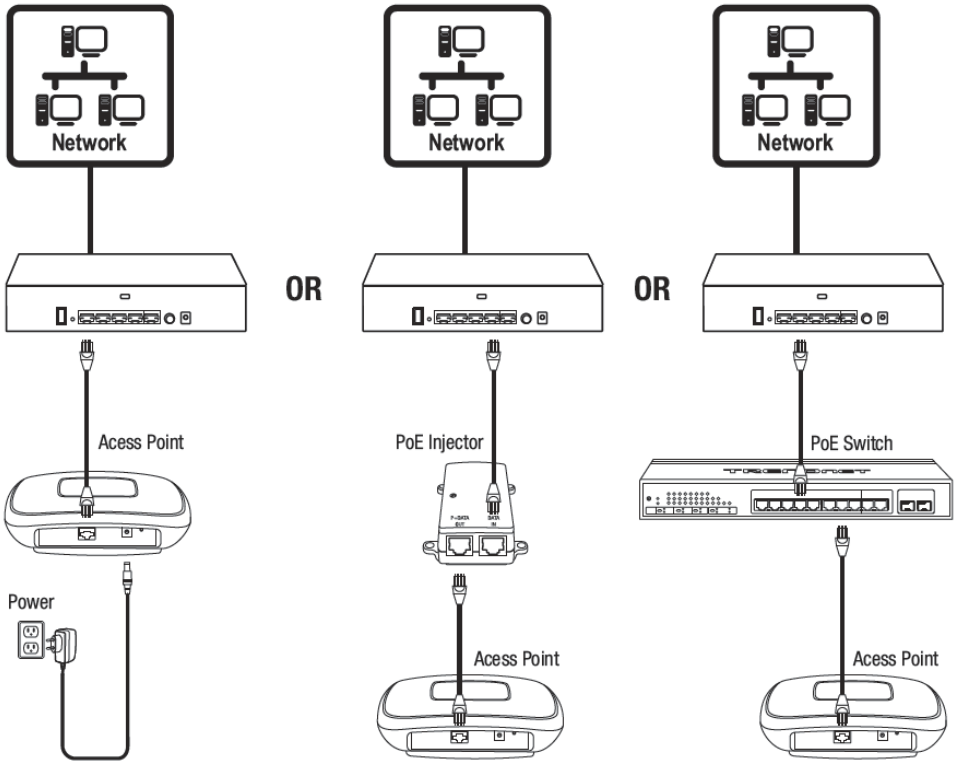


Connect your wireless access points

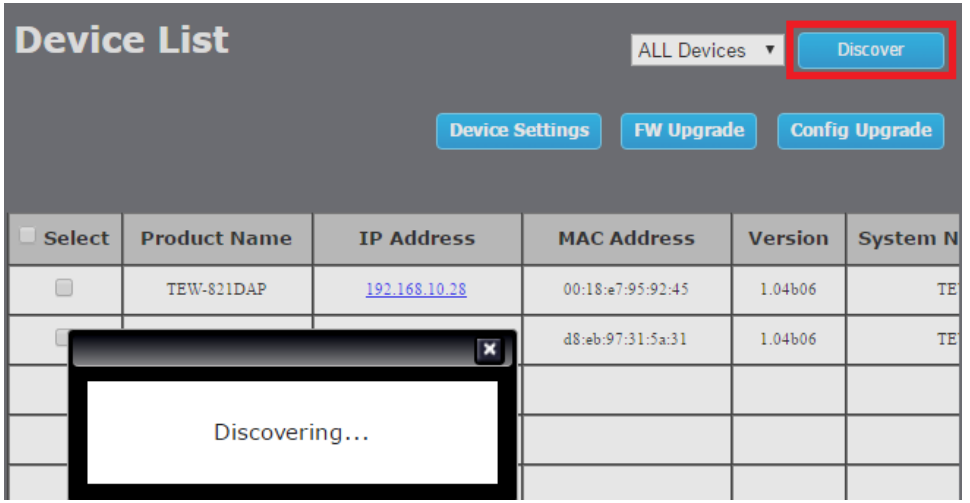
Important Note: *Please make sure your access points have met the requirements in the earlier section* ***Access Point Compatibility*** *on page 4.*

1. Using an Ethernet cable, connect each wireless access point to the wireless controller or your network.

Note: *If powering your access points using their power adapters, you can connect the access points directly to your network or the wireless controller. If powering the access point(s) using power over Ethernet (PoE), you can connect your access points to your network or to the wireless controller using a separate PoE injector or PoE switch (not included).*



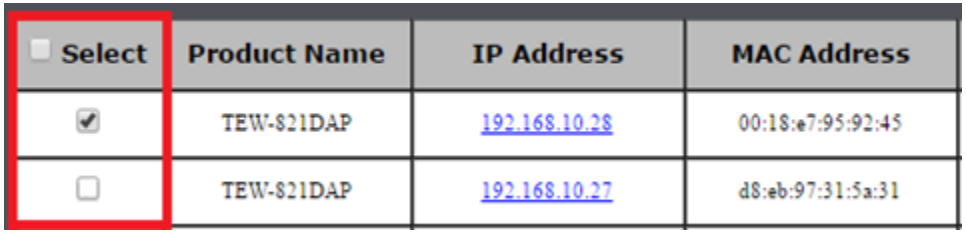
2. After the access points are connected to your network and powered on, click on **Basic**, click on **AP Management**, and **Device List** in the wireless controller management page. Then click on **Discover** to search for available wireless access points.



3. After your access points have been found, they will automatically appear in the **Device List**.

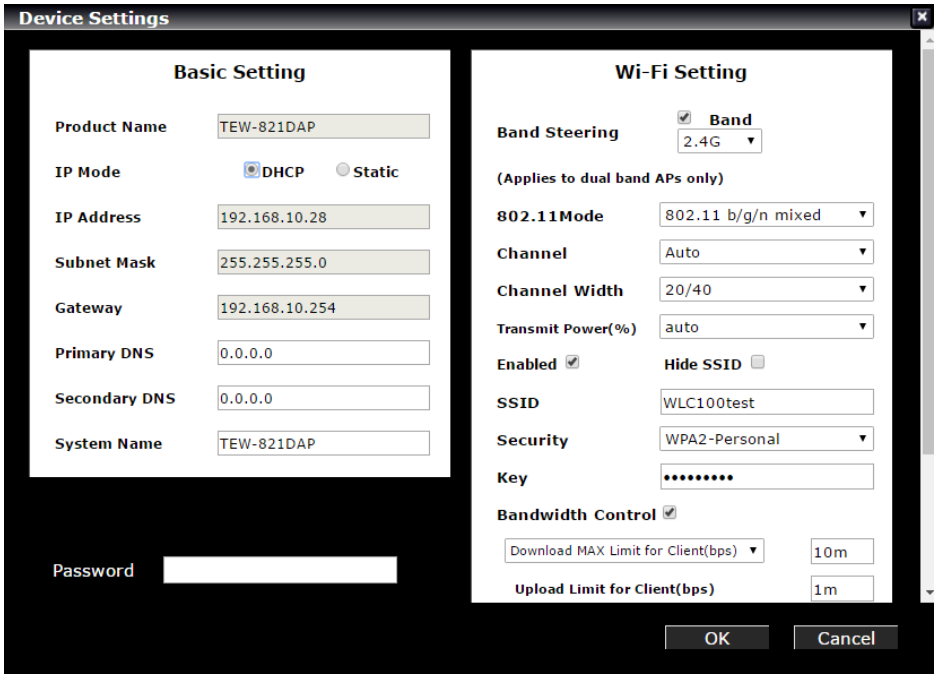
Select	Product Name	IP Address	MAC Address
☐	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45
☐	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31

4. To configure access point settings, under the **Select** column, check one or multiple access points you would like to configure and click on **Device Settings** to configure the access points.



