

Access Point

APAC1200

Product Information.....	2
Package Contents	2
Hardware Overview	3
LED Status.....	3
<i>Quick Installatin Guide</i>	4
Mounting the access point to a ceiling.....	7
Browser Based Configuration Interface	11
System Information.....	11
Wireless Clients	15
Wireless Monitor	17
Log	19
Network Settings.....	21
LAN-Side IP Address.....	21
LAN Port	23
VLAN	24
Wireless Settings	25
2.4GHz(5GHz).....	25
Basic.....	25
Advanced.....	27
Security.....	30
No Authentication	31
WEP.....	32
IEEE802.1x/EAP.....	32
WPA-PSK	32
WPA-EAP	33
Additional Authentication	33
WDS	35
WPS.....	37
RADIUS	39
RADIUS Settings	40
Internal Server	42
RADIUS Accounts	44
MAC Filter.....	46
WMM	48
Management.....	50
Admin.....	50
Date and Time	53

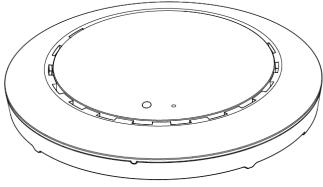
Syslog Server	55
Find Me.....	56
Advanced.....	57
LED Settings.....	57
Update Firmware	58
Save/Restore Settings	59
Factory Default	61
Reboot	62
Reset	62

Appendix.....63

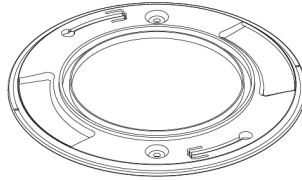
Configuring your IP address	63
Windows XP	64
Windows Vista	66
Windows 7	68
Windows 8	72
Mac	76
Hardware Specification.....	78
ENVIRONMENT & PHYSICAL	78
Safety Information.....	78

Product Information

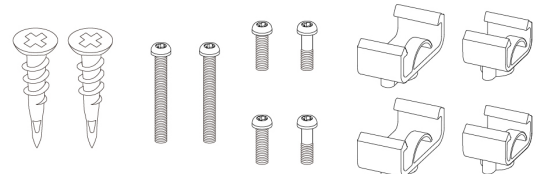
Package Contents



1



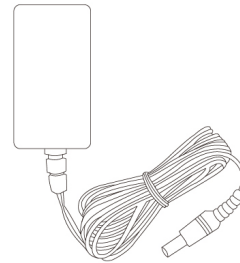
2



3



4



5

1. Access Point

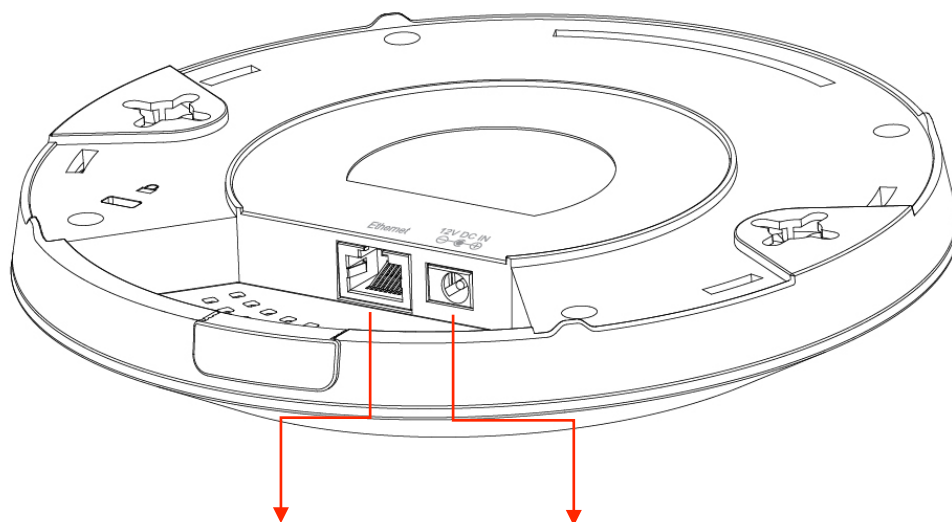
2. Ceiling Mount Bracket

3. Mounting Kit

4. Quick Installation Guide

5. Power Adapter

Hardware Overview



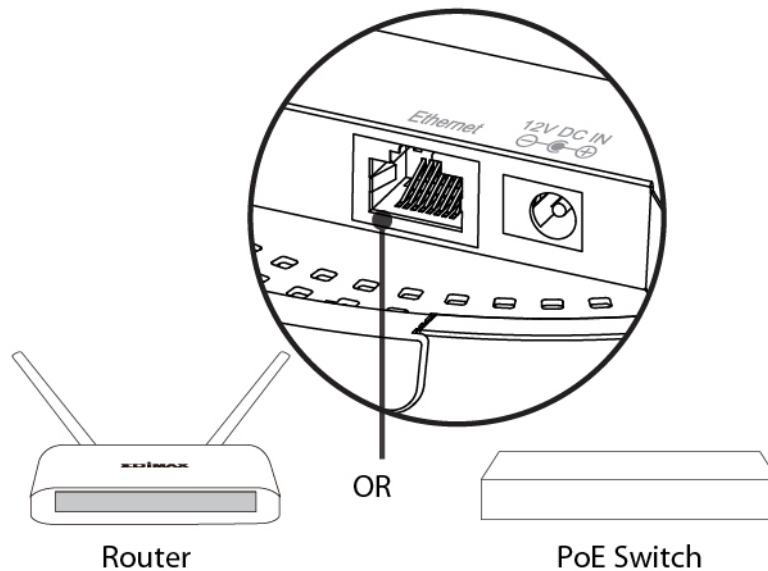
Ethernet Port Power Jack (DC)

LED Status

LED Color	LED Status	Description
Blue	On	The access point is starting up.
Purple	On	The access point is on.
Amber	Flashing	Error.
Off	Off	The access point is off.

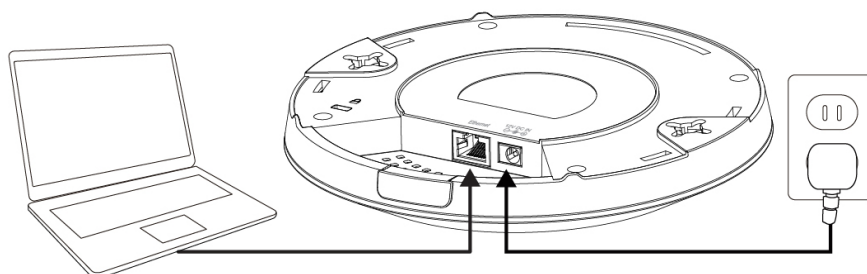
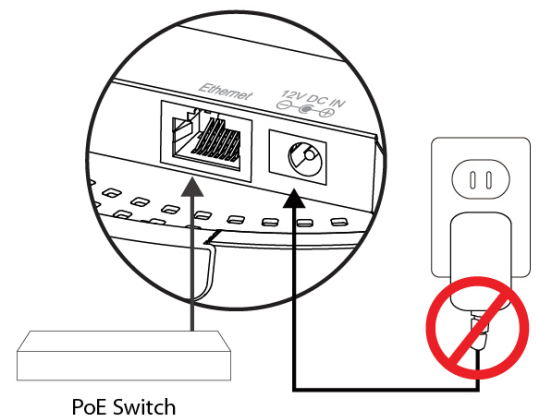
Quick Installatin Guide

1. Connect a router or PoE switch to the access point's **LAN** port using an Ethernet cable.



2. If you are using a router, then connect the power adapter to the access point's 12V DC port and plug the power adapter into a power supply.

3. If you are using a PoE (Power over Ethernet) switch then it is not necessary to use the included power adapter, the access point will be powered by the PoE switch.



4. Set your computer's IP address to **192.168.2.x** where **x** is a number in the range **2 – 254**.
5. Enter the access point's default IP address **192.168.2.1** into the URL bar of a web browser.



6. You will be prompted for a username and password. The default username is **“admin”** and the default password is **“admin”**, it is recommended that you change the password.
7. To change the SSID of your access point's wireless network(s), go to **“Wireless Setting” > “2.4GHz or 5GHz” > “Basic”**. Enter the new SSID for wireless network in the **“SSID”** field and click **“Apply”**.

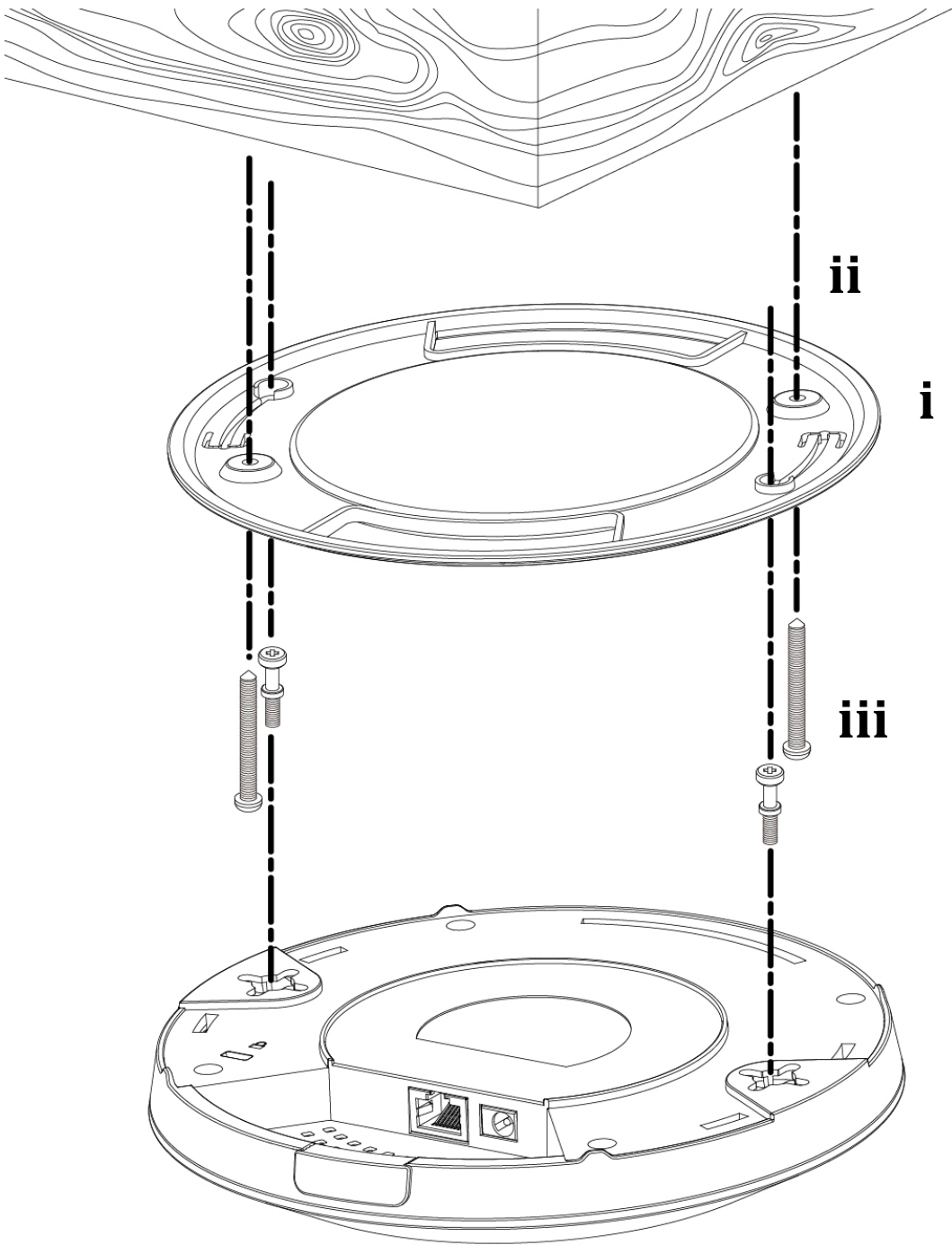
2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n
Enable SSID number	1
SSID1	CAP1200-CCDD10_G VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11
Auto Channel Interval	One day <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto
BSS BasicRateSet	1,2,5.5,11 Mbps

