

WX-1500 Series Wireless LAN Access Point

User' s Manual

Version 2.2 – Oct. 2001

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 the minimum distance between your body and the antenna as shown in the table below:

Low gain indoor antennas($\leq 6\text{dBi}$)	4.5cm (1.8 inches)

Note: Detached antennas, whether installed indoors or out, should be installed **ONLY** by experienced antenna installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities.

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise without the prior writing of the publisher.

Printed in Taiwan, Oct. 2001

1 Contents

1 Contents	3
2 Introduction	4
3 Installation	5
4 Configuring the Access Point	6
Installing KickStart	7
Contents of Web Interface	12
Wireless Settings	13
Security Against Unauthorized Network Access	14
Security Against Eavesdropping	17
Security Against Unauthorized Configuration	19
Identity	21
5 Troubleshooting	23
6 Technical Specifications of WX-1500 Series	24

2 Introduction

Thank you for purchasing your WX-1500 Series Wireless Access Point.

This manual will assist you with the installation procedure.

The package you have received contains the following items:

- User manual,
- WX-1500 Series Wireless Access Point,
- Power adapter,
- CD containing configuration software and this manual.

Note: if anything is missing, please contact your vendor

A wireless LAN is normally used in a predefined environment. In such a network, Access Points are mounted at assigned places, each covering its own area in which wireless nodes can operate. These Access Points are connected to a wired network to communicate with each other and with servers and clients on that network.

The WX-1500 Access Point can be connected to a 10/100 Mbps Ethernet network through a RJ45 (UTP) connector.

3 Installation

1. Mount the Access Point firmly to the wall on the position that is determined during the site survey.
2. Make sure the antennas are in a vertical position (if not, rotate over 90 degrees).
3. Insert the power connector.
4. Attach the Access Point to Ethernet network by using UTP Ethernet cable.

At the front of the Access Point you will see three LEDs.

If all goes well, the leftmost LED (Power) is green and the rightmost (LINK) and middle (ACT) LEDs flash whenever there is traffic on the respective networks which is at least ten times per second for the wireless LAN because of so-called ‘beacons’.

The Access Point automatically selects the medium attached. When the cable network is detected, the network LED will turn yellow.

Reset the Access Point

1. You can reset the Access Point's settings to factory defaults by pushing a paperclip in the little hole next to the UTP port while the Access Point is on.
2. Release the reset button when the LED has stopped burning.
All settings are deleted.
3. Use KickStart to install new IP settings.
If you have a DHCP server the IP settings will probably remain the same.
4. You can now use the Web Interface to manage the Access Point again.

4 Configuring the Access Point

The Access Point is a ready to use device. It is delivered with default settings which allow you to have access to it without configuring it.

When you do configure the Access Point, you can change the settings with respect to security, radio channels, etc.

IP settings can be installed automatically or manually.

Install IP settings, when

1. **Automatically** : If the Access Point is part of a network with a DHCP server, the DHCP server assigns the IP settings to the Access Point for you. Now it will start the Web Interface.
2. **Manually** : If there is no DHCP server, you need to install the IP settings using the KickStart application.

Note: If there is no DHCP server available, the system might take over one minute to find the AP.

The Kickstart application is needed only when:

1. You start the Access Point for the first time, or
2. You have reset the Access Point to factory defaults and must install the IP settings again.

Note 1: If you would like to assign new IP address to AP, please run the command line from **Start → Run** windows with “**kickstart/a**” command to proceed.

Note 2: We highly recommend that to use wired method while assign IP address to AP, which is connect Access Point to your wired network adapter then do configuration.