5. You can modify the access point basic settings such as SSID and encryption key on each band.

Note: *If you are using a combination of single band (2.4G) and dual band access points (2.4G & 5G), the 5G settings will only be applied to dual band access points.*



6. After modifying the settings, scroll down to the **Password** field, enter the access point(s) management password (default access point password: admin) and click **OK** to apply the settings to the access points.

Configure your wireless controller

Access your wireless controller management page

Note: *Your switch default management IP address http://192.168.10.200 is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.*

1. Open your web browser and go to the IP address http://192.168.10.200. Your switch will prompt you for a user name and password.

2. Enter the user name and password. By default:

   User Name: **admin**
   Password: **admin**
   Note: *User Name and Password are case sensitive.*

Change your controller LAN IP address

Advanced > Setup > LAN Settings

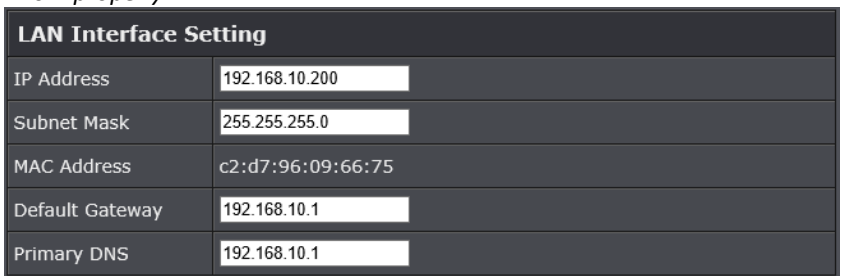
This section allows you to change your controller LAN IP address settings. Typically, the IP address settings should be changed to match your existing network subnet in order to access the switch management page on your network.

Default Controller IP Address: 192.168.10.200

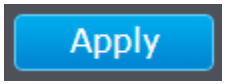
Default Controller IP Subnet Mask: 255.255.255.0

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).
2. Click on **Advanced**, click on **Setup**, and click on **LAN Settings**.
3. Review the settings. When you have completed making changes, click **Apply** to save the settings.

- **IP Address:** Enter the new controller IP address. (e.g. *192.168.200.200*)
- **Subnet Mask:** Enter the new controller subnet mask. (e.g. *255.255.255.0*)
- **MAC Address:** Displays the controller MAC address.
- **Default Gateway:** Enter the default gateway IP address. (e.g. 192.168.200.1 or typically your router/gateway to the Internet).
- **Primary DNS:** Enter the primary DNS server IP address in order to resolve domain or host names. (e.g. 192.168.200.20)
  Note: *The default gateway and primary DNS settings need to be entered in order for NTP server time resolution and online firmware upgrade check functions to work properly.*



4. Click **Apply**.



Upgrade your controller firmware

Advanced > Setup > Firmware

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet controller model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. http://www.trendnet.com/support or use the **Online Firmware Check** in controller management interface.

In addition, it is also important to verify if the latest firmware version is newer than the one your controller is currently running. To identify the firmware that is currently loaded on your controller, log in to the controller, click on the Administrator section and then on the Status. The firmware used by the controller is listed at the top of this page. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

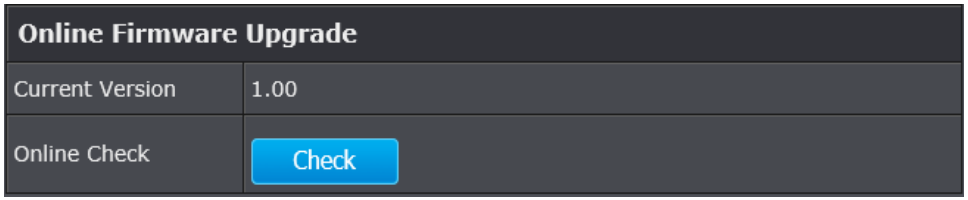
Automatic Firmware Upgrade

Note: *Make sure controller LAN IP address, default gateway, and primary DNS settings are correctly in order for the controller to check the Internet for available firmware upgrades.*

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Advanced**, click on **Setup**, and click on **Firmware**.

3. Under **Online Firmware Upgrade,** click **Check** to check if there are any available firmware upgrades.



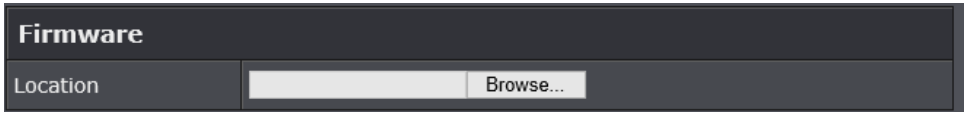
4. If there are any available firmware upgrade, a prompt will appear to download and upgrade to the new firmware version. Follow the steps to complete the online firmware upgrade.

Manual Firmware Upgrade

1. If a firmware upgrade is available (http://www.trendnet.com/support) , download the firmware to your computer.
2. Unzip the file to a folder on your computer.
3. Log into your controller management page (see "Access you wireless controller management page" on page 8).

4. Click on **Advanced** and click **Setup**, then click **Firmware.**

5. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.



6. Navigate to the folder on your computer where the unzipped firmware file (*.bin*) is located and select it.

7. Click **Apply**. If prompted, click **Yes** or **OK**.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your controller.

Change your controller administrative login password

Advanced > Setup > Management

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Advanced** and click on **Setup**, then click on **Management**.

3. Under the **Administrator Settings** section, in the **Password** field.

Note: *The idle timeout setting is used to define the period of inactivity in the controller management page before automatically logging out.*

Administrator Settings	
Account	admin
Password	Show password
Idle Timeout	300 (seconds)

4. To save changes to this section, click **Apply** when finished.

Note: *If you change the controller login password, you will need to access the controller management page using the User Name "admin" and the new password.*

Note: *You can also change the device or system host name under Device Name Settings.*

Device Name Settings	
Device Name	TEW-WLC100

Check the controller system information

Advanced > Administrator > Status

You may want to check the system information of your controller such as system uptime, device time settings, and firmware version.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Advanced** and click on **Administrator**, then click on **Status**

System

- **Firmware Version** – The current firmware version your controller is running.
- **Time:** The current time set on your controller.
- **System Up Time** – The duration your controller has been running continuously without a restart/power cycle (hard or soft reboot) or reset.

System	
Firmware Version	1.00
System Time	Thu Oct, 20, 2016 10:49:41
System Up Time	0d, 1h 58m 18s

LAN

- **MAC Address** – The current MAC address of your controller's wireless or interface configuration.
- **IP Address** - Displays your controller's current IP address.
- **Subnet Mask** – Displays your controller's current subnet mask.