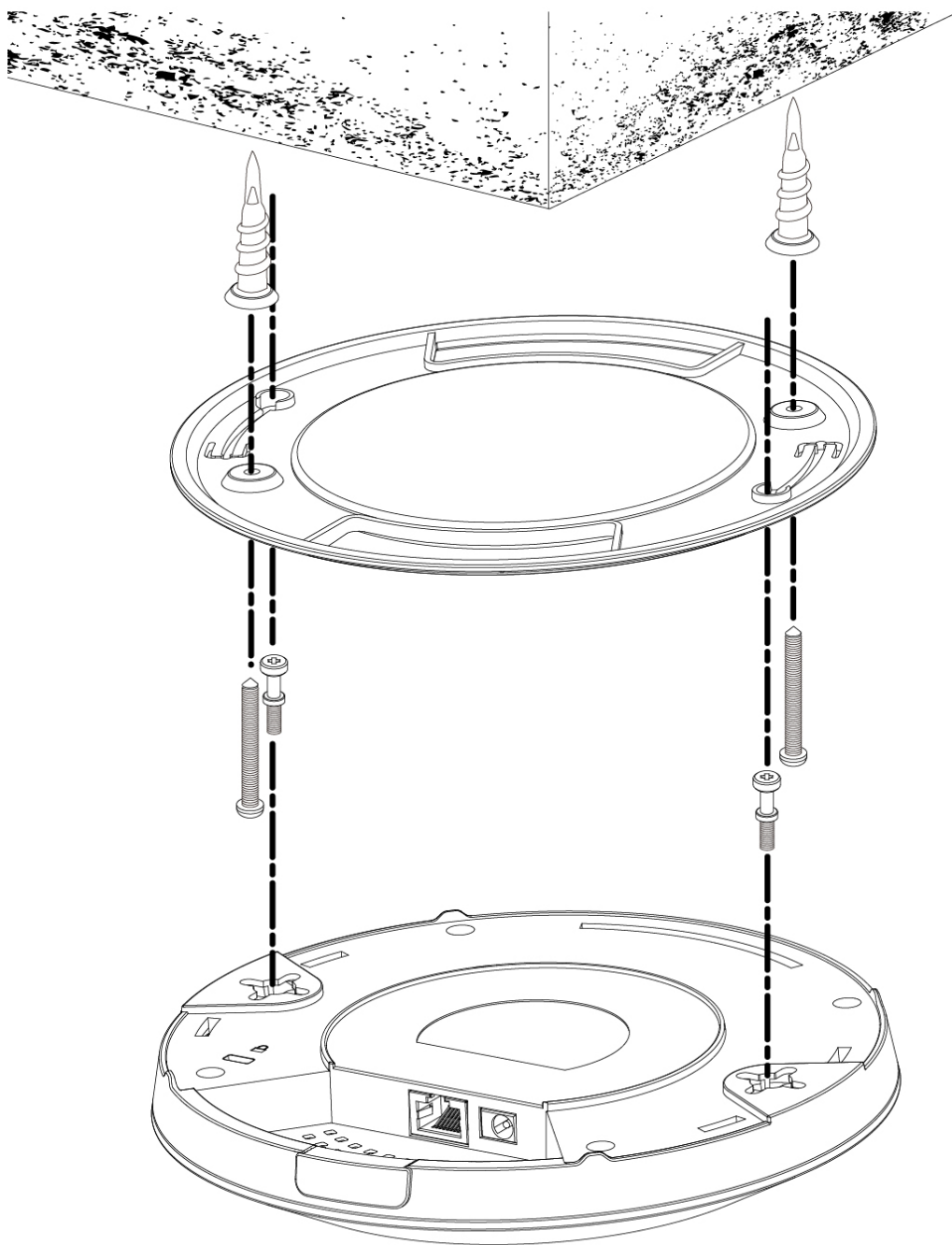
8. To configure the security of your access point's wireless network(s), go to **“Wireless Setting” > “2.4GHz or 5GHz” > “Security”**.

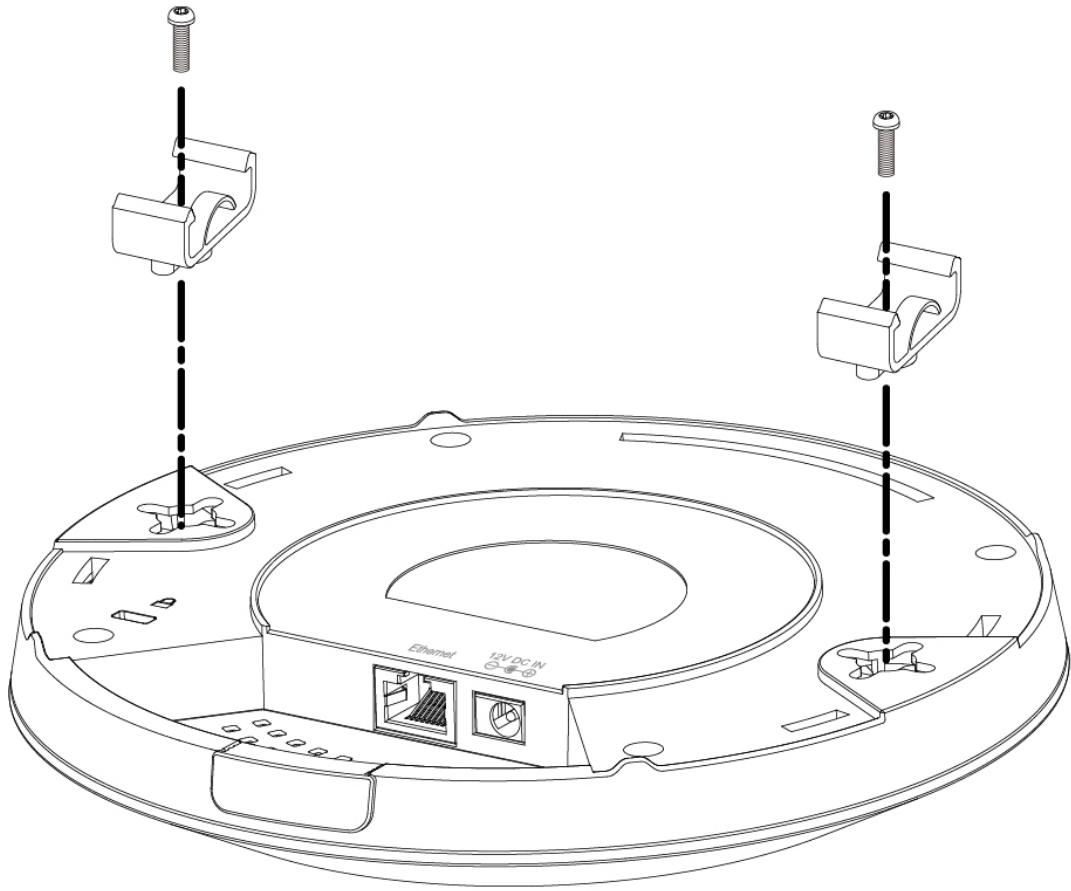
Select an “Authentication Method” and enter a “Pre-shared Key” or “Encryption Key” depending on your choice, then click “Apply”.

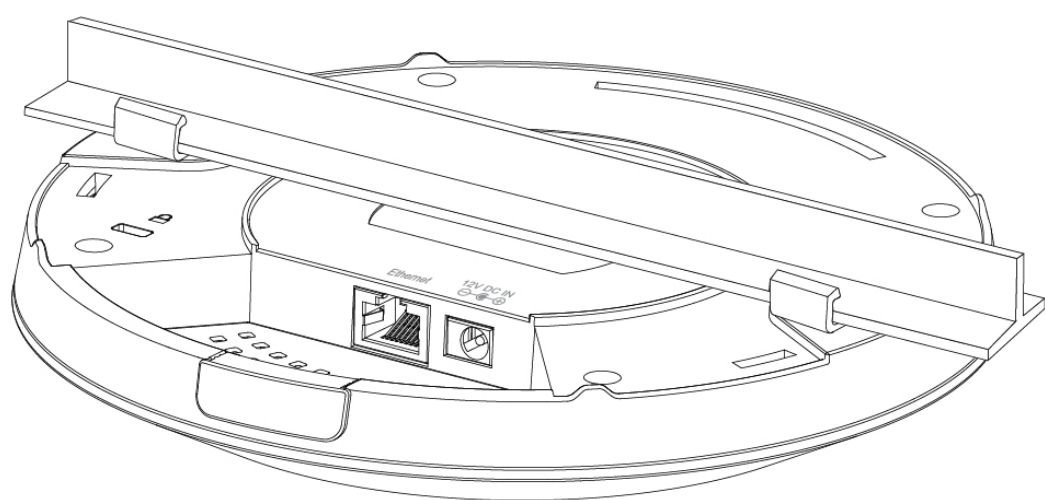
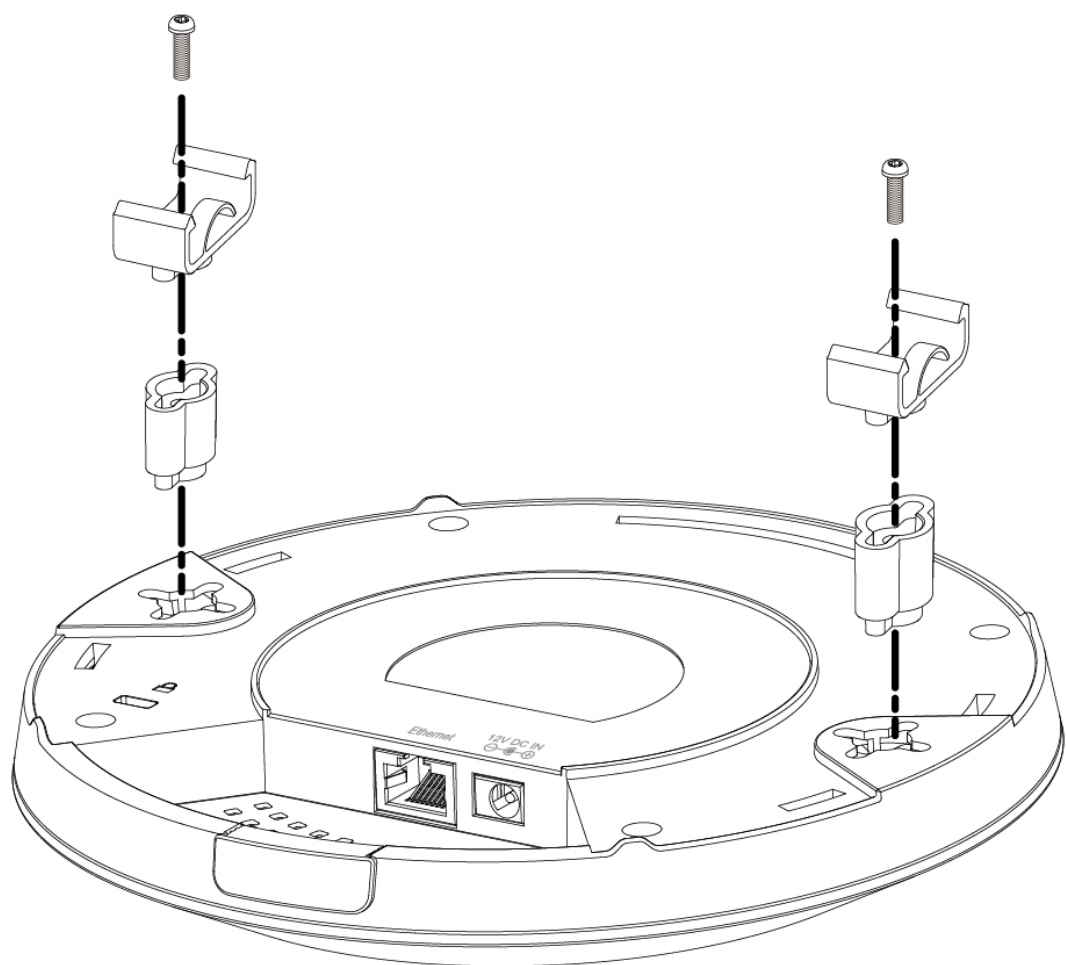
2.4GHz Wireless Security Settings	
SSID	CAP1200-CCDD10_G ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 /50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

Mounting the access point to a ceiling









Browser Based Configuration Interface

1. Enter your access point's IP address in the URL bar of a web browser. The access point's default IP address is **192.168.2.1**.
2. You will be prompted for a username and password. The default username is "**admin**" and the default password is "**admin**", it is recommended that you change the password during setup

System Information

The "System Information" page displays basic system information about the access point.