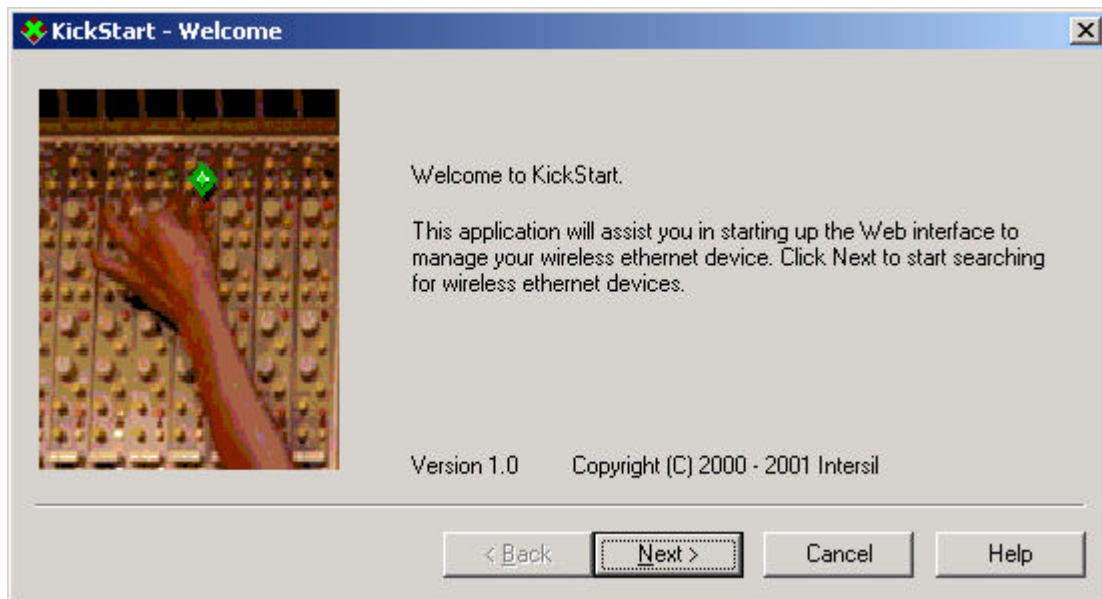
The Kickstart application can be found in the CD.

Installing KickStart

You can install KickStart on a Pc or notebook in the network to which the Access Point will be connected. Follow the instructions of the install wizard.

Launch KickStart

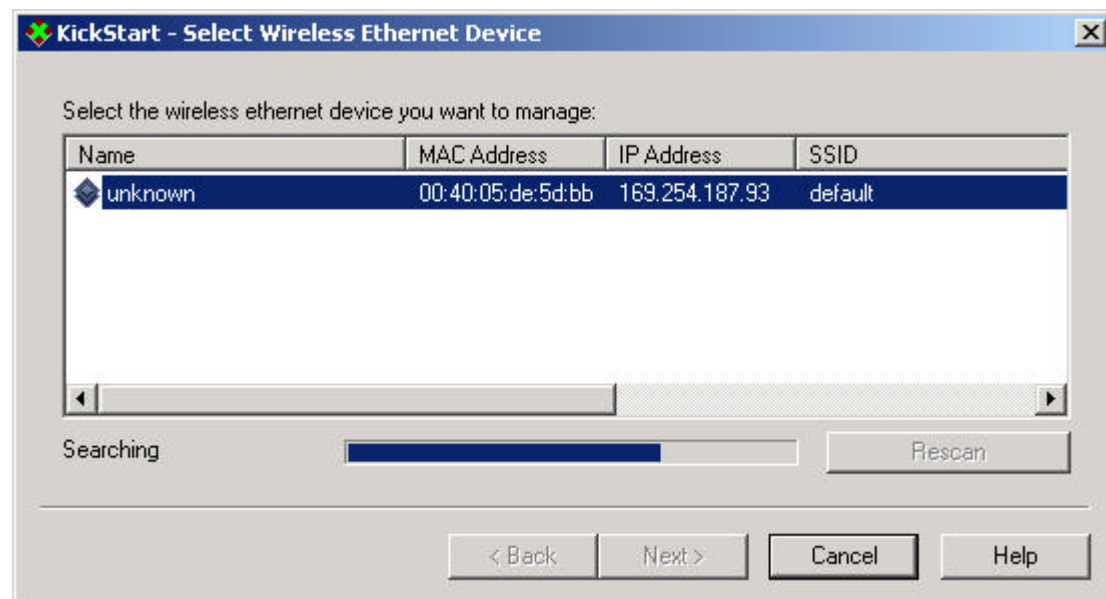
Double click the KickStart icon. The application starts up.



When you click **Next**, KickStart will search for all Access Points within range, whether they have been configured properly or not.

Select wireless Ethernet device

You can select the device you want to manage from the list as showed below.