LAN	
MAC Address	C2:D7:96:09:66:75
IP Address	192.168.10.200
Subnet Mask	255.255.255.0

View your controller system log

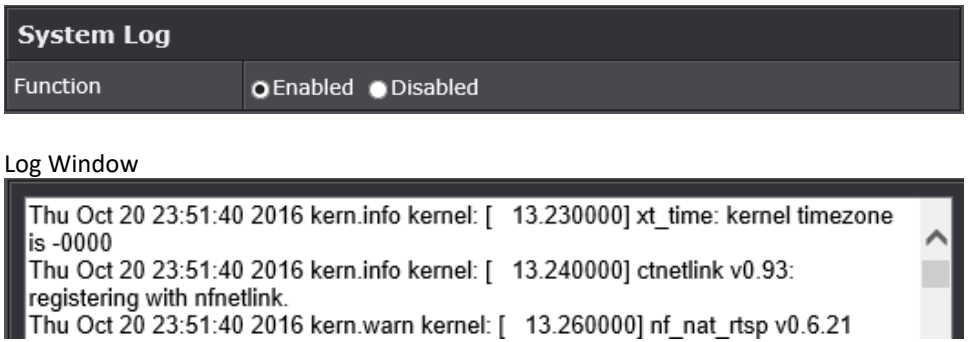
Advanced > Administrator > System Log

Your controller system log can be used to obtain activity information on the functionality of your controller or for troubleshooting purposes.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Advanced** and click on **Administrator**, then click on **System Log.**

3. Next to **Function,** select **Enabled** or **Disabled** to enable or disable logging. Then click **Apply**. The logging will display in the log window.



Log Window

Basic Connectivity Test

Advanced > Administrator > Ping Test

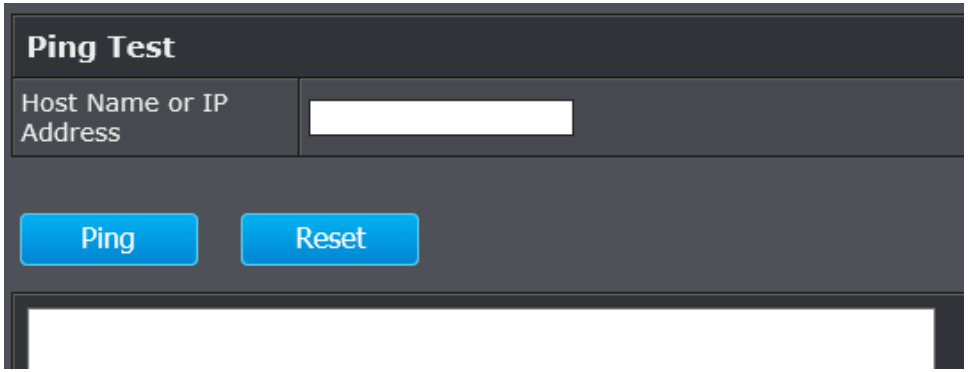
The controller a built in ping test tool to check for basic connectivity.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Advanced** and click on **Administrator**, then click on **Ping Test.**

3. Enter the host name or IP address to check connectivity and click **Ping**.

Note: *Host name connectivity tests require the IP default gateway and primary DNS server settings to configured properly.*



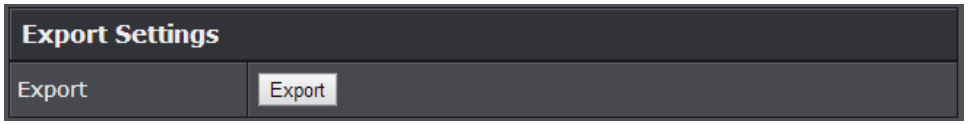
Backup and restore your controller configuration settings

Advanced > Administrator > Settings Management

You may have added many customized settings to your controller and in the case that you need to reset your controller to default, all your customized settings would be lost and would require you to manually reconfigure all of your controller settings instead of simply restoring from a backed up controller configuration file.

To backup your controller configuration:

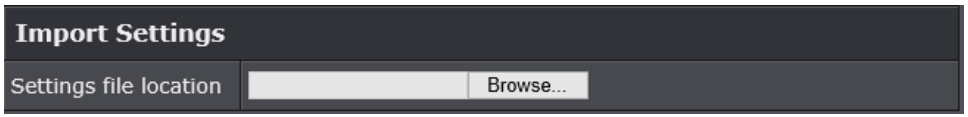
1. Log into your controller management page (see "Access you wireless controller management page" on page 8).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **Export Settings** section and **Export**, click **Export**.



4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *backup-TEW-WLC100-YYYY-MM-DD.tar.gz)*

To restore your controller configuration:

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **Import Settings** section and **Settings File Location**, click **Browse**.



4. A separate file navigation window should open.
5. Select the controller configuration file to restore and click **Import**. (Default Filename: *backup-TEW-WLC100-YYYY-MM-DD.tar.gz)*. If prompted, click **Yes** or **OK**.
6. Wait for the controller to restore settings.

Reboot your controller

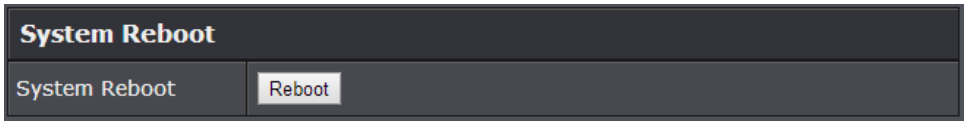
Advanced > Administrator > Settings Management

You may want to restart your controller if you are encountering difficulties with your controller and have attempted all other troubleshooting.

There are two methods that can be used to restart your controller.

- **Turn the controller** off for 10 seconds using the controller On/Off switch located on the rear panel of your controller or disconnecting the power port, see "Product Hardware Features" on page 2.
  Use this method if you are encountering difficulties with accessing your controller management page. This is also known as a hard reboot or power cycle.
  OR
- **Controller Management Page** – This is also known as a soft reboot or restart.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **System Reboot**, click **Reboot**.



4. Wait for the device to reboot.

Reset your controller to factory defaults

Advanced > Administrator > Settings Management

You may want to reset your controller to factory defaults if you are encountering difficulties with your controller and have attempted all other troubleshooting. Before you reset your controller to defaults, if possible, you should backup your controller configuration first, see "Backup and restore your controller configuration settings" on page 12.

There are two methods that can be used to reset your controller to factory defaults.

- **Reset Button** – Located on the rear panel of your controller, see "Product Hardware Features" on page 2. Use this method if you are encountering difficulties with accessing your controller management page.

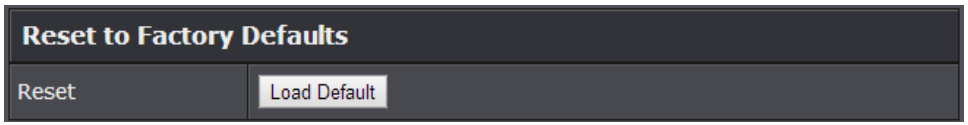
  OR

- **Controller Management Page**

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.

3. Next to **Reset to Factory Default Settings** and **Reset**, click **Load Default**. When prompted to confirm this action, click **OK**.