System	
Model	CAP1200
Product Name	AP801F0275EA6E
Uptime	0 day 00:12:57
Boot from	Internal memory
Version	0.0.5
MAC Address	80:1F:02:75:EA:6E
Management VLAN ID	1
IP Address	192.168.2.2
Default Gateway	---
DNS	---
DHCP Server	---

Wired LAN Port Settings

Wired LAN Port	Status	VLAN Mode/ID
Wired Port (#1)	Connected (100 Mbps Full-Duplex)	Untagged Port / 1

Wireless 2.4GHz

Status	Enabled
MAC Address	00:AA:BB:CC:DD:10
Channel	Ch 4 + 8 (Auto)
Transmit Power	100%

Wireless 2.4GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
CAP1200-CCDD10_G	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Wireless 5GHz

Status	Enabled
MAC Address	00:AA:BB:CC:DD:11
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100%

Wireless 5GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
CAP1200-CCDD10_A	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 5GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Refresh

System	
Model	Displays the model number of the access point.
Product Name	Displays the product name for reference, which consists of “AP” plus the MAC address.
Uptime	Displays the total time since the device was turned on.
Boot From	Displays information for the booted hardware.
Version	Displays the firmware version.
MAC Address	Displays the access point’s MAC address.
Management VLAN ID	Displays the management VLAN ID.
IP Address	Displays the IP address of this device. Click “Refresh” to update this value.
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of DNS (Domain Name Server).
DHCP Server	IP address of DHCP Server.

Wired LAN Port Settings	
Wired LAN Port	Specifies which LAN port.
Status	Displays the status of the LAN port (connected or disconnected).
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the LAN port.

Wireless 2.4GHz (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the access point’s MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmit power level as a percentage.

Wireless 2.4GHz (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID.
Encryption Type	Displays the encryption type for the specified SSID. See
VLAN ID	Displays the VLAN ID for the specified SSID.
Additional Authentication	Displays the additional authentication type for the specified SSID.
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID.

Wireless 2.4GHz (5GHz) / WDS Status	
MAC Address	Displays the peer access point's MAC address.
Encryption Type	Displays the encryption type for the specified WDS.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS.

Refresh	Click to refresh all information.
----------------	-----------------------------------

Wireless Clients

The “Wireless Clients” page displays information about all wireless clients connected to the access point on the 2.4GHz or 5GHz frequency.

Refresh time

Auto Refresh time

☒ 5 seconds
 ☐ 1 second
 ☐ Disable

Manual Refresh

Refresh

2.4GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time
1	CAP1200-CCDD10_G	F8:A9:D0:0B:7D:A8	0 Bytes	1.8 KBytes	100	25 secs	3

5GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time
No wireless client							

Refresh time	
Auto Refresh Time	Select a time interval for the client table list to automatically refresh.
Manual Refresh	Click refresh to manually refresh the client table.

2.4GHz (5GHz) WLAN Client Table	
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays the wireless signal strength for

	the specified client.
Connected Time	Displays the total time the wireless client has been connected to the access point.
Idle Time	Client idle time is the time for which the client has not transmitted any data packets i.e. is idle.
Vendor	The vendor of the client's wireless adapter is displayed here.

Wireless Monitor

Wireless Monitor is a tool built into the access point to scan and monitor the surrounding wireless environment. Select a frequency and click “Scan” to display a list of all SSIDs within range along with relevant details for each SSID.

Wireless Monitor

Site Survey

☒ Wireless 2.4G/ 5G
 ☐ 2.4G
 ☐ 5G
 Scan

Channel Survey result

Export

Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
1	Matt	00:E0:4C:81:96:C1	WPA2PSK/AES	100	11b/g/n	REALTEK SEMICONDUCTOR CORP.

Wireless 5GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

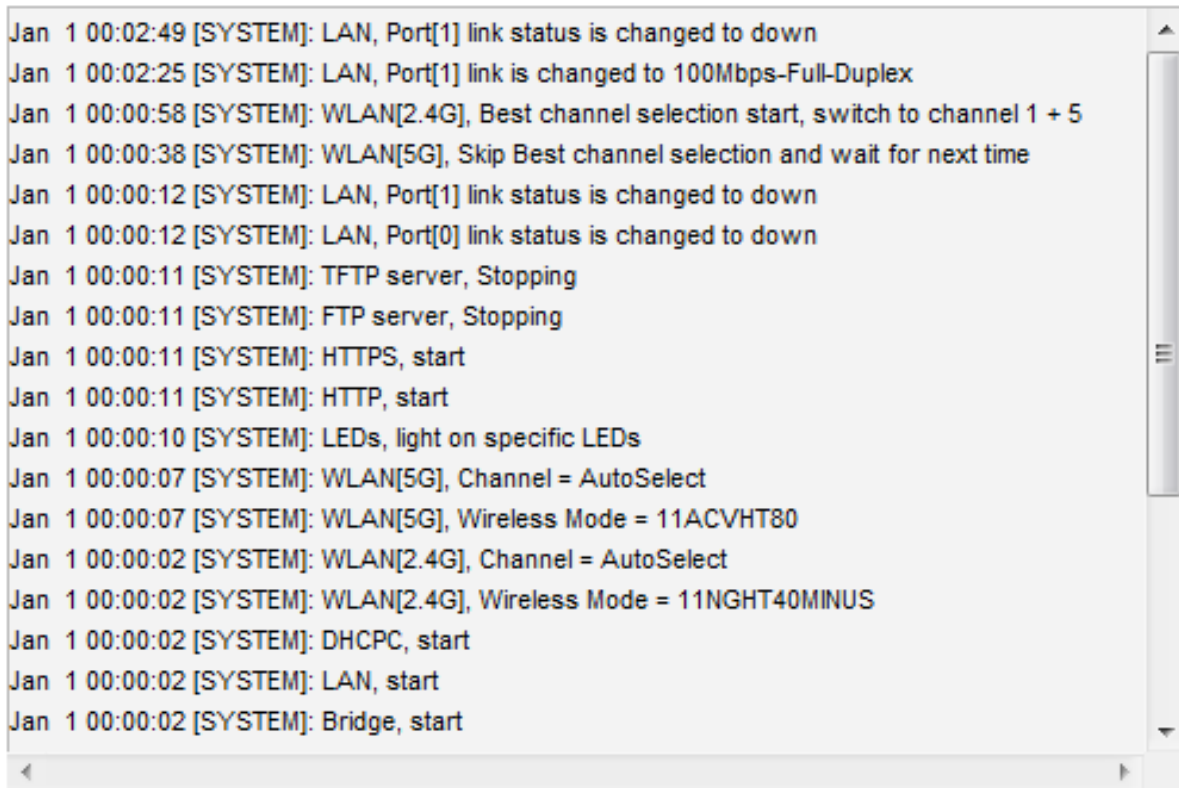
Wireless Monitor	
Site Survey	Select which frequency (or both) to scan, and click “Scan” to begin.
Channel Survey Result	After a scan is complete, click “Export” to save the results to local storage.

Site Survey Results	
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/access point for the specified SSID.
Security	Displays the authentication/encryption

	type of the specified SSID.
Signal (%)	Displays the current signal strength of the SSID.
Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/access point for the specified SSID.

Log

The system log displays system operation information such as up time and connection processes. This information is useful for network administrators.



```
Jan 1 00:02:49 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan 1 00:02:25 [SYSTEM]: LAN, Port[1] link is changed to 100Mbps-Full-Duplex
Jan 1 00:00:58 [SYSTEM]: WLAN[2.4G], Best channel selection start, switch to channel 1 + 5
Jan 1 00:00:38 [SYSTEM]: WLAN[5G], Skip Best channel selection and wait for next time
Jan 1 00:00:12 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan 1 00:00:12 [SYSTEM]: LAN, Port[0] link status is changed to down
Jan 1 00:00:11 [SYSTEM]: TFTP server, Stopping
Jan 1 00:00:11 [SYSTEM]: FTP server, Stopping
Jan 1 00:00:11 [SYSTEM]: HTTPS, start
Jan 1 00:00:11 [SYSTEM]: HTTP, start
Jan 1 00:00:10 [SYSTEM]: LEDs, light on specific LEDs
Jan 1 00:00:07 [SYSTEM]: WLAN[5G], Channel = AutoSelect
Jan 1 00:00:07 [SYSTEM]: WLAN[5G], Wireless Mode = 11ACVHT80
Jan 1 00:00:02 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan 1 00:00:02 [SYSTEM]: WLAN[2.4G], Wireless Mode = 11NGHT40MINUS
Jan 1 00:00:02 [SYSTEM]: DHCP, start
Jan 1 00:00:02 [SYSTEM]: LAN, start
Jan 1 00:00:02 [SYSTEM]: Bridge, start
```

Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

The following information/events are recorded by the log:

- **Wireless Client**
Connected & disconnected
Key exchange success & fail
- **Authentication**
Authentication fail or successful.
- **Association**
Success or fail
- **WPS**
M1 - M8 messages
WPS success
- **Change Settings**
- **System Boot**
Displays current model name
- **NTP Client**
- **Wired Link**
LAN Port link status and speed status
- **Proxy ARP**
Proxy ARP module start & stop
- **Bridge**
Bridge start & stop.
- **SNMP**
SNMP server start & stop.
- **HTTP**
HTTP start & stop.
- **HTTPS**
HTTPS start & stop.
- **SSH**
SSH-client server start & stop.
- **Telnet**
Telnet-client server start or stop.
- **WLAN (2.4G)**
WLAN (2.4G) channel status and country/region status
- **WLAN (5G)**
WLAN (5G) channel status and country/region status
- **ADT**

Network Settings

LAN-Side IP Address

The “LAN-side IP address” page allows you to configure your access point on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router’s DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers.

LAN-side IP Address

IP Address Assignment	DHCP Client ▾	
IP Address	192.168.2.1	
Subnet Mask	255.255.255.0	
Default Gateway	From DHCP ▾	

DNS Servers

Primary Address	From DHCP ▾	
Secondary Address	From DHCP ▾	

LAN-side IP Address	
IP Address Assignment	Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select “Static IP” to manually specify a static/fixed IP address for your access point (below).
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP

	server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.
--	--

DHCP users can select to get DNS servers’ IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

Primary Address	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
Secondary Address	Users can manually enter a value when DNS server’s primary address is set to “User-Defined”.

LAN Port

The “LAN Port” page allows you to configure the settings for your access point’s wired LAN (Ethernet) ports.

Wired LAN Port Settings				
Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
Wired Port (#1)	Enabled ▾	Auto ▾	Enabled ▾	Enabled ▾

Wired LAN Port	Identifies LAN port 1.
Enable	Enable/disable LAN port.
Speed & Duplex	Select a speed & duplex type for LAN port, or use the “Auto” value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets transfer/receive.
Flow Control	Enable/disable flow control. Flow control can pause new session request until current data processing is complete, in order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient Ethernet feature which disables unused interfaces to reduce power usage.

VLAN

The “VLAN” (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other.

Note: VLAN IDs 1 – 4094 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port (#1)	Untagged Port ▼	1
Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [CAP1200-CCDD10_G]	Untagged Port	1
Wireless 5GHz	VLAN Mode	VLAN ID
SSID [CAP1200-CCDD10_A]	Untagged Port	1

Management VLAN	
VLAN ID	1

VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port 1 and wireless SSIDs (2.4GHz or 5GHz).
VLAN Mode	Select “Tagged Port” or “Untagged Port” for LAN interface.
VLAN ID	Set a VLAN ID for specified interface, if “Untagged Port” is selected.