After that you can

- click on **Next** to continue to the next screen, or
- click on **Rescan** to rescan for a wireless device.

Device data

The Scan Screen contains the data of the wireless devices that can be found.

Description

MAC address: Every Ethernet device has a unique address that is permanently linked to that device. It cannot be changed.

IP address : In order to access a TCP/IP network, a device must have an IP address.

SSID: The SSID is also known as Service Set ID. This is the name of your wireless network.

Scanning and rescanning for devices

If the device that you want to manage is in the list, select it, and click **Next**.

If you click the **Rescan** button, KickStart will search for Access Points again.

Use this to find Access Points that have just been switched on or reset.

IP settings

In this screen you can select to either use dynamic (if DHCP is available) or static IP settings.



Select Dynamic IP settings when you install the Access Point in a network with a DHCP server or Auto IP.

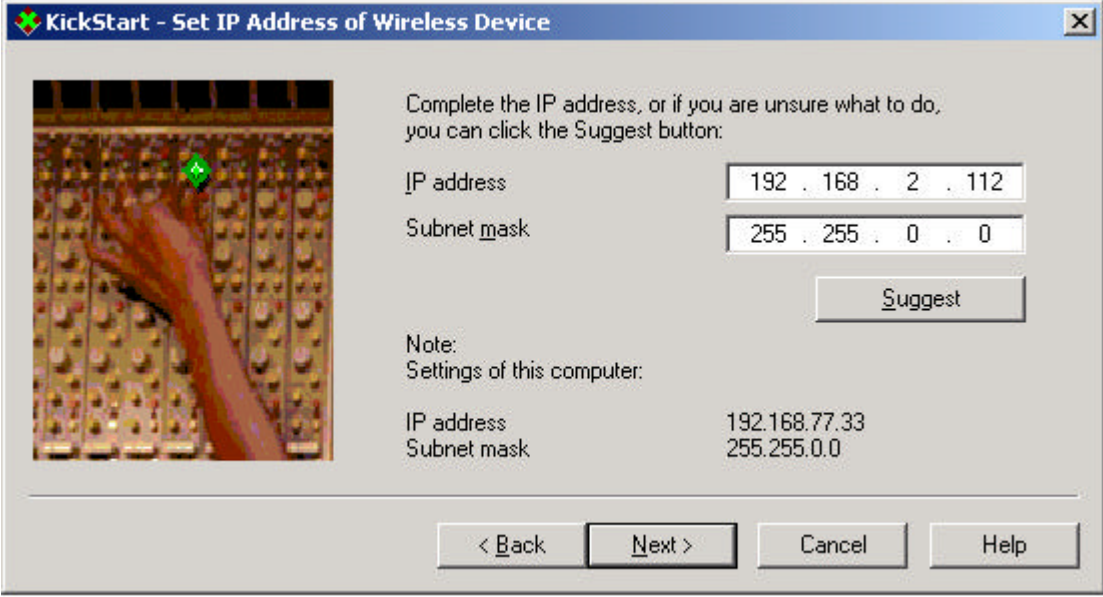
Select Static IP settings when you want to configure the IP settings manually.

Click on the Next button to continue to the next screen.

- If you selected the option Use dynamic IP settings, you will continue to the screen of Changing IP settings directly.
- If you selected the option Use static IP settings you will continue to the screen Set IP address of Wireless Device, see '[Static IP settings](#)'.

Static IP settings

When you have selected the option Use static IP setting in below appears:



KickStart - Set IP Address of Wireless Device

Complete the IP address, or if you are unsure what to do, you can click the Suggest button:

IP address: 192 . 168 . 2 . 112

Subnet mask: 255 . 255 . 0 . 0

Suggest

Note:
Settings of this computer:

IP address: 192.168.77.33
Subnet mask: 255.255.0.0

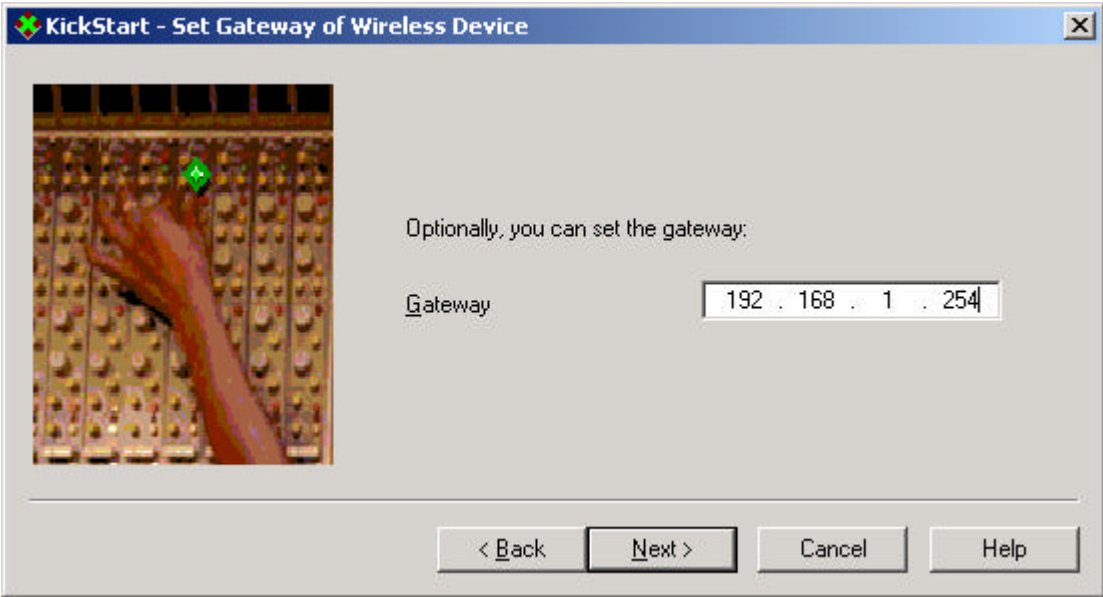
< Back Next > Cancel Help

In this screen you can either manually insert the IP address and Subnet mask, or you can click on the button of “**Suggest**” to let the system find the IP settings.

Click **Next** to continue to the next screen.

Gateway settings

In this screen you can install the Gateway address of the wireless device. Click on **Next** to continue to the next screen.



KickStart - Set Gateway of Wireless Device

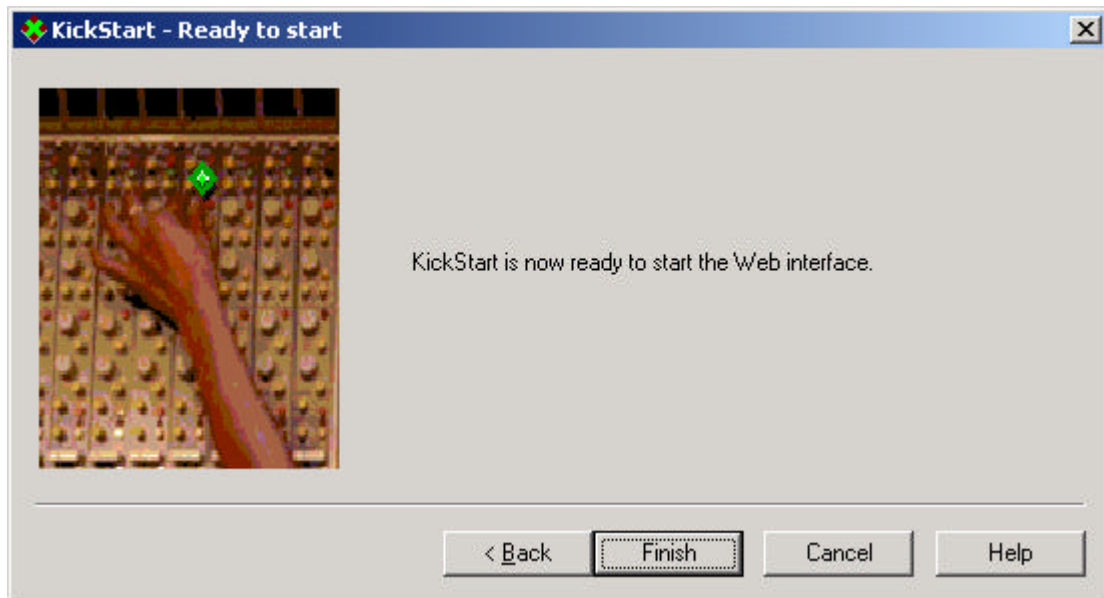
Optionally, you can set the gateway:

Gateway: 192 . 168 . 1 . 254

< Back Next > Cancel Help

Ready to start the Web Interface

If you click Finish in this screen, KickStart will launch a Web browser and open the administration page (Web interface) for the Access Point you have chosen. Then KickStart quits.