Controller Default Settings

Administrator User Name	admin
Administrator Password	admin
Controller IP Address	192.168.10.200
Controller Subnet Mask	255.255.255.0
Controller Default Gateway	192.168.10.1
Primary DNS Server	192.168.10.1

Set your controller date and time

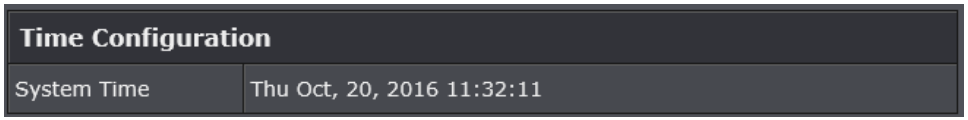
Advanced > Administrator > Time

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

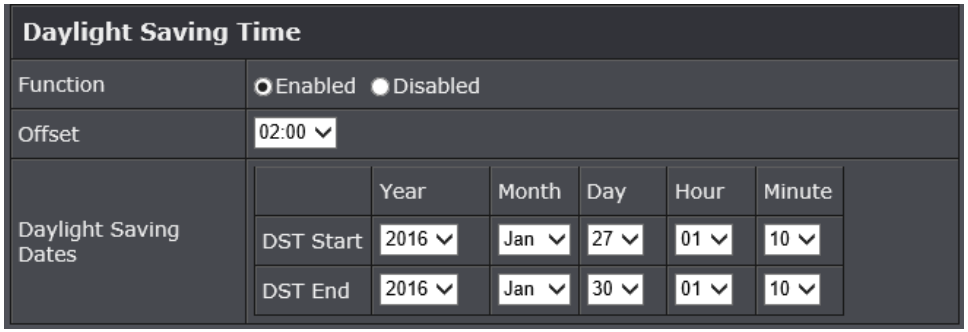
2. Click on **Advanced** and click on **Administrator**, then click **Time**.

3. Review the Time settings. To save changes to this section, click **Apply** when finished.

- **Time:** Displays the current device time and date information.

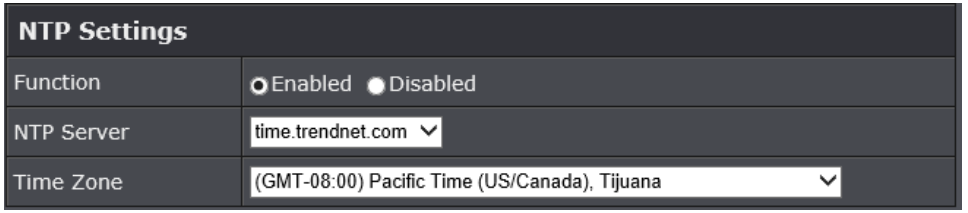


- **Enable Daylight Saving:** Check the option to enable daylight savings time and set the annual range when daylight saving is activated.



- **Automatically synchronize with Internet Time Server –** Check the **Enable NTP Server** option to set your controller date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to Default NTP server, (e.g. pool.ntp.org). Click the **Time Zone** drop-down list to select the appropriate zone and you can optionally change your NTP Sync period.

***Note**: NTP servers are used for computers and other network devices to synchronize time across an entire network.*



AP management and monitoring

AP Compatibility

Before you proceed, please ensure you are using one of the access point models in the list and the firmware version your access points has been upgraded accordingly to the versions indicated in the list below. Please reset all access point to the factory default configuration. Also, make sure your network is using a DHCP server to distribute IP addresses to the access points. By default, TRENDnet access point models listed below will obtain an IP address automatically through DHCP or otherwise default back to 192.168.10.100 / 255.255.255.0 if a DHCP server is not available on your network. Each access point must be assigned ma unique IP address on the same network.

Access Point Model	Description	Firmware Version
TEW-755AP	N300 PoE Access Point	1.02 or above
TEW-821DAP	AC1200 Dual Band PoE Access Point	1.04 or above

You can download the access point firmware from http://www.trendnet.com/support which include instructions on how to upgrade the firmware.

Discover and configure access points

Basic > AP Management > Device List

This section allows you to discover TRENDnet access points on your network, apply configuration settings, deploy batch firmware upgrades and deploy configuration to multiple access points simultaneously.

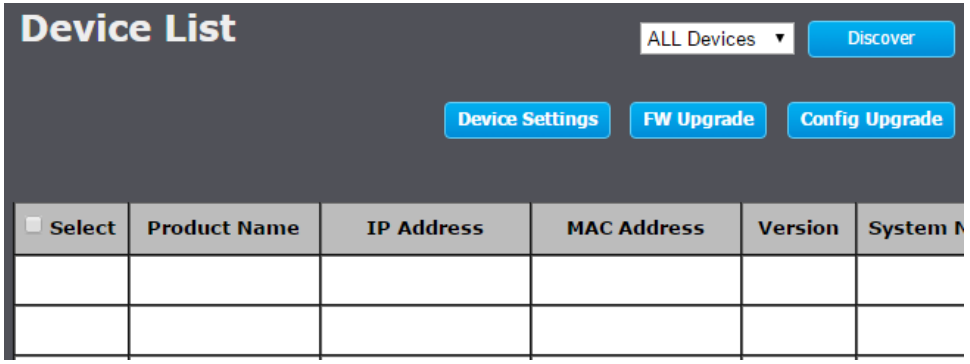
1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

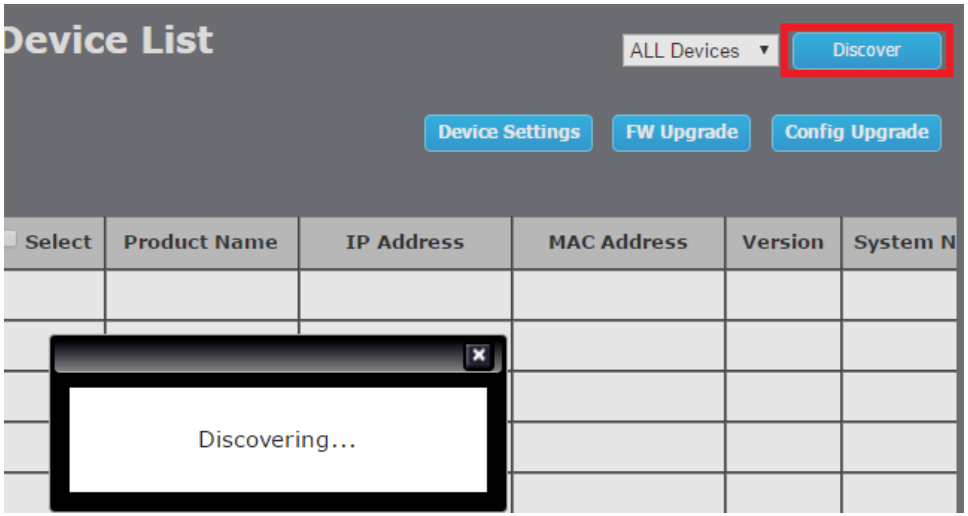
2. Click on **Basic**, click on **AP Management**, and then click on **Device List.**

3. Please review the functional descriptions below.

- **Discover** – Click Discover to discover all compatible TRENDnet access points on the network and automatically add them to the device list. The controller may also automatically detect access points without initiating this function manually.

  Note: The controller can only discover access points located within the same IP subnet.





Select	Product Name	IP Address	MAC Address
☐	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31
☐	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45

- **Device Settings** – First, under the **Select** column, check the access points you would like to configure and then click on Device Settings. A configuration window will appear with all of the available configurable access point settings.