Management VLAN	
VLAN ID	Specify the VLAN ID of the management VLAN. Only the hosts belonging to the same VLAN can manage the device.

Wireless Settings

2.4GHz(5GHz)

Basic

2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n ▼
Enable SSID number	1 ▼
SSID1	CAP1200-CCDD10_G VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11 ▼
Auto Channel Interval	One day ▼ <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto ▼
BSS BasicRateSet	1,2,5.5,11 Mbps ▼

Wireless	Enable or disable the access point's 2.4GHz (5GHz) wireless radio. When disabled, no SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID Number	Select how many SSIDs to enable from the drop down menu. A maximum of 16 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.

When auto channel is disabled, select a wireless channel manually:

Channel	Select a wireless channel from.
Channel Bandwidth	Set the channel bandwidth: Manual select Bandwidth or set to Auto.
BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

Advanced

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

2.4GHz Advanced Settings	
Contention Slot	Short ▼
Preamble Type	Short ▼
Guard Interval	Short GI ▼
802.11g Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256-2346)
Multicast Rate	Auto ▼
Tx Power	100% ▼
Beacon Interval	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)

Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM.
------------------------	--

Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is "Short Preamble".
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the "Auto" setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.

Station idle timeout	Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active.
-----------------------------	--

Security

2.4GHz Wireless Security Settings	
SSID	CAP1200-CCDD10_G ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 /50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).

Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu appropriate for your method.

No Authentication

Authentication is disabled and no password/key is required to connect to the access point.

Note: Disabling wireless authentication is not recommended.
When disabled, anybody within range can connect to your device's network.

WEP

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from “ASCII” (any alphanumeric character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key.
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above.

IEEE802.1x/EAP

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
-------------------	--

WPA-PSK

WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA only. WPA2 is safer than WPA only, but not supported by all wireless clients. Please make sure your wireless client supports your selection.
Encryption	Select “TKIP/AES Mixed Mode” or “AES” encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.
Pre-Shared Key Type	Choose from “Passphrase” (8 – 63 alphanumeric characters) or “Hex” (up to 64 characters from 0-9, a-f and A-F).

Pre-Shared Key	Please enter a security key/password according to the format you selected above.
-----------------------	--

WPA-EAP

WPA Type	Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP.
Encryption	Select “TKIP/AES Mixed Mode” or “AES” encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.

Note: WPA-EAP must be disabled to use MAC-RADIUS authentication.

Additional Authentication

Additional wireless authentication methods can also be used:

MAC Address Filter

Restrict wireless clients access based on MAC address specified in the MAC filter table.

MAC Filter & MAC-RADIUS Authentication

Restrict wireless clients access using both of the above MAC filtering & RADIUS authentication methods.

MAC-RADIUS Authentication

Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.

MAC RADIUS Password

☒ Use MAC address
☐ Use the following password

MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select "Use the following password", enter the password in the field below. The password should match the "Shared Secret".
--------------------------------	---

WDS

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

Note: When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

WDS must be configured on each access point, using correct MAC addresses. All access points should use the same wireless channel and encryption method.

2.4GHz	
WDS Functionality	Disabled
Local MAC Address	Disabled
	WDS with AP
	Dedicated WDS

WDS Peer Settings	
WDS #1	MAC Address
WDS #2	MAC Address
WDS #3	MAC Address
WDS #4	MAC Address

WDS VLAN	
VLAN Mode	Untagged Port (Enter at least one MAC address.)
VLAN ID	1

WDS Encryption method	
Encryption	None (Enter at least one MAC address.)

2.4GHz/5GHz	
WDS Functionality	Select “WDS with AP” to use WDS with access point or “Dedicated WDS” to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your access point.

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDS devices you wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

WDS Encryption method	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters.

WPS

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device's configuration interface (known as PBC or "Push Button Configuration").

WPS	<input checked="" type="checkbox"/> Enable
-----	--

Apply

WPS

Product PIN	58327142	Generate PIN
Push-button WPS	Start	
WPS by PIN		Start

WPS Security

WPS Status	Not Configured	Release
------------	----------------	---------

WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication
Product PIN	Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click “Generate PIN” to generate a new WPS PIN code.
Push-Button WPS	Click “Start” to activate WPS on the access point for approximately 2 minutes. This has the same effect as physically pushing the access point’s WPS button.
WPS by PIN	Enter the PIN code of another WPS device and click “Start” to attempt to establish a WPS connection for approximately 2 minutes.
WPS Status	WPS security status is displayed here. Click “Release” to clear the existing status.

RADIUS

The RADIUS sub menu allows you to configure the access point's RADIUS server settings, categorized into three submenus: RADIUS settings, Internal Server and RADIUS accounts.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point can utilize both a primary and secondary (backup) RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz). External RADIUS servers can be used or the access point's internal RADIUS server can be used.

RADIUS Settings

Configure the RADIUS server settings for 2.4GHz & 5GHz. Each frequency can use an internal or external RADIUS server.

RADIUS Server (2.4GHz)	
Primary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>
Secondary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

RADIUS Server (5GHz)

Primary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

Secondary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Accounting	Enable or disable RADIUS accounting.

Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535.
------------------------	---

Internal Server

The access point features a built-in RADIUS server which can be configured as shown below used when “Internal” is selected for “RADIUS Type” in the “Wireless Settings” → “RADIUS” → “RADIUS Settings” menu.

Internal Server

Internal Server	<input type="checkbox"/> Enable
EAP Internal Authentication	PEAP(MS-PEAP) ▼
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
EAP Certificate File	<input type="button" value="Upload"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> second(s)
Termination-Action	<input checked="" type="radio"/> Reauthentication (RADIUS-Request) <input type="radio"/> Not-Reauthentication (Default) <input type="radio"/> Not-Send

Internal Server	Check/uncheck to enable/disable the access point's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.

Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length. This should match the “MAC-RADIUS” password.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Termination Action	Select a termination-action attribute: “Reauthentication” sends a RADIUS request to the access point, “Not-Reauthentication” sends a default termination-action attribute to the access point, “Not-Send” no termination-action attribute is sent to the access point.

RADIUS Accounts

The internal RADIUS server can authenticate up to 256 user accounts. The “RADIUS Accounts” page allows you to configure and manage users.

RADIUS Accounts

User Name
Example: USER1, USER2, USER3, USER4

User Registration List

Select	User Name	Password	Customize
<input type="checkbox"/>	EDIMAX	Not Configured	<input type="button" value="Edit"/>

Edit User Registration List

User Name	<input type="text" value="EDIMAX"/> (4-16characters)
Password	<input type="text"/> (6-32characters)

User Name	Enter the user names here, separated by commas.
------------------	---

Add	Click “Add” to add the user to the user registration list.
Reset	Clear text from the user name box.

Select	Check the box to select a user.
User Name	Displays the user name.
Password	Displays if specified user name has a password (configured) or not (not configured).
Customize	Click “Edit” to open a new field to set/edit a password for the specified user name (below).

Delete Selected	Delete selected user from the user registration list.
Delete All	Delete all users from the user registration list.

Edit User Registration List

User Name	Existing user name is displayed here and can be edited according to your preference.
Password	Enter or edit a password for the specified user.

MAC Filter

Mac filtering is a security feature that can help to prevent unauthorized users from connecting to your access point.

This function allows you to define a list of network devices permitted to connect to the access point. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the access point, it will be denied.

The MAC address filtering table is displayed below:

Add MAC Addresses

Add

Reset

MAC Address Filtering Table

Select	MAC Address
<input type="checkbox"/>	FC:F8:AE:43:43:7E

Delete Selected

Delete All

Export

Add MAC Address	Enter a MAC address of computer or network device manually e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses separated with commas, e.g. 'aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg'
Add	Click "Add" to add the MAC address to the MAC address filtering table.

Reset	Clear all fields.
--------------	-------------------

MAC address entries will be listed in the “MAC Address Filtering Table”. Select an entry using the “Select” checkbox.

Select	Delete selected or all entries from the table.
MAC Address	The MAC address is listed here.
Delete Selected	Delete the selected MAC address from the list.
Delete All	Delete all entries from the MAC address filtering table.
Export	Click “Export” to save a copy of the MAC filtering table. A new window will pop up for you to select a location to save the file.

WMM

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

WMM-EDCA Settings				
WMM Parameters of Access Point				
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47

WMM Parameters of Station				
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
Best Effort	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can further be adjusted manually:

CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). The CWMin value must be lower than the CWMax value. The contention window scheme helps to avoid frame collisions and determine priority of frame transmission. A shorter window has a higher probability (priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above).
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
TxOP	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value effects higher priority.

Management

Admin

Account to Manage This Device

Administrator Name	<input type="text" value="admin"/>		
Administrator Password	<input type="password" value="•••••"/>	(4-32 Characters)	
	<input type="password" value="•••••"/>	(Confirm)	

Apply

Advanced Settings

Product Name	<input type="text" value="AP801F02F1968A"/>		
Management Protocol	<div><input checked="" type="checkbox"/> HTTP</div> <div><input checked="" type="checkbox"/> HTTPS</div> <div><input checked="" type="checkbox"/> TELNET</div> <div><input type="checkbox"/> SSH</div> <div><input type="checkbox"/> SNMP</div>		
SNMP Version	<input type="text" value="v1/v2c"/> ▼		
SNMP Get Community	<input type="text" value="public"/>		
SNMP Set Community	<input type="text" value="private"/>		
SNMP Trap	<input type="text" value="Disabled"/> ▼		
SNMP Trap Community	<input type="text" value="public"/>		
SNMP Trap Manager	<input type="text"/>		

Apply

Account to Manage This Device	
Administrator Name	Set the access point's administrator name. This is used to log in to the browser based configuration interface and must be between 4-16 alphanumeric characters (case sensitive).

Administrator Password	Set the access point's administrator password. This is used to log in to the browser based configuration interface and must be between 4-32 alphanumeric characters (case sensitive).
-------------------------------	---

Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
SNMP Version	Select SNMP version appropriate for your SNMP manager.
SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager.

HTTP

Internet browser HTTP protocol management interface

HTTPS

Internet browser HTTPS protocol management interface

TELNET

Client terminal with telnet protocol management interface

SSH

Client terminal with SSH protocol version 1 or 2 management interface

SNMP

Simple Network Management Protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (USM) architecture.

Date and Time

You can configure the time zone settings of your access point here. The date and time of the device can be configured manually or can be synchronized with a time server.

Date and Time Settings

Local Time

2012

▼

Year

Jan

▼

Month

1

▼

Day

0

▼

Hours

00

▼

Minutes

00

▼

Seconds

Acquire Current Time from Your PC

NTP Time Server

Use NTP

☐ Enable

Server Name

Update Interval

24

(Hours)

Time Zone

Time Zone

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼

Date and Time Settings	
Local Time	Set the access point's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time and date.

NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.

Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

Time Zone	
Time Zone	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.

Syslog Server

The system log can be sent to a server.

Syslog Server Settings

Transfer Logs

☐ Enable Syslog Server

Transfer Logs	Check/uncheck the box to enable/disable the use of a syslog server, and enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.
---------------	--

Find Me

The access point features a built-in buzzer which can sound on command using the “Find Me” page. This is useful for network administrators and engineers working in complex network environments to locate the access point.

Duration of Sound

Duration of Sound

10

(1-300 seconds)

Sound Buzzer

Duration of Sound	Set the duration for which the buzzer will sound when the “Sound Buzzer” button is clicked.
Sound Buzzer	Activate the buzzer sound for the above specified duration of time.

Advanced

LED Settings

The access point's LEDs can be manually enabled or disabled according to your preference.

LED Settings

Power LED	<input checked="" type="radio"/> On <input type="radio"/> Off
Diag LED	<input checked="" type="radio"/> On <input type="radio"/> Off

Power LED	Select on or off.
Diag LED	Select on or off.

Update Firmware

The “Firmware” page allows you to update the system firmware to a more recent version. Updated firmware versions often offer increased performance and security, as well as bug fixes. You can download the latest firmware from the website.

Firmware Location

Update firmware from

☒ a file on your PC

Update firmware from PC

Firmware Update File

Browse...