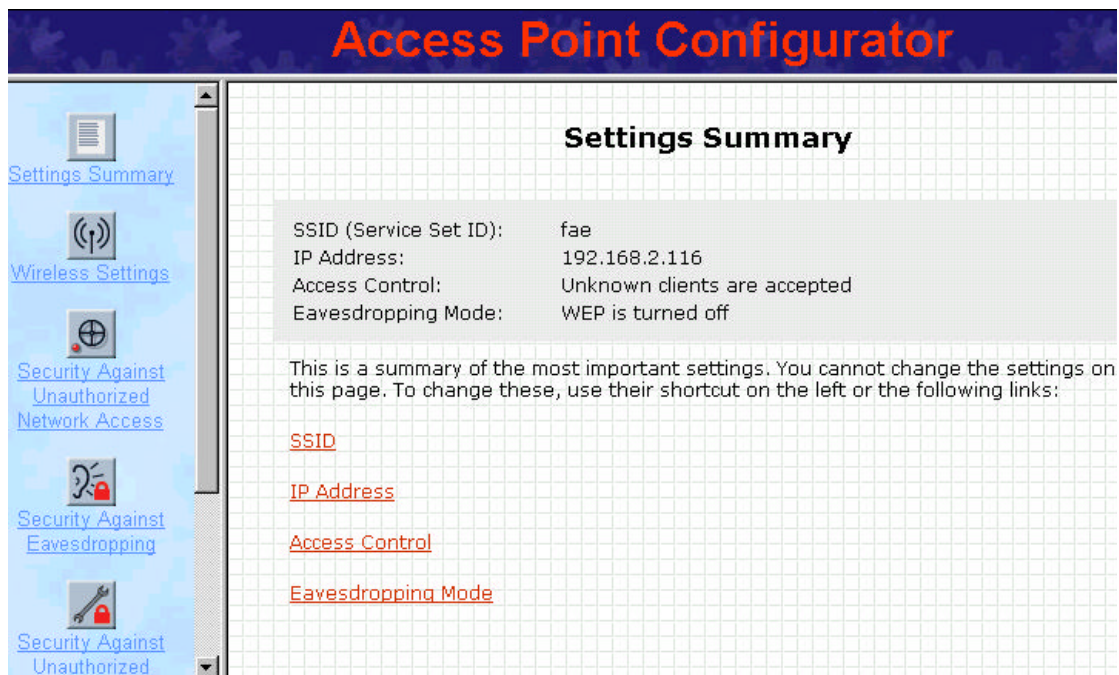
Web Interface is launched

Once the KickStart application has finished and the Access Point is available for configuration in the network, the Web Interface application is launched in a web browser. You can now edit the settings for the Access Point.

Contents of Web Interface

The Web Interface application contains the following subjects:

Settings Summary : On this page you will find an overview of the current settings.



The screenshot displays the 'Access Point Configurator' web interface. The title bar at the top is dark blue with the text 'Access Point Configurator' in red. On the left side, there is a vertical navigation menu with five items, each with an icon and a link: 'Settings Summary' (document icon), 'Wireless Settings' (signal icon), 'Security Against Unauthorized Network Access' (globe icon), 'Security Against Eavesdropping' (lock icon), and 'Security Against Unauthorized' (key icon). The main content area has a light blue grid background. At the top of this area is the heading 'Settings Summary'. Below it is a grey box containing the following settings:

SSID (Service Set ID):	fae
IP Address:	192.168.2.116
Access Control:	Unknown clients are accepted
Eavesdropping Mode:	WEP is turned off

Below the grey box, there is a paragraph: 'This is a summary of the most important settings. You cannot change the settings on this page. To change these, use their shortcut on the left or the following links:'. Underneath this paragraph are four red underlined links: [SSID](#), [IP Address](#), [Access Control](#), and [Eavesdropping Mode](#).