Select	Product Name	IP Address
☑	TEW-821DAP	192.168.10.27

Device Settings

Important Note: *For any changes to be applied under device settings, you must enter the access point management password before clicking* ***OK*** *and applying the changes. By default, the compatibility TRENDnet access point user name and password is set to* ***admin / admin****.*

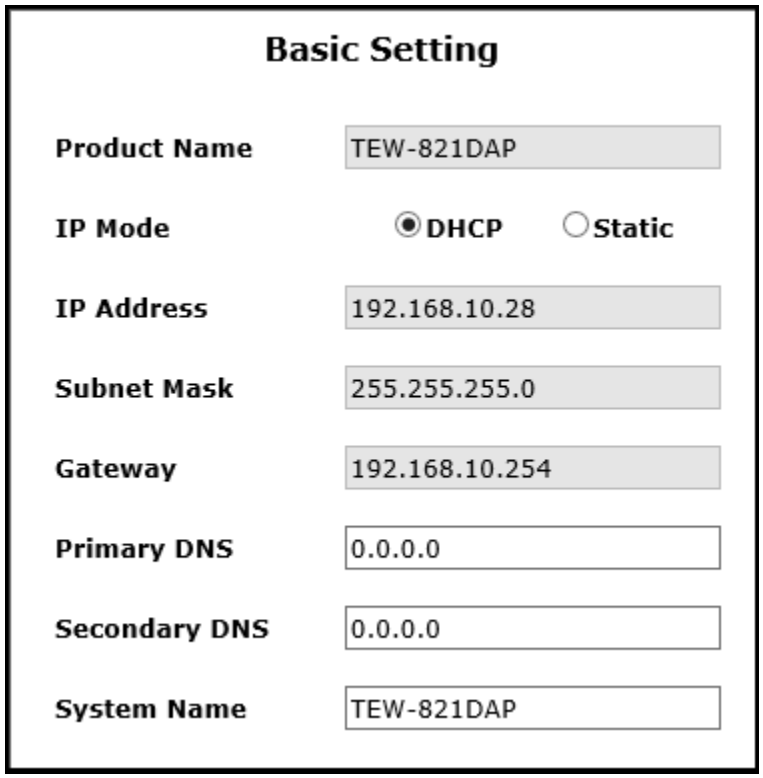
.

For usability with the wireless controller, it is recommended to change all of the access point management passwords to the same unique password. This allows the controller push out configuration to multiple access points simultaneously.

To change the access point management password, you must manually log into the access point management user interface and change each access point password. To easily access each access point management interface, you can simply click on the IP address link in the IP address field next to each access point which will automatically open up the access point management interface in a new browser tab or window.

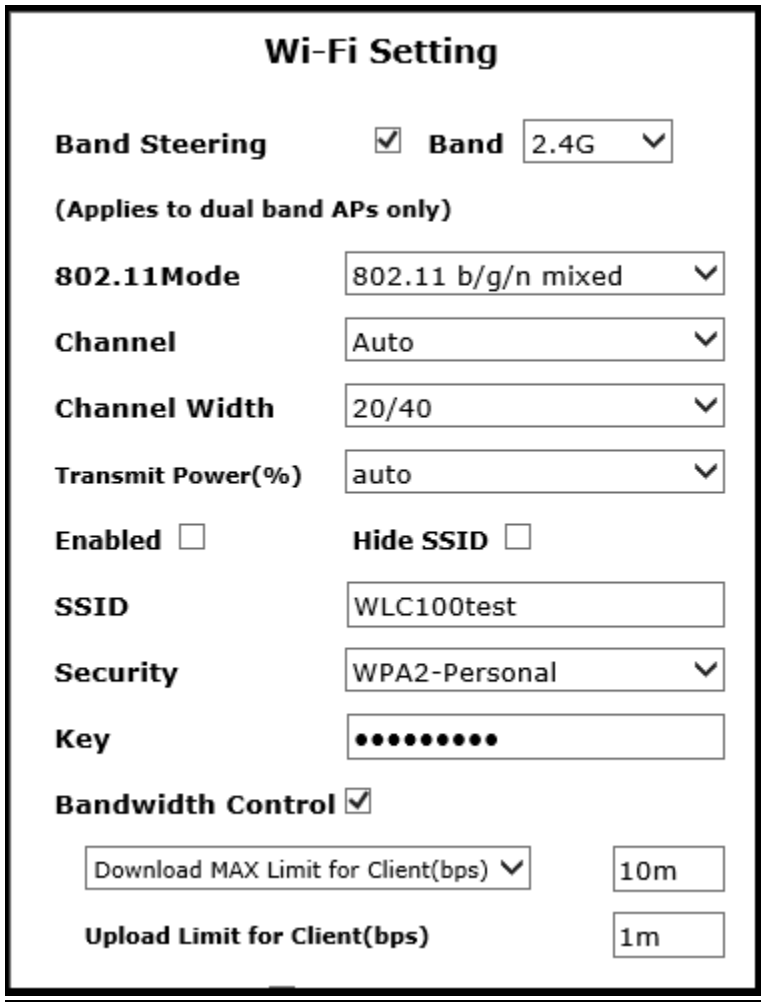
IP Address
192.168.10.27

Basic Settings



- **IP Mode –** Change the IPv4 address assignment type of the access point(s).
  - **DHCP** – Sets the access point(s) to obtain the IP address settings automatically from a DHCP server on your network. This is the default and recommended setting.
  - **Static –** Allows you to set the access point(s) IP address settings manually to specific parameters: **IP Address, Subnet Mask,** and **Gateway.**
- **Primary DNS –** Sets the access point(s) primary DNS server IPv4 address for name resolution.
- **Secondary DNS –** Sets the access point(s) secondary DNS server IPv4 address for name resolution.
- **System Name –** Sets the access point(s) device or network name.

Wi-Fi Settings



- **Band Steering –** Check to enable or uncheck to disable band steering functionality on the access point(s). When enabled, Band steering automatically detects if wireless clients have dual band capability and will automatically push wireless clients to the less congested 5GHz wireless network.

Note: *Applies only to TRENDnet dual band access point models: TEW-821DAP*

- **Band** – Click the drop-down list to select which band configuration parameters to configure, 2.4GHz or 5GHz.
  Note: *5GHz settings apply only to TRENDnet dual band access point models: TEW-821DAP)*
- **802.11 Mode –** Restricts wireless client connections to specified 802.11 standards only. The default and recommended mode is 802.11b/g/n and 802.11a/n/ac mixed modes. When applying the 802.11 Mode setting, please keep in mind the following:
  - Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
  - Wireless devices that support 802.11ac are backwards compatible and can connect wirelessly at 802.11n or 802.11a.
  - Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
  - Connecting at 802.11a or 802.11n will limit the capability of your 802.11ac supported wireless devices from obtaining higher performance and data rates.
  - Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
  - Allowing 802.11a or 802.11n devices to connect to an 802.11ac capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11ac.
  - Wireless devices that only support 802.11n or 802.11a will not be able to connect to a wireless network that is set to 802.11ac only mode.
  - Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
  - Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.
  - Wireless devices that only support 802.11a will not be able to connect to a wireless network that is set to 802.11n only mode.
- **Channel –** Selecting the Auto option will set your controller to scan for the appropriate wireless channel to use automatically. Click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks. The recommended and default setting is Auto.
- **Channel Width:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n and 802.11ac. For greater 802.11n performance, select **Auto 20/40MHz** (Options: 20MHz or Auto 20/40MHz). It is recommended to use the default channel bandwidth settings.
  For greater 802.11ac performance, select **Auto 20/40/80MHz** (Options: 20MHz, Auto 20/40MHz, Auto 20/40/80MHz). It is recommended to use the default channel width settings.
  Note: *Please note that the default settings may provide more stability than the higher channel bandwidth settings such as Auto* 20/40/80MHz *for connectivity in busy wireless environments where there are several wireless networks in the area.*
  - **20 MHz** – This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n on both 2.4GHz and 5GHz. This setting may provide more stability than 20/40MHz (Auto) for connectivity in busy wireless environments where there are several neighboring wireless networks in the area.
  - **Auto 20/40MHz (11n) or Auto 20/40/80MHz (11ac)** –When this setting is active, this mode is capable of providing higher performance only if the wireless devices support the channel width settings. Enabling Auto 20/40MHz or Auto 20/40/80 MHz typically results in substantial performance increases when connecting an 802.11ac/n wireless client.
- **Transmit Power % –** This setting allows you to adjust the wireless transmit power to a lower setting. In busy wireless environments, lowering the transmit power may improve better performance and connectivity and decrease interference with neighboring wireless networks. It is recommended to keep the default transmit power settings.