Update

Note: Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.

Update Firmware From	Select “a file on your PC” to upload firmware from your local computer.
Firmware Update File	Click “Browse” to open a new window to locate and select the firmware file in your computer.
Update	Click “Update” to upload the specified firmware file to your access point.

Save/Restore Settings

The access point’s “Save/Restore Settings” page enables you to save/backup the access point’s current settings as a file to your local computer, and restore the access point to previously saved settings.

Save/Restore Method

Using Device

☒ Using your PC

Save Settings to PC

Save Settings

☐ Encrypt the configuration file with a password.

Save

Restore Settings from PC

Restore Settings

Browse...

☐ Open file with password.

Restore

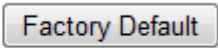
Save / Restore Settings	
Using Device	Select “Using your PC” to save the access point’s settings to your local computer.
Save Settings to PC	
Save Settings	Click “Save” to save settings and a new window will open to specify a location to save the settings file. You can also check the “Encrypt the configuration file with a password” box and enter a password to protect the file in the field underneath, if you wish.

Restore Settings from PC	
Restore Settings	Click the browse button to find a previously saved settings file on your computer, then click “Restore” to replace your current settings. If your settings file is encrypted with a password, check the “Open file with password” box and enter the password in the field underneath.

Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the location of the access point is not convenient to access the reset button.

This will restore all settings to factory defaults.



Factory Default	Click “Factory Default” to restore settings to the factory default. A pop-up window will appear and ask you to confirm.
------------------------	---

Reboot

This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

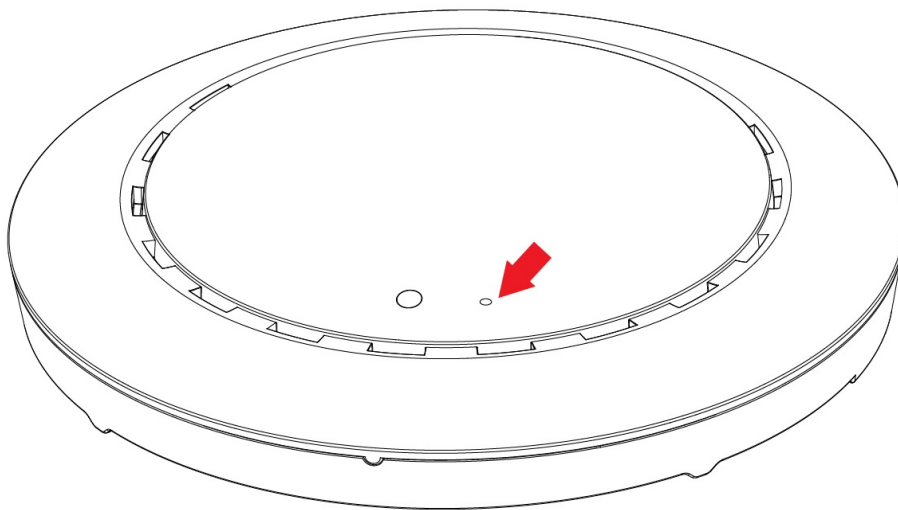
Reboot

Reboot

Click "Reboot" to reboot the device. A countdown will indicate the progress of the reboot.

Reset

1. Press and hold the reset button on the access point for at least 10 seconds then release the button.



2. Wait for the access point to restart. The access point is ready for setup when the LED is **Purple**.

Appendix

Configuring your IP address

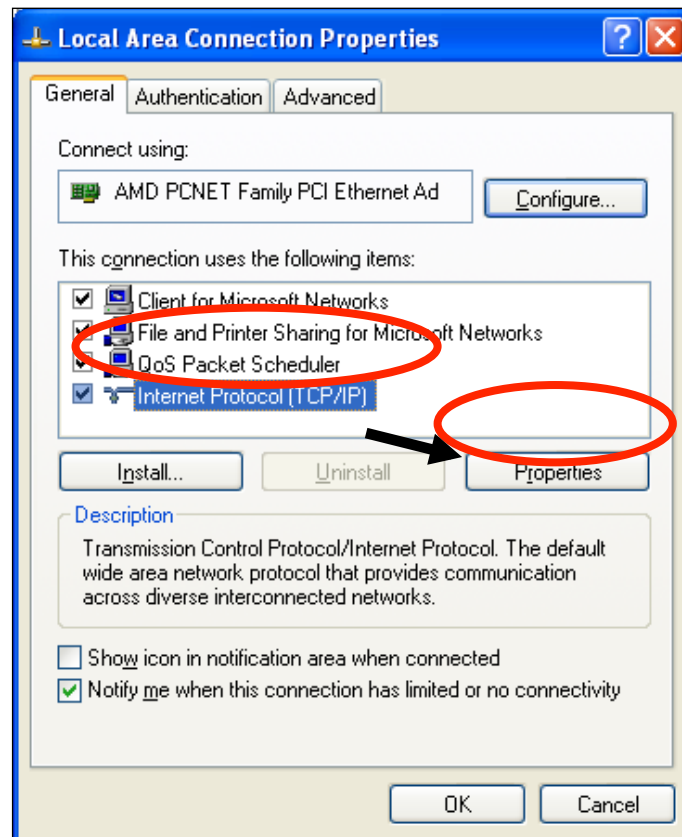
The access point uses the default IP address **192.168.1.1**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.1.x (x = 2 – 254)**.

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system.

In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.1.x (x = 2 – 254)**.

Windows XP

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Double-click the “Network and Internet Connections” icon, click “Network Connections”, and then double-click “Local Area Connection”. The “Local Area Connection Status” window will then appear, click “Properties”.

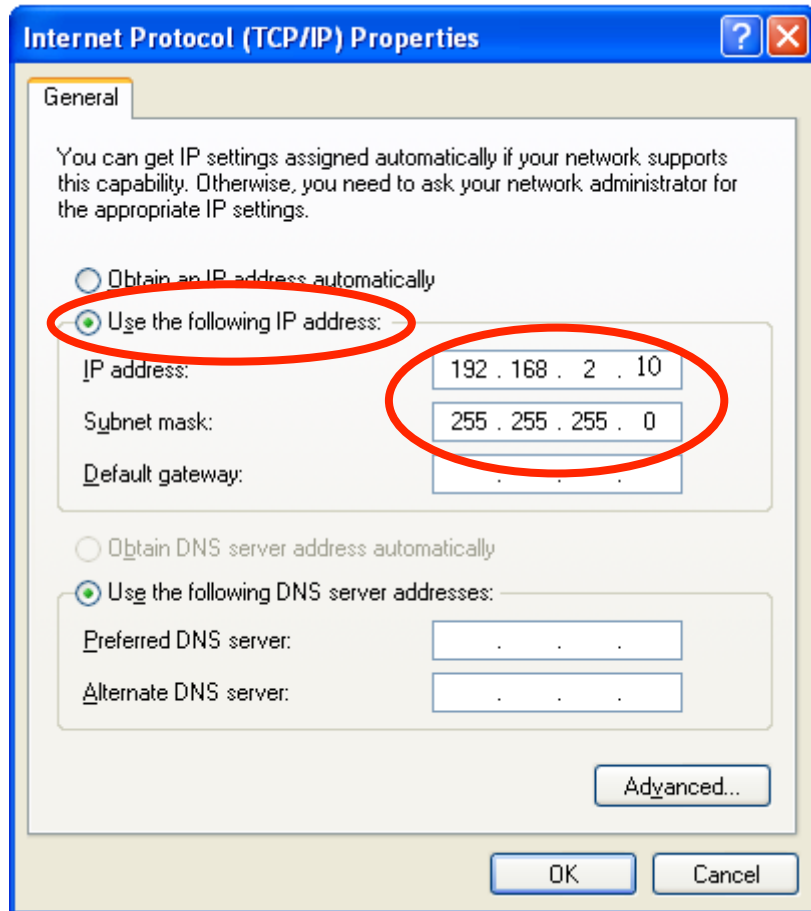


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

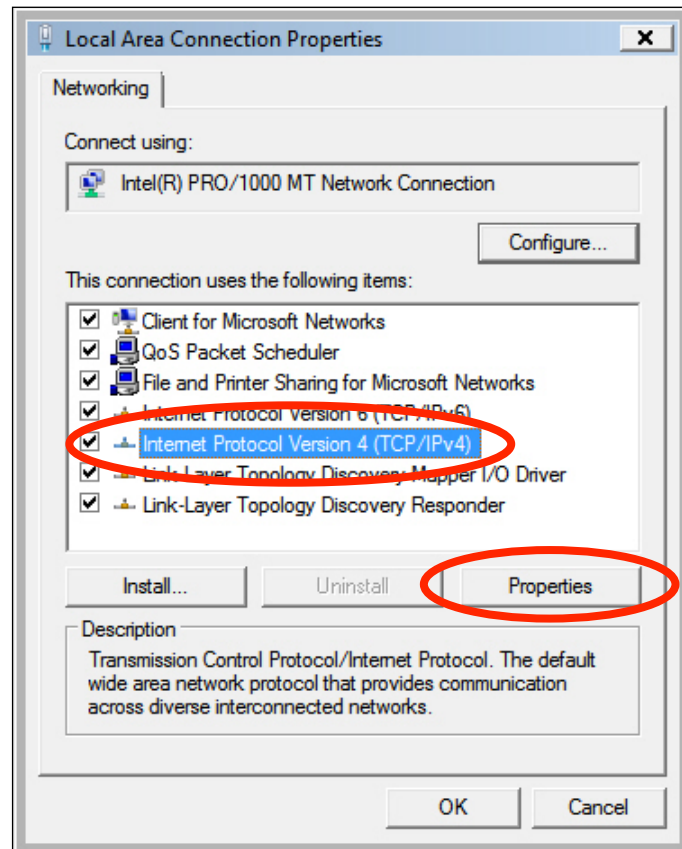
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



Windows Vista

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Click “View Network Status and Tasks”, then click “Manage Network Connections”. Right-click “Local Area Network”, then select “Properties”. The “Local Area Connection Properties” window will then appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.

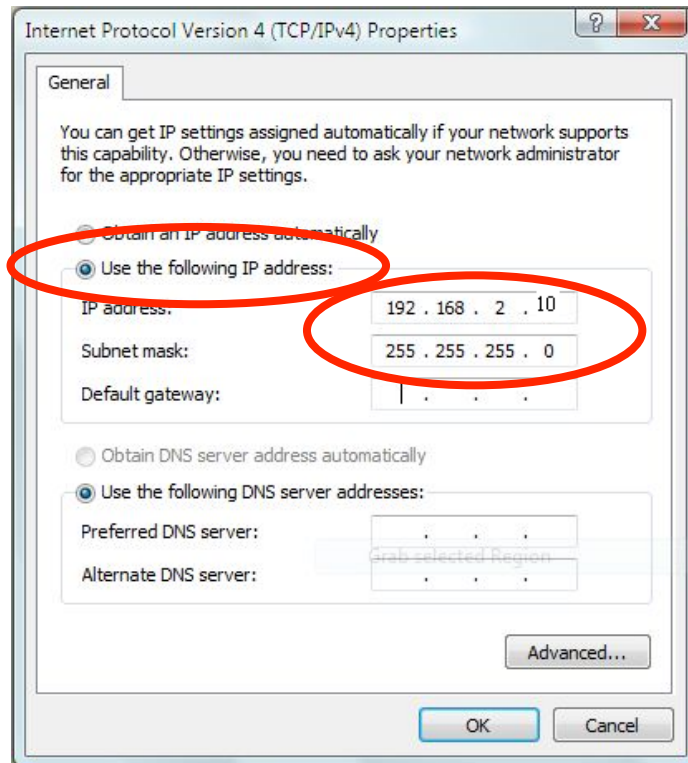


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

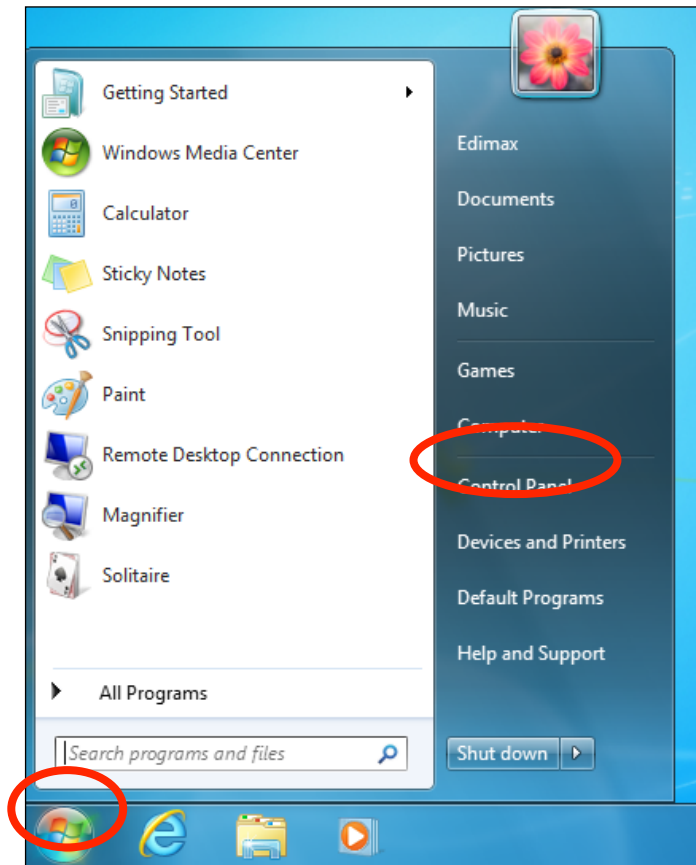
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