Wireless Settings : The settings of the wireless device are displayed here, and you can edit some of these settings.

The screenshot shows the 'Access Point Configurator' interface. On the left is a sidebar with navigation links: 'Settings Summary', 'Wireless Settings' (highlighted in green), 'Security Against Unauthorized Network Access', 'Security Against Eavesdropping', and 'Security Against'. The main area is titled 'Wireless Settings' and contains the following fields: 'SSID (Service Set ID):' with a text box containing 'fae', 'Radio Channel:' with a dropdown menu showing '3', 'Regulatory Domain:' with a text box containing 'ETSI (All countries in Europe except France)', and 'High Rate:' with a checked checkbox. Below these fields are 'Cancel' and 'Apply' buttons. At the bottom, there is a descriptive paragraph and a bulleted list explaining the SSID and Radio Channel settings.

Access Point Configurator

Wireless Settings

SSID (Service Set ID): fae

Radio Channel: 3

Regulatory Domain: ETSI (All countries in Europe except France)

High Rate: ☒

Cancel Apply

This page contains settings for the identification and radio channel use of the Access Po

- SSID (Service Set ID): this is the name of the network that the client can see and select to join.
- Radio Channel: the channel that the Access Point uses to transmit and receive information. Unless you have multiple Access Points in the vicinity, there is norma

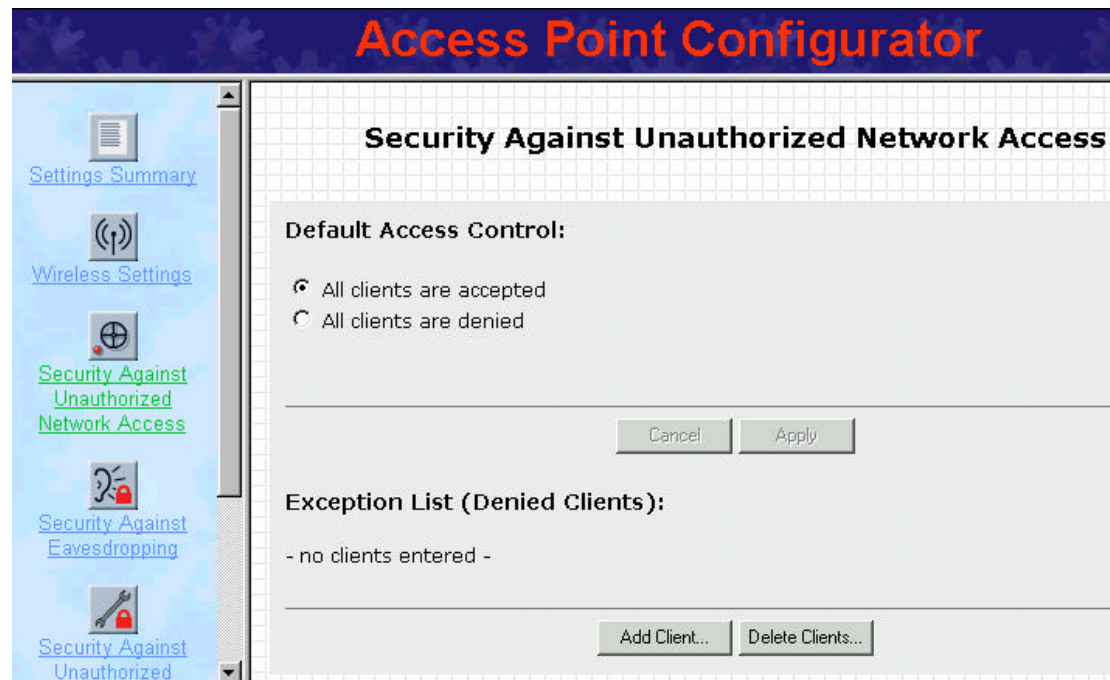
SSID : This is the Service Set ID. Only Access Points and clients that share the same SSID are able to communicate with each other.

Radio Channel: This is the channel that the Access Point uses to transmit and receive information. The channel that you select here is restricted to the channels that can be used within your Regulatory domain.