- **Enabled –** This setting allows you to enable or disable the wireless radio on the selected band. If checked, this will enable the wireless radio and if unchecked will disable the wireless radio.
- **Hide SSID –** This setting allows you to enable or disable the primary SSID broadcast on the selected band. If unchecked, the SSID broadcast is enabled, if checked the SSID broadcast will be disabled. This setting does not disable the wireless radio, only hides the SSID/wireless network name visibility and prevents client devices from easily discovering the AP.
- **SSID –** This setting allows you to change the primary SSID/wireless network name on the selected band.
- **Security** – This setting allows you to set the wireless encryption type for the primary SSID/wireless network name for the selected band.

If choosing WEP, WPA/WPA2-Personal:

- **Key -** For WEP security, enter the encryption key to assign in this field. For WPA-Personal or WPA2-Personal security, enter the passphrase in this field.
  Note: *The WEP key index is Index 1.*
- This is the password or key that is used to connect your computer to this access points wirelessly.

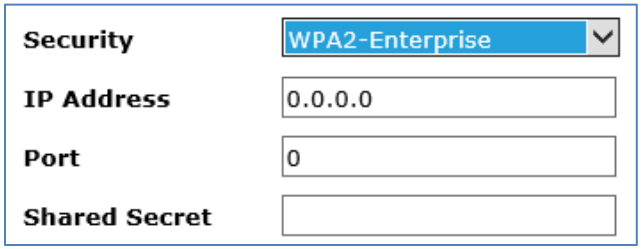
WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,C,?,*, /,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

WPA/WPA2-Personal Passphrase Format: *8-63 alphanumeric characters (a,b,C,?,*, /,1,2, etc.)*

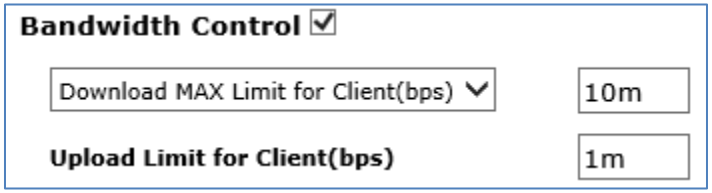
If choosing WPA/WPA2-Enterprise:

Note: *This security type requires an external RADIUS server which requires more complex security configuration.*

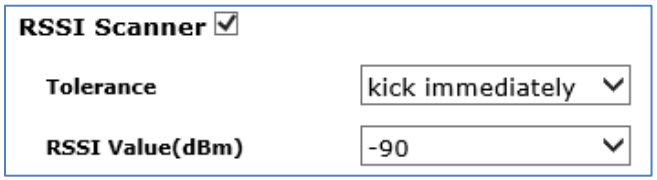
- **IP Address:** Enter the IP address of the RADIUS server. *(e.g. 192.168.10.250)*
- **Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
- ***Note:*** *It is recommended to use port 1812 which is typical default RADIUS port.*
- **Shared Secret:** Enter the shared secret used to authorize your controller with your RADIUS server.



- **Bandwidth Control** – This setting allows you to set the maximum download and upload rate limits per client for the primary SSID in bits per second (bps). Add "m" to the end of the value to indicate megabits per second (Mbps) or add "k" to the end of the value to indicate kilobits per second. Check the option to enable the feature and uncheck to disable.



- **RSSI Scanner** – This setting allows you to set the maximum RSSI value or reception connection strength of client device detected by the AP and the action/tolerance. The lower the value, the less connection strength the client device has with the access point (ex. a client device with a -90dBm RSSI has lower quality connection and signal strength to the access point than another client device with -60dBm RSSI). Once the set RSSI value is detected for a specific client device, the action/tolerance can be set whether to disconnect or kick the client immediately or wait a specified amount of time before disconnecting the client device. This setting can be used benefit wireless roaming for client devices.
  Note: *In a wireless environment with multiple wireless access points, this setting can be particularly useful by forcing client devices disconnect and move/roam to an access point where signal strength is much higher than the original access point due to the change in the client(s) mobility and location. The typical behavior of wireless client devices is to remain connected to the same access point as long as the signal is detected which can result in poor connectivity when the client changes is location or position. This feature can benefit the client device connection quality when changing position or location and help maintain the client device is connected to the strongest signal access point relative to it's position whenever possible.*



- **802.11k** – This setting allows you to enable or disable 802.11k. 802.11k is an provides assisted roaming capability for 802.11k capable client devices only to request neighbor reports about known neighboring access points. This can help client device limit or eliminate the need for additional scanning and determine which is the next best neighboring access point to connect to relative to it's position or location and help with efficient use of access point utilization by determine client load capacity.

How to choose the type of security for your wireless network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new controller.

There are a few different wireless security types supported in wireless networking each having its own characteristics which may be more suitable for your wireless network taking into consideration compatibility, performance, as well as the security strength along with using older wireless networking hardware (also called legacy hardware).

It is strongly recommended to enable wireless security to prevent unwanted users from accessing your network and network resources (personal documents, media, etc.).

In general, it is recommended that you choose the security type with the highest strength and performance supported by the wireless computers and devices in your network. Please review the security types to determine which one you should use for your network.

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 b or 802.11g wireless adapters or computers with old embedded wireless cards(wireless clients), you may have to set your access point to WEP to allow the old adapters to connect to the access point.
  Note: *This encryption standard will limit connection speeds to 54Mbps.*
- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
  - **WPA-**Auto: This setting provides the access point with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption.
    Note: *WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps*

- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your access point to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your access point to either WPA or WPA-Auto encryption.
  Note: *Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported. Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.*

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n/ac
Highest Performance Under This Setting	**Up to 54Mbps**	**Up to 54Mbps**	**Up to 800Mbps (11n) or 1.7 Gbps (11ac) or max. 11n & 11ac data rates.**
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, 450Mbps, 600Mbps, 800Mbps) or maximum 802.11ac data rate supported by the device (433Mbps, 867Mbps, 1.3Gbps, 1.7Gbps).