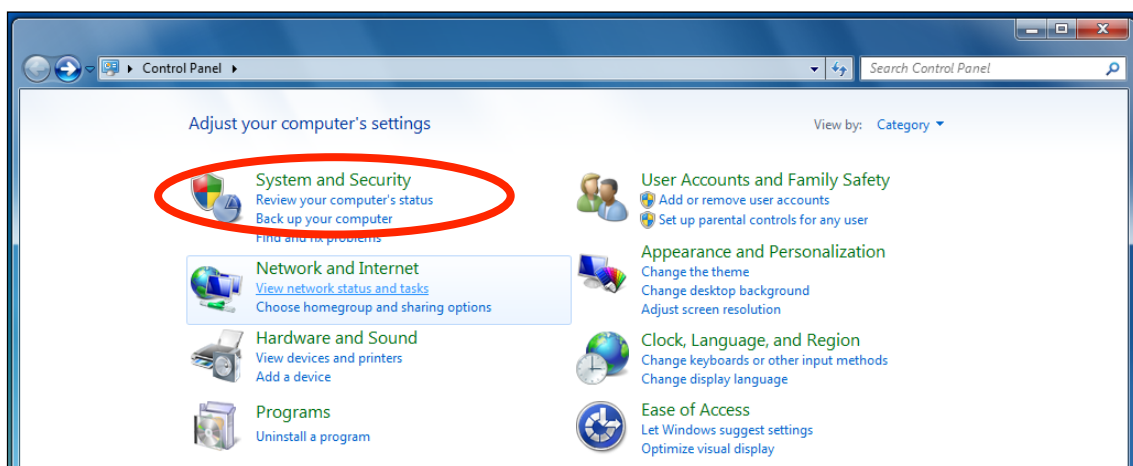


Windows 7

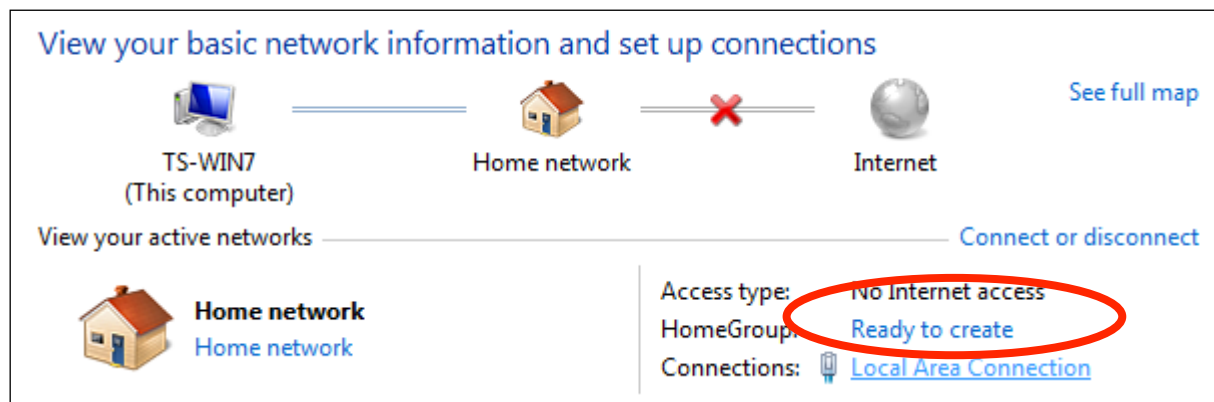
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



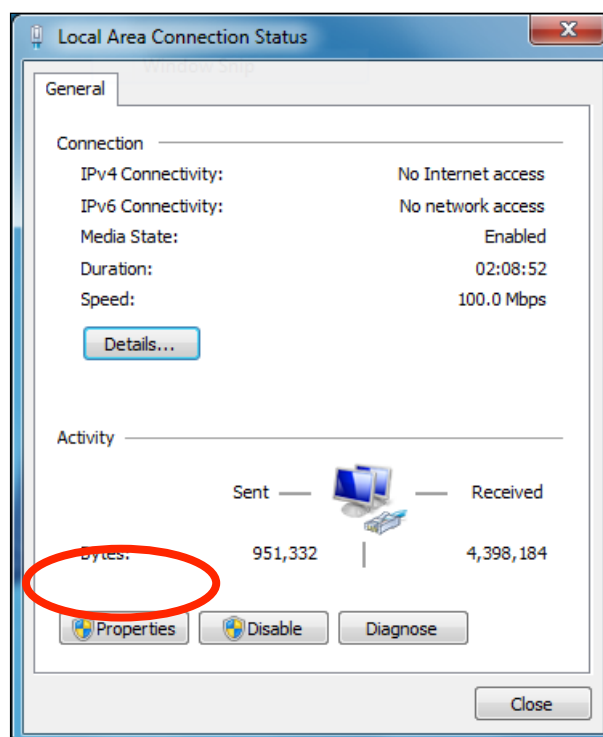
2. Under “Network and Internet” click “View network status and tasks”.



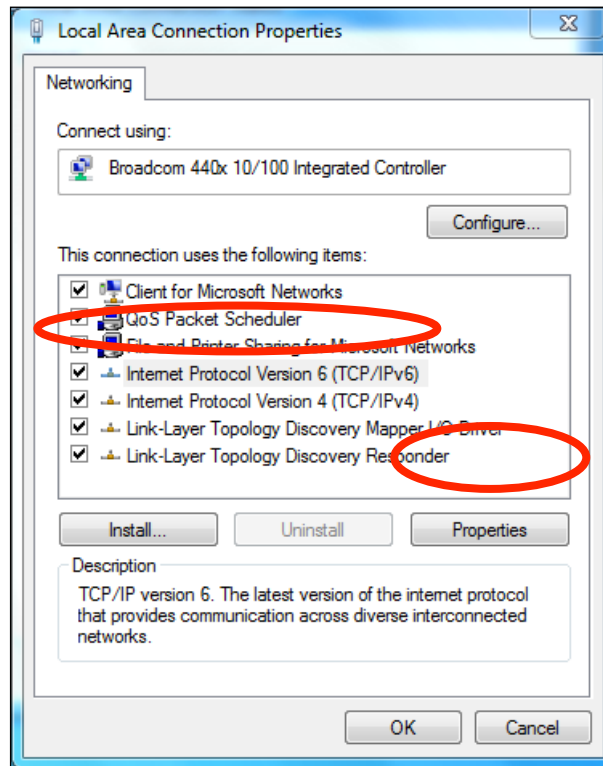
3. Click “Local Area Connection”.



4. Click “Properties”.



5. Select “Internet Protocol Version 4 (TCP/IPv4)” and then click “Properties”.

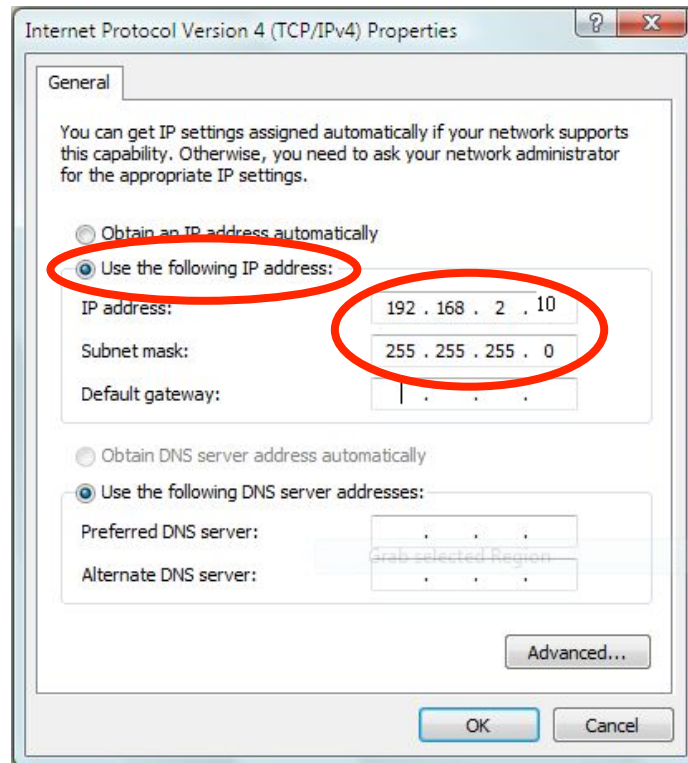


6. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

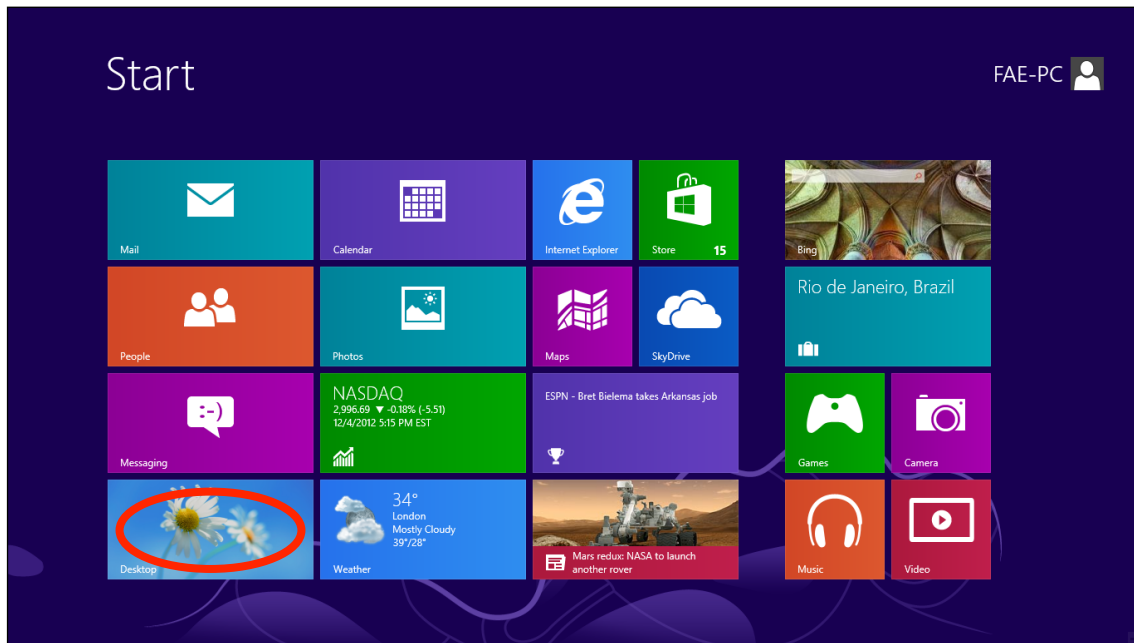
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