Regulatory Domain: The Regulatory domain is displayed here. Every country has a Regulatory Domain concerning radio channels that can be used to transmit and receive signals. This setting is a factory default that cannot be changed.

Security Against Unauthorized Network Access :On this page you can allow or deny access to the Access Point by clients.

To protect your network against unauthorized network access you can create an Access Control List (ACL).



You can choose to allow access to all clients or deny access to all clients, and create a list of exceptions for both options.

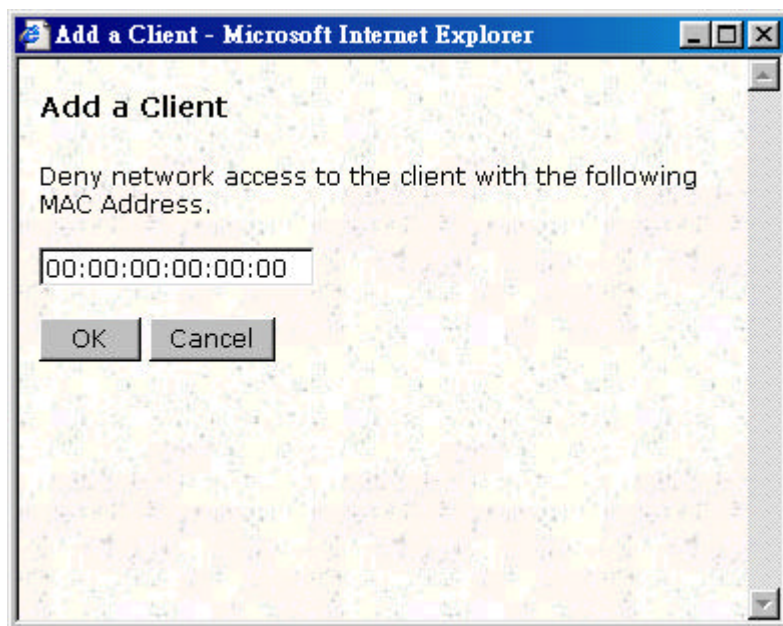
All clients are accepted: When you select this option, you allow access to all PC Cards, except for ones that you specify in the Exception list. This option can be useful if you do not want to keep track of all PC Cards but you do know some PC Cards that need to be denied access because they were stolen or some other reasons.

All clients are denied: When you select this option, you deny access to all PC Cards except the ones you specify in the Exception List.

Select the option and press the “ **Apply** ” button, then add Exception List.

If you selected “Allow access to all clients, you can add the MAC address of the client that you want to deny access to in the MAC Address field.

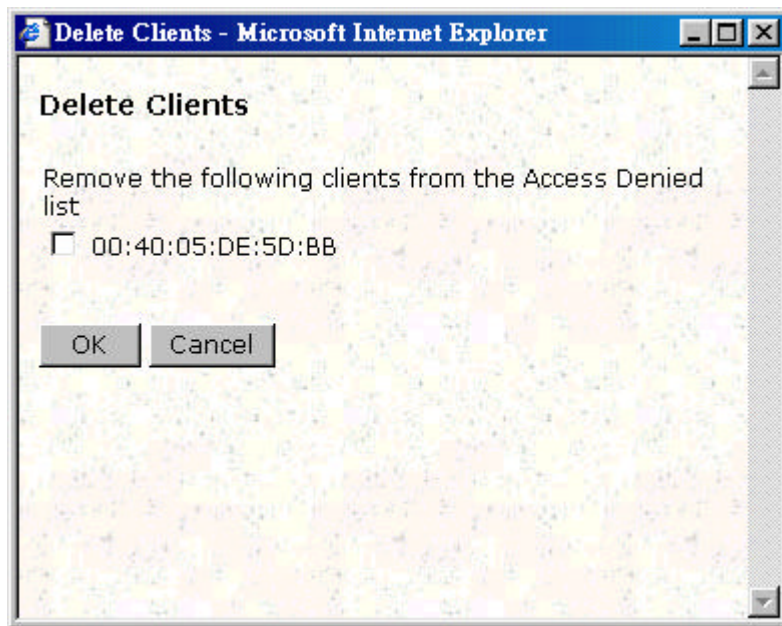
If you selected “Deny access to all clients, you can add the MAC address of the client that you want to allow access to in the MAC Address field.