Batch configuration upload and firmware upgrade

Batch Configuration Deployment

Basic > AP Management > Device List

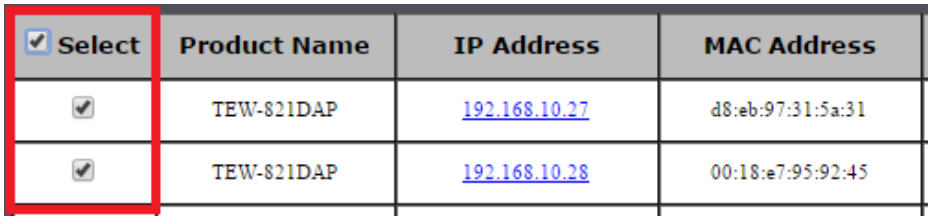
The controller allows you to upload access point configuration to multiple wireless access points from a single backed up configuration file. This feature can simplify deployment and configuration of multiple wireless access points. The configuration file must be backed up from one of the wireless access points directly. On TRENDnet compatible access points you can back up the access point configuration on the Management > Backup/Restore Settings under Export Settings. Create and save the encryption key to secure the backup configuration file and click Export (default filename: TRENDnet EAP_config.bin)

Batch configuration deployment can only be applied to the same model TRENDnet access point. (ex. If using a configuration file exported from a TRENDnet TEW-821DAP, the configuration can only be deployed to multiple TEW-821DAP access points only.)

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Basic**, click on **AP Management**, and then click on **Device List.**

3. In the device list under the **Select** column, check the access points you would like to deploy configuration. You can also check the box at the top of the **Select** column to select all access points in the list.



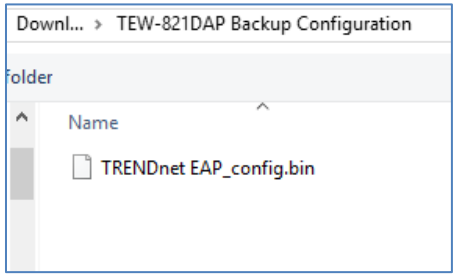
4. At the top, click on **Config Upgrade**.

5. The list will display all of the access points you have selected and the configuration upload status of each access point.

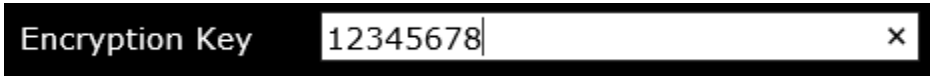
Index	Product Name	IP Address	MAC Address	Firmware Version	Status
1	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31	1.04b06	
2	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45	1.04b06	

6. Next to **Config Path**, click on **Browse** or **Choose File**, and navigate to the previously backed up configuration file to upload and select it.

Note: *Default backup configuration filename for TRENDnet access points is TRENDnet EAP_config.bin. The file should have a .bin extension.*



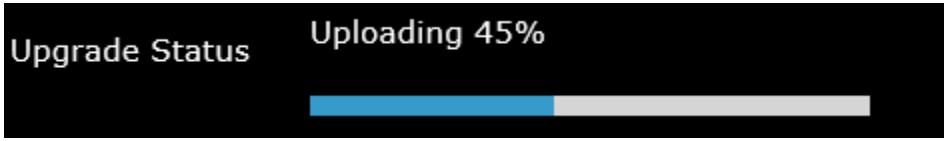
7. After selecting the configuration file, for **Encryption Key**, enter the you assigned previously when exporting settings from the access point (default: 12345678).



8. Enter the administrative management password for the access points, (default TRENDnet access point password: admin) in the **Password** field.

9. Click **Upgrade** to start the batch configuration deployment. Please wait for the batch configuration deployment process to complete.

Note: *The Upgrade Status bar will indicate the progress % and list under Status field for each device will indicate also indicate the status of each access point. Do not close the window until the process has been full completed.*



Index	Product Name	IP Address	MAC Address	Firmware Version	Status
1	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31	1.04b06	Processing
2	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45	1.04b06	

Note: *When the all of the access points display a status report, the process is completed. A success message indicated that the process was successfully completed. After the process is complete you can close this window.*

Index	Product Name	IP Address	MAC Address	Firmware Version	Status
1	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31	1.04b06	Success
2	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45	1.04b06	Success

Batch Firmware Upgrade Deployment

Basic > AP Management > Device List

The controller allows you to upgrade firmware on multiple access points. Firmware upgrades for the access points can be downloaded from the TRENDnet support site http://www.trendnet.com/support and selecting the access point model under Product Downloads. Batch firmware upgrade can only be applied to the same model TRENDnet access point. (ex. If upgrading firmware for the TRENDnet TEW-821DAP, the firmware upgrade can only be deployed to multiple TEW-821DAP access points only.)

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Basic**, click on **AP Management**, and then click on **Device List.**

3. In the device list under the **Select** column, check the access points you would like to deploy configuration. You can also check the box at the top of the **Select** column to select all access points in the list.

Select	Product Name	IP Address	MAC Address
☑	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31
☑	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45

4. At the top, click on **FW Upgrade**.

5. The list will display all of the access points you have selected and the configuration upload status of each access point.

Index	Product Name	IP Address	MAC Address	Firmware Version	Status
1	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31	1.04b06	
2	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45	1.04b06	

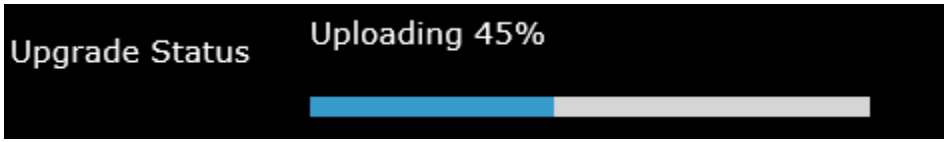
6. Next to **Firmware Path**, click on **Browse** or **Choose File**, and navigate to the unzipped firmware file to upload and select it.

Note: *Please make sure to unzip or extract the downloaded firmware file. The firmware file should have a .bin extension.*

7. After selecting the firmware file to deploy, enter the administrative management password for the access points, (default TRENDnet access point password: admin) in the **Password** field.

8. Click **Upgrade** to start the firmware upgrade deployment. Please wait for the firmware upgrade deployment process to complete.

Note: *The Upgrade Status bar will indicate the progress % and list under Status field for each device will indicate also indicate the status of each access point. Do not close the window until the process has been full completed.*



Index	Product Name	IP Address	MAC Address	Firmware Version	Status
1	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31	1.04b06	Processing
2	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45	1.04b06	

Note: *When the all of the access points display a status report, the process is completed. A success message indicated that the process was successfully completed. After the process is complete you can close this window. You can also verify that the new firmware version has been upgraded listed in the Firmware Version column.*

Index	Product Name	IP Address	MAC Address	Firmware Version	Status
1	TEW-821DAP	192.168.10.27	d8:eb:97:31:5a:31	1.04b06	Success
2	TEW-821DAP	192.168.10.28	00:18:e7:95:92:45	1.04b06	Success

AP and client status monitoring

Access Point List

Basic > AP Management > Access Points

The controller displays a status of all the SSIDs on each band for all access points. For example, for a dual band access point such as the AC1200 TEW-821DAP, at default two entries will be listed in the access point list, one primary SSID for 5GHz and another primary SSID for 2.4GHz. If multiple SSIDs are enabled for each access point, they will appear in the list.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Basic**, click on **AP Management**, and then click on **Access Points.**

- **System Name** – Displays the identifying system name of each access point associated with each SSID/wireless network.
- **BSSID** – Displays the wireless MAC address interface of each access point associated with each SSID/wireless network.
- **IP Address –** Displays the currently assigned IP address of each access point associated with each SSID/wireless network.
- **Model Name –** Displays the model name of the access point associated with each SSID/wireless network.
- **Firmware Version** – Displays the current firmware version of the access point associated with each SSID/wireless network.
- **Status –** Displays the status of the access point associated with each with each SSID/wireless network.
- **SSID** – Displays the SSID/wireless network name.
- **Channel** – Displays the current operating wireless channel of the access point associated with each SSID/wireless network.
- **Total Clients –** Displays the total of currently connected wireless client devices connected to each access point associated with each SSID/wireless network.
- **Upload (Mbytes)** – Displays the total amount of bandwidth currently being transmitted by the access point for each wireless network in megabytes (MB).
- **Download (Mbytes)** – Displays the total amount of bandwidth currently being received by the access point for each wireless network in megabytes (MB).