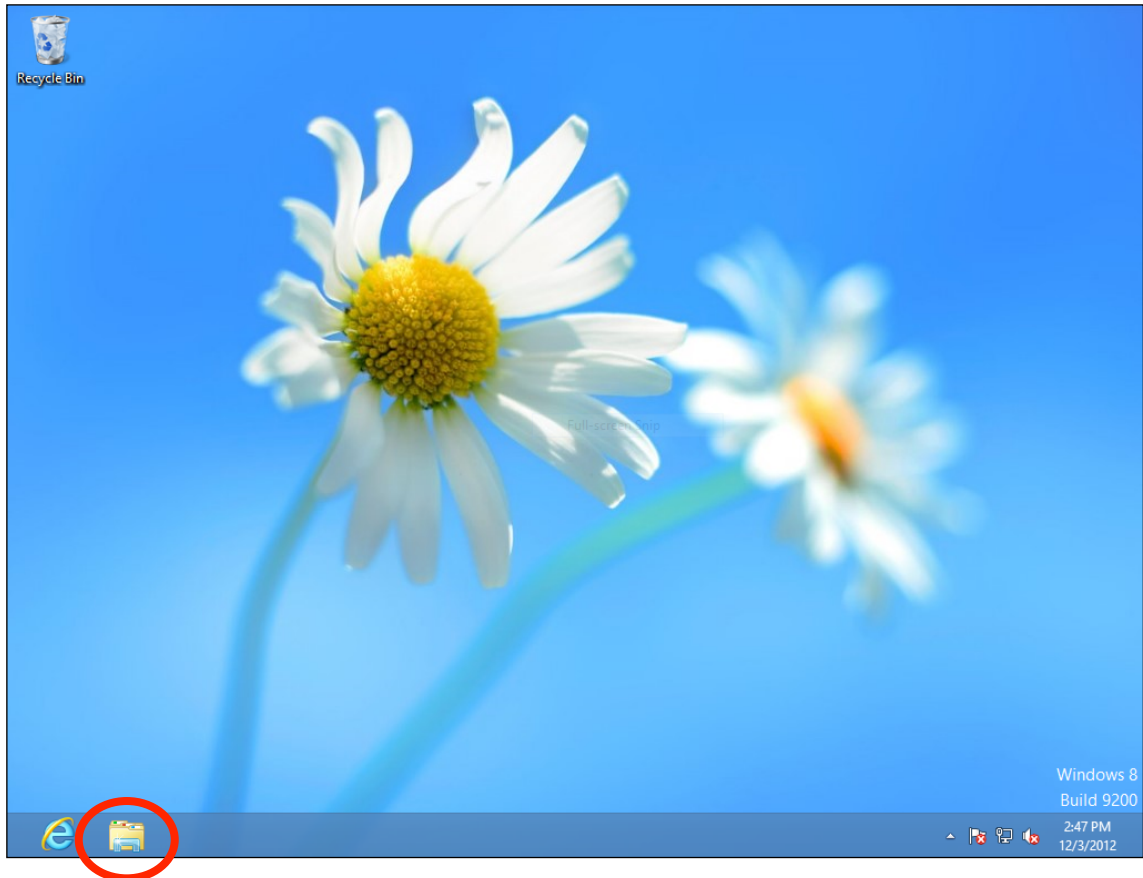


Windows 8

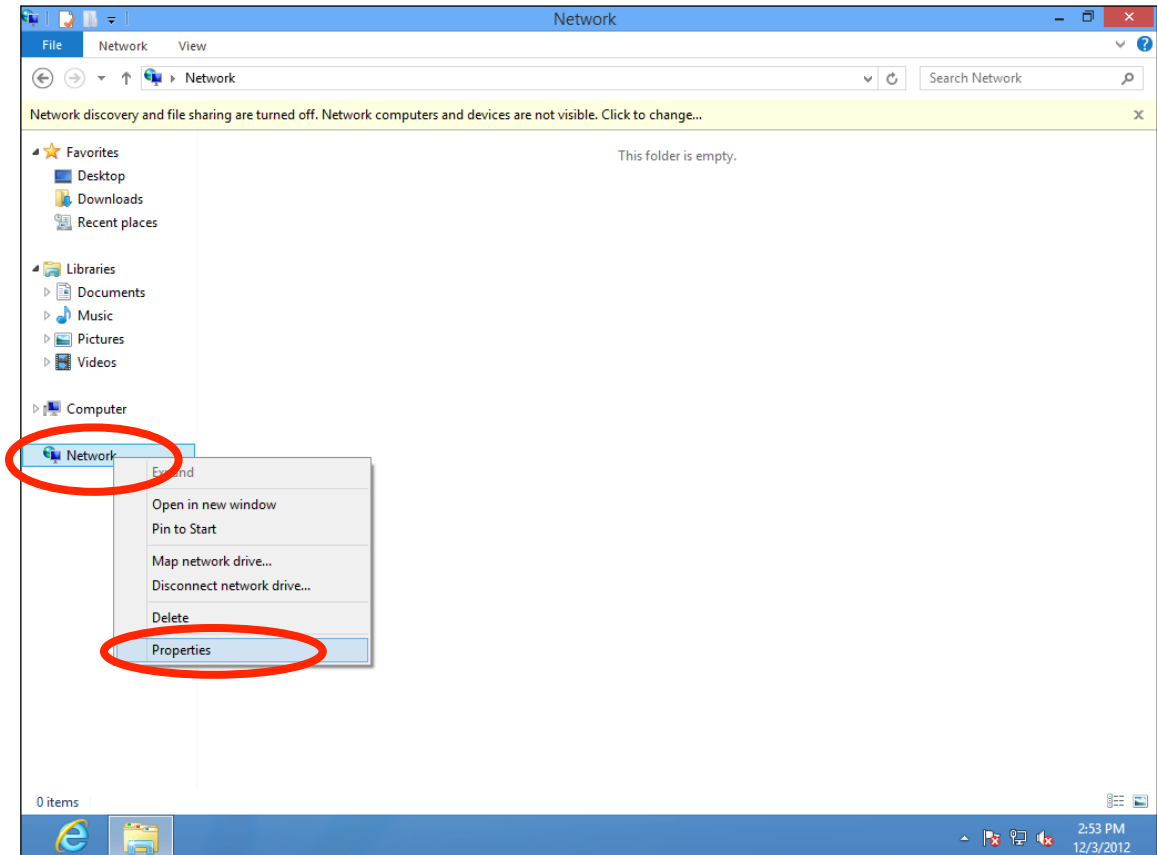
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your cursor to the bottom left of the screen and click.



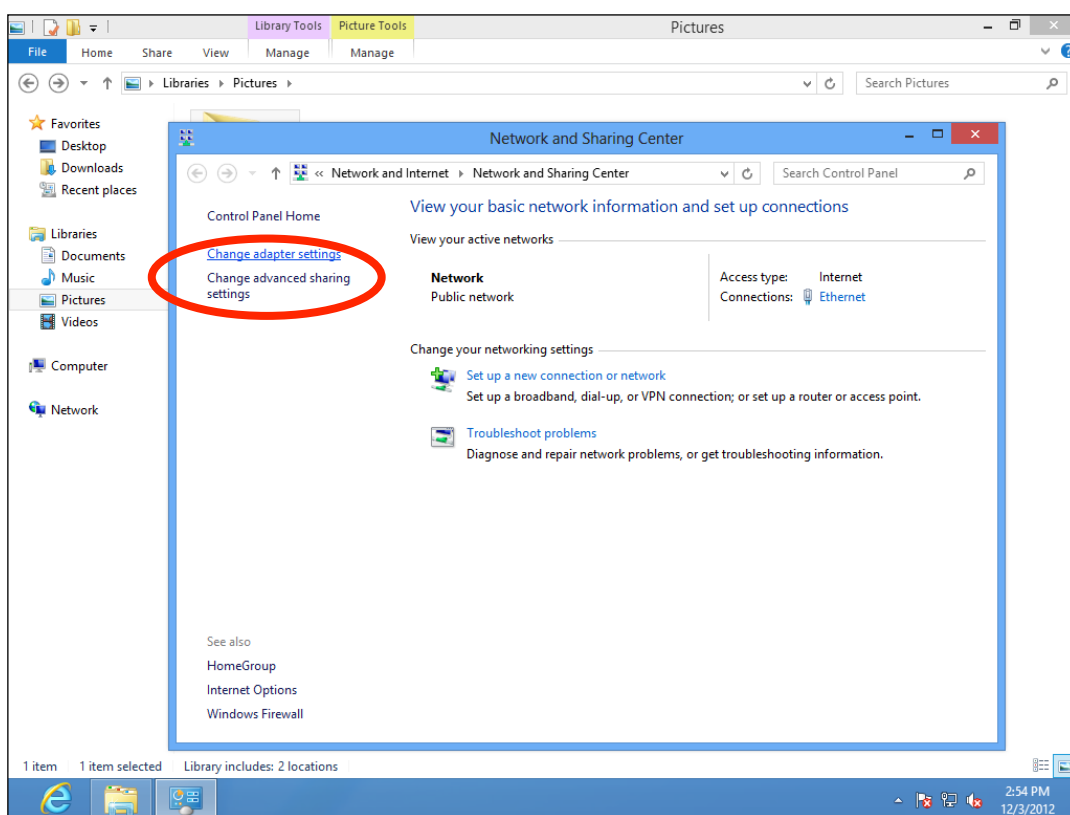
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



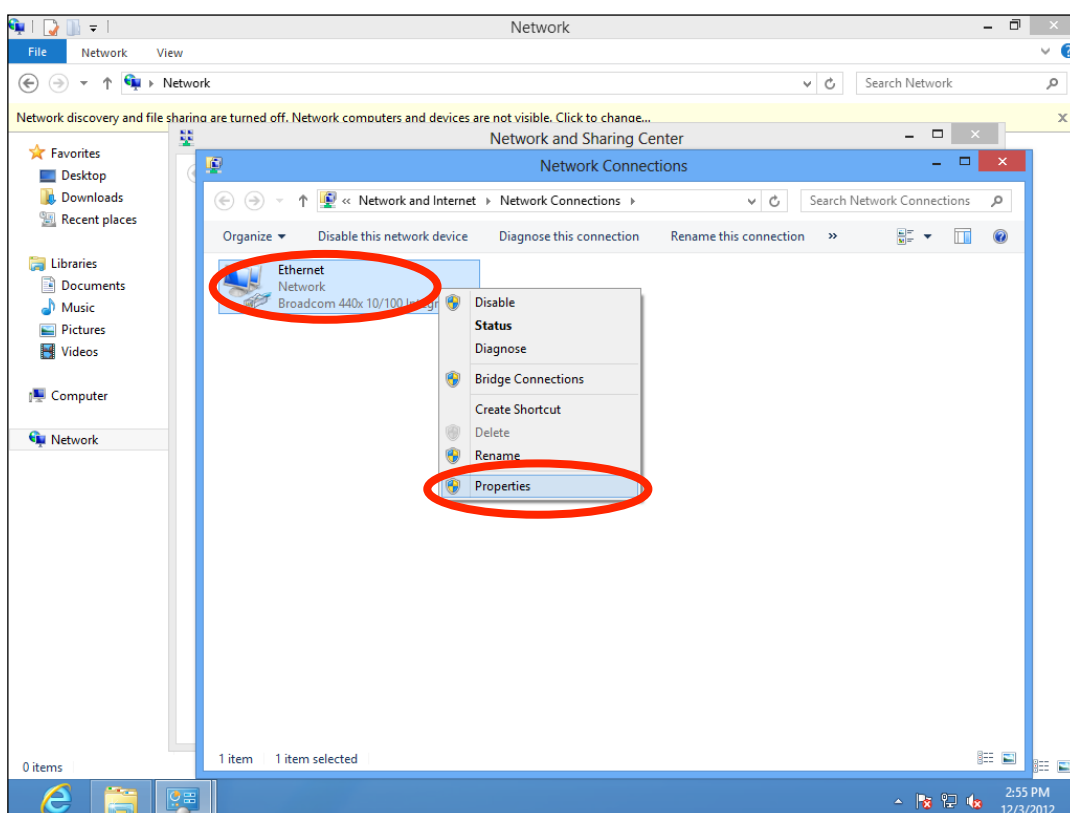
3. Right click “Network” and then select “Properties”.



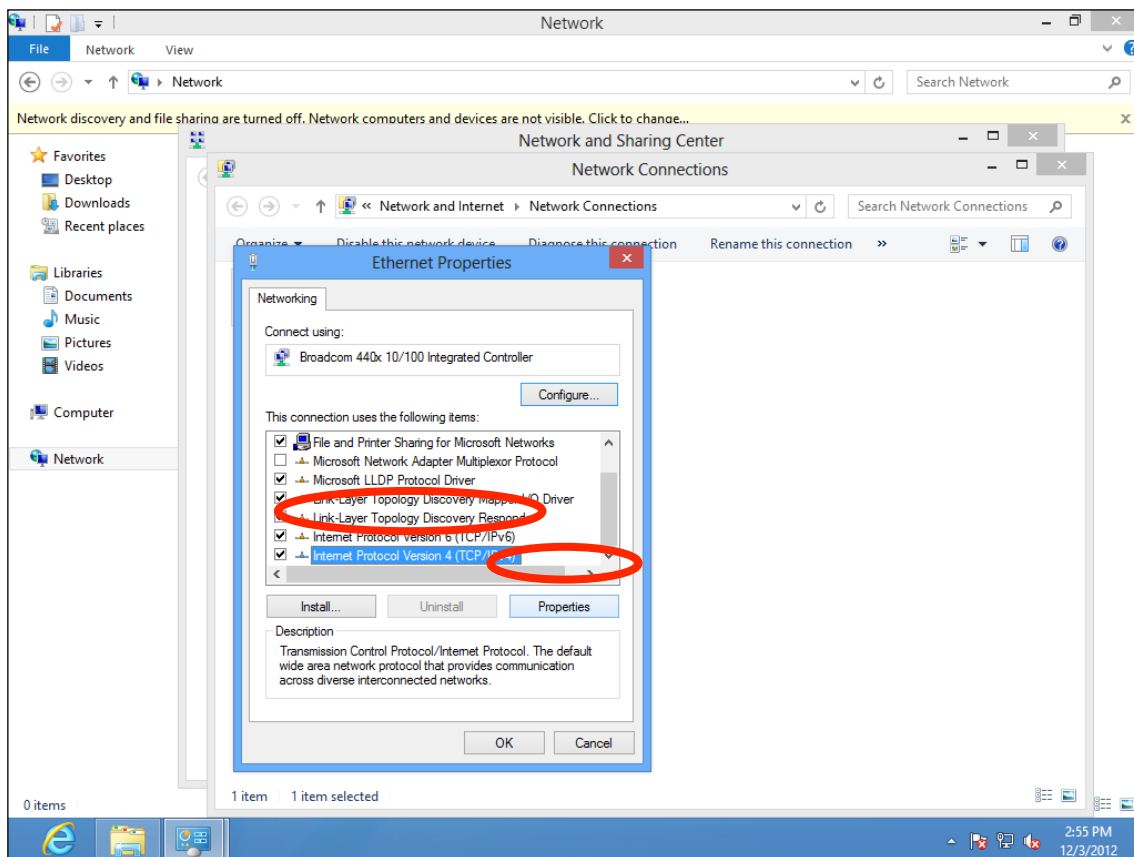
4. In the window that opens, select “Change adapter settings” from the left side.



5. Choose your connection and right click, then select “Properties”.



6. Select “Internet Protocol Version 4 (TCP/IPv4)” and then click “Properties”.



7. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

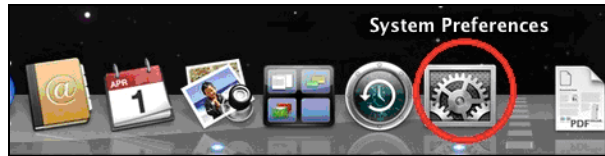
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

Mac

1. Have your Macintosh computer operate as usual, and click on “System Preferences”

Error! Objects cannot be created from editing field codes.

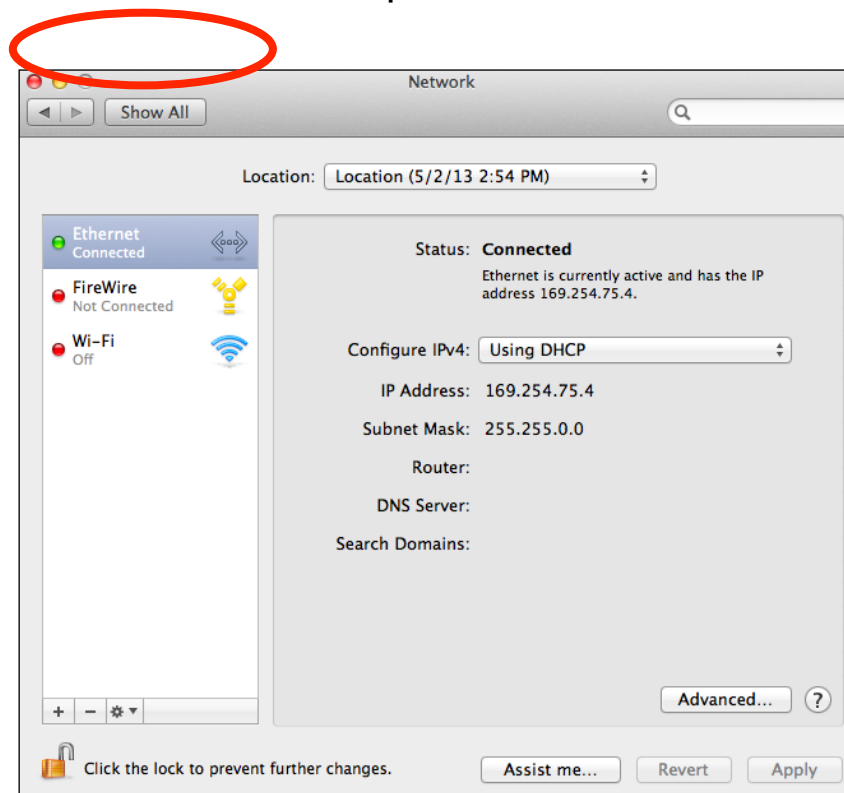


2. In System Preferences, click on “Network”.

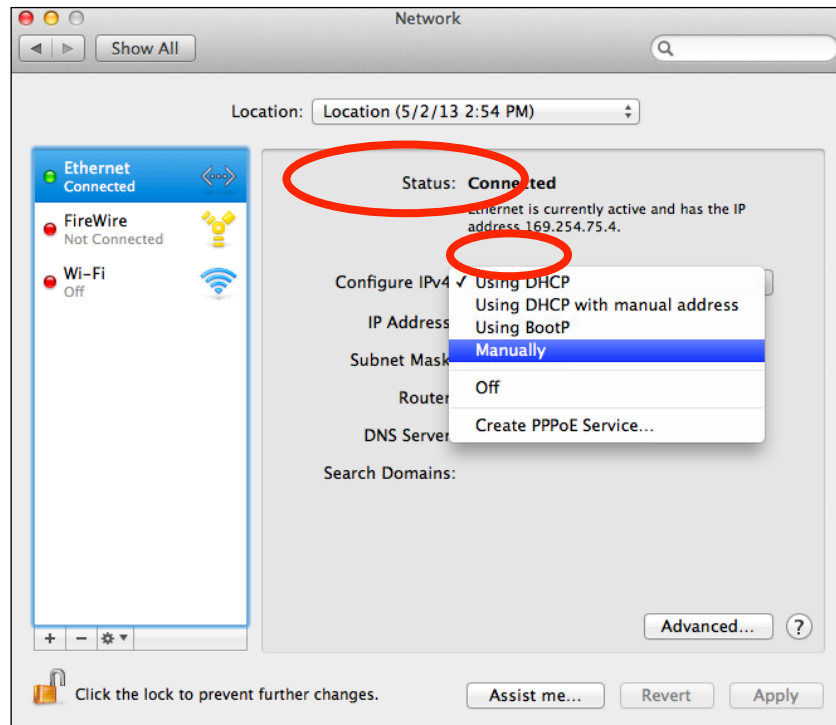
Error! Objects cannot be created from editing field codes.



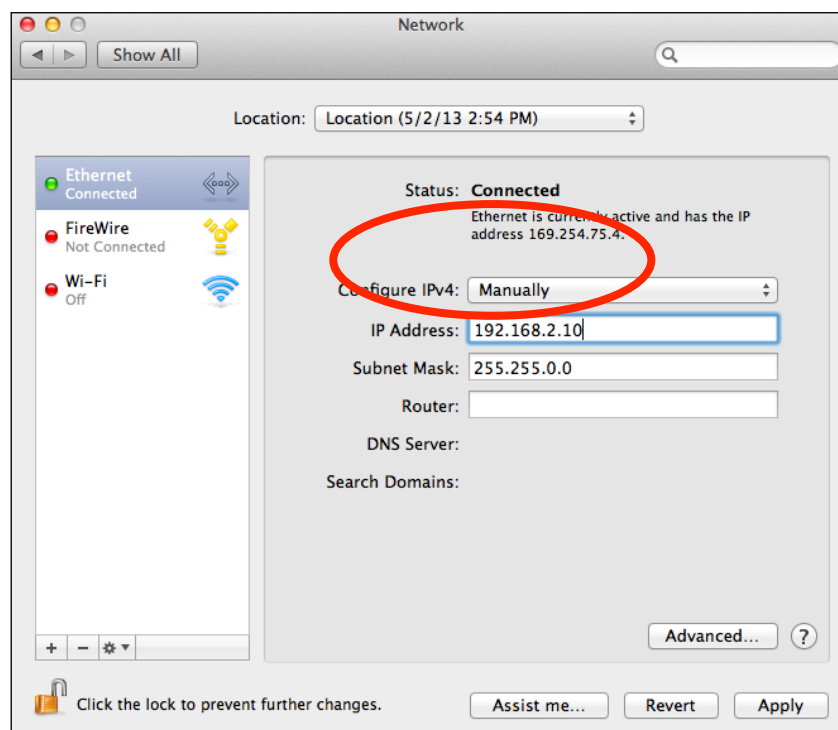
3. Click on “Ethernet” in the left panel.



4. Open the drop-down menu labeled “Configure IPv4” and select “Manually”.



5. Enter the IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on “Apply” to save the changes.



Hardware Specification

Memory	DDR2 64MB
Flash	8MB
Physical Interface	-LAN: 10/100/1000 Gigabit Ethernet with PoE support 802.3af (PD In) -Reset Button -DC Power Jack
Power Requirement	Power over Ethernet, IEEE 802.3af DC : 12V / 1A
Antenna	Internal PIFA Antenna (3dBi 2.4GHz x 2, 4dBi 5GHz x 2)

ENVIRONMENT & PHYSICAL

Temperature Range	Operation : 0 to 40°C (32°F to 104°F) Storage : -20 to 60°C (-4°F to 140°F)
Humidity	90% or less – Operating, 90% or less - Storage
Certifications	FCC, CE
Dimensions	176(D) x 30(H)mm
Weight	306g

Safety Information

In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

1. The access point is designed for indoor use only; do not place the access point outdoors.
2. Do not place the access point in or near hot/humid places, such as a kitchen or bathroom.
3. Do not pull any connected cable with force; carefully disconnect it from the access point.
4. Handle the access point with care. Accidental damage will void the warranty of the access point.
5. The device contains small parts which are a danger to small children under 3 years old. Please keep the access point out of reach of children.
6. Do not place the access point on paper, cloth, or other flammable materials. The access point may become hot during use.
7. There are no user-serviceable parts inside the access point. If you experience problems with the access point, please contact your dealer of purchase and ask for help.
8. The access point is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.

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 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 or more of the following measures:

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

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. 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. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

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 device is restricted to indoor use.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece,

Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None