System Name	BSSID	IP Address	Model Name
TEW-821DAP	D8:EB:97:31:5A:31	192.168.10.27	TEW-821DAP
TEW-821DAP	D8:EB:97:31:5A:32	192.168.10.27	TEW-821DAP
TEW-821DAP	00:18:E7:95:92:45	192.168.10.28	TEW-821DAP
TEW-821DAP	00:18:E7:95:92:46	192.168.10.28	TEW-821DAP

Firmware Version	Status	SSID	Channel
1.04b06	Ready	TRENDnet821_2.4GHz_AXZD	1
1.04b06	Ready	TRENDnet821_5GHz_AXZD	36
1.04b06	Ready	TRENDnet821_2.4GHz_0045	6
1.04b06	Ready	TRENDnet821_5GHz_0045	36

Total Clients	Upload (MBytes)	Download (MBytes)
0	0.02	0.02
0	0.00	0.00
0	0.03	0.02
0	0.00	0.00

Clients List

Basic > AP Management > Clients

The controller displays a list of a currently connected wireless client devices to all access points.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Basic**, click on **AP Management**, and then click on **Clients.**

- **MAC** – Displays the client device MAC address.
- **BSSID** – Displays the SSID/wireless network the client device is currently connected.
- **Signal Strength** – Displays the signal strength reception (dBm) or RSSI of the client device to the connected access point and 802.11 capability of the client device. (ex. A signal strength reception of -41dBm is better than -48dBm)
- **Uptime –** Displays the total amount of time the client device has been connected. If a client device disconnects and reconnects from the wireless network, the uptime will reset to zero.

MAC	WLAN(SSID)
d8:eb:97:25:65:bb	WLC100test
9c:f4:8e:07:11:00	WLC100test

Signal strength(dBm)	Uptime
-41(11anac)	0h1m51s
-48(11anac)	0h2m24s

Client Traffic Statistics

Basic > AP Management > Statistics

The controller displays more detailed information about wireless client devices traffic utilization on all access points.

1. Log into your controller management page (see "Access you wireless controller management page" on page 8).

2. Click on **Basic**, click on **AP Management**, and then click on **Statistics.**

Technical Specifications

Standards

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab

Device Interface

- 5 x Gigabit ports
- 1 x USB port
- On/Off Power button
- LED indicators
- Reset button

Data Transfer Rate

- Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)
- Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)
- Gigabit Ethernet: 2000 Mbps (full duplex)

Management

- HTTP Web based GUI
- Local or online Firmware upgrade
- Internal log
- Configuration Backup/Restore
- NTP

Access Point Management

- Manage up to 32 access points
- IP address, gateway, and DNS settings
- SSID/Network name
- Wireless channel
- Wireless encryption: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise 802.1X
- 802.11 mode
- Channel width
- Transmit power
- SSID broadcast
- Bandwidth control (download limit per SSID & client, upload limit per client)
- Set RSSI scanning/threshold
- Enable/disable 802.11k radio resource management
- Enable/disable Band steering
- Access point/client statistics monitoring
- Batch configuration deployment
- Batch firmware upgrade deployment

Access Point Compatibility

- TEW-755AP (Firmware Version: 1.02 or above)
- TEW-821DAP (Firmware Version: 1.04 or above)

Power

- Input: 100 – 240 V AC, 50/60 Hz
- Output: 12V DC, 1A external power adapter
- Consumption: 12W (max.)

Operating Temperature

- 0 – 40°C (32 – 104°F)

Operating Humidity

- Max. 90% non-condensing

Dimensions

- 215 x 130 x 44.45 mm (8.27 x 6.3 x 1.73 in.)
- Rack mountable 1U height

Weight

- 68 g (1.5 lbs.)

Certifications

- CE
- FCC

Troubleshooting

Q: I typed http://192.168.10.200 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the controller management page?
Answer:
1. Check your hardware settings again. See "Access point Installation" on page 8.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Use the following IP address* or *Static IP*(see the steps below).
4. Make sure your computer is connected to one of the Ethernet controller ports.
5. Since the controller default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

Windows 7/8.1/10

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: If my controller IP address is different than my network's subnet, what should I do?
Answer:
You should still configure the controller first. After all the settings are applied, go to the controller configuration page, click on System, click IPv4 Setup and change the IP address of the controller to be within your network's IP subnet. Click Apply, then click OK. Then click Save Settings to Flash (menu) and click Save Settings to Flash to save the IP settings to the NV-RAM.

Q: I changed the IP address of the controller, but I forgot it. How do I reset my controller?
Answer:
Using a paper clip, push and hold the reset button on the front of the controller and release after 15 seconds.
The default IP address of the controller is 192.168.10.200. The default user name and password is "admin".

Appendix

How to find your IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Command Prompt Method

Windows 2000/XP/Vista/7/8.1/10

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type ***cmd*** to bring up the command prompt.
3. In the command prompt, type ***ipconfig /all*** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type ***ipconfig getifaddr <en0 or en1>*** to display the wired or wireless IP address settings.

Note: en0 *is typically the wired Ethernet and* ***en1*** *is typically the wireless Airport interface.*

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to configure your network settings to use a static IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Windows 7/8.1/10

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.

b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.

c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon

b. Right-click the **Local Area Connection** icon and the click **Properties**.

c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.

b. Click the **Network** icon.

c. From the **Location** drop-down list, select **Automatic**.

d. Select and view your Ethernet connection.

In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

e. Configure TCP/IP to use a static IP.
In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Manually** and assign your network adapter a static IP address. Then click the **Apply Now** button.
In MAC 10.5/10.6, from the **Configure** drop-down list, select **Manually** and assign your network adapter a static IP address . Then click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7/8.1/10,

Your computer MAC addresses are also displayed in this window, however, you can type ***getmac –v*** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

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:

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.

Country Code selection feature to be disabled for products marketed to the US/CANADA

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

- **EN60950-1 : 2006 + A11 : 2010 + A12: 2011 + A2: 2013**
- **EN 55022: 2010 + AC: 2011**
- **EN 55024: 2010 + A1: 2015**
- **EN 55032: 2015**

Directives:

Low Voltage Directive 2014/35/EC
EMC Directive 2014/30/EC
RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
REACH Regulation (EC) No. 1907/2006
R&TTE Directive 1999/5/EC
Ecodesign Directive 2009/125/EC

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

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, or (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. International customers

shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

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, NEGLECT, 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").

Visit http://www.trendnet.com/gpl or the support section on http://www.trendnet.com and search 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 visit http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP07172015v3 2016/10/28

TRENDnet®

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