Then click on the **OK** button. The client is now added to the exception list.

To delete a client from the exception list

1. Click on the button of “**Delete clients**”, a separate window opens in which the Exception list is displayed.



2. Select the MAC Address(es) of the client(s) that you want to remove from the list.
3. Then click on the **OK** button. The exception list is updated.

Security Against Eavesdropping :On this page you can install security methods to prevent eavesdropping on the connection to the Access Point.

The screenshot shows the 'Access Point Configurator' interface. The title bar is dark blue with 'Access Point Configurator' in red. The left sidebar is light blue and contains several icons and links: 'Settings Summary' (document icon), 'Wireless Settings' (Wi-Fi icon), 'Security Against Unauthorized Network Access' (globe icon), 'Security Against Eavesdropping' (key icon, highlighted in green), and 'Security Against Unauthorized' (key icon). The main content area has a white background with a grid pattern. It is titled 'Security Against Eavesdropping' in bold. Below the title, there are two radio button options: 'Open System (No Authentication)' which is selected, and 'WEP' with a red 'Change Settings' link next to it. Below these options are 'Cancel' and 'Apply' buttons. A paragraph of text explains that on this page, users can enable or disable WEP (Wired Equivalent Privacy). It lists two bullet points: 'Open System: clients have access without a password.' and 'WEP: the client must enter a password to connect to the Access Point.' A final paragraph explains that WEP requires specifying a key size and a key, with links to 'Change Settings'. It specifies that for WEP 40, the password is exactly 10 characters long, and for WEP 128, it is exactly 26 characters long. It also notes that only hexadecimal characters (0-9 and a-f) can be used.

Access Point Configurator

Security Against Eavesdropping

☒ Open System (No Authentication)
☐ WEP [Change Settings](#)

Cancel Apply

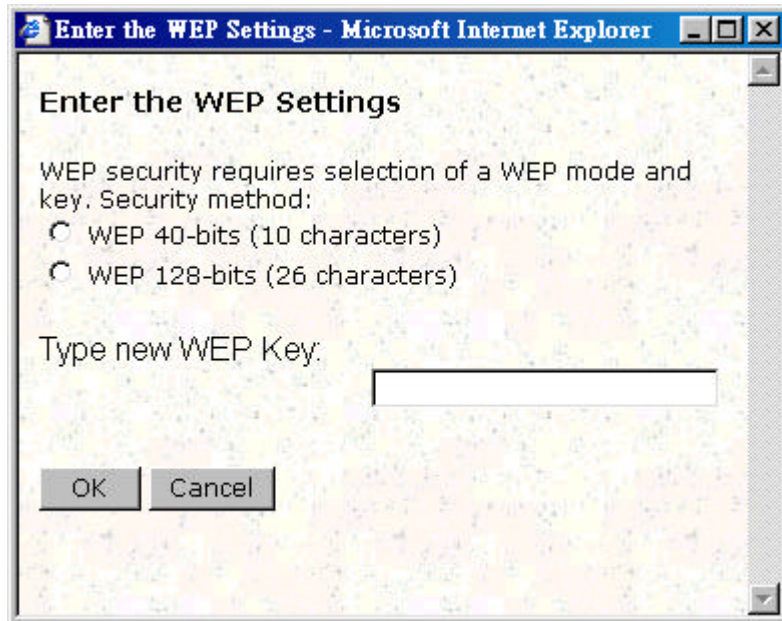
On this page you can enable or disable WEP (Wired Equivalent Privacy):

- Open System: clients have access without a password.
- WEP: the client must enter a password to connect to the Access Point.

WEP (Wired Equivalent Privacy) requires you to specify a key size and a key. Click the 'Change Settings' link to do so. There are two WEP key sizes. For WEP 40, the password is exactly 10 characters long. For WEP 128, the password is exactly 26 characters long. You can only enter hexadecimal characters (from 0 to 9, and from a to f).

Open System :When you select this option, clients have access without a password.

WEP Change Settings: When you select this option, you can activate the WEP security method.



1.Select the WEP method:40 bit or 128 bit.

2.Enter a password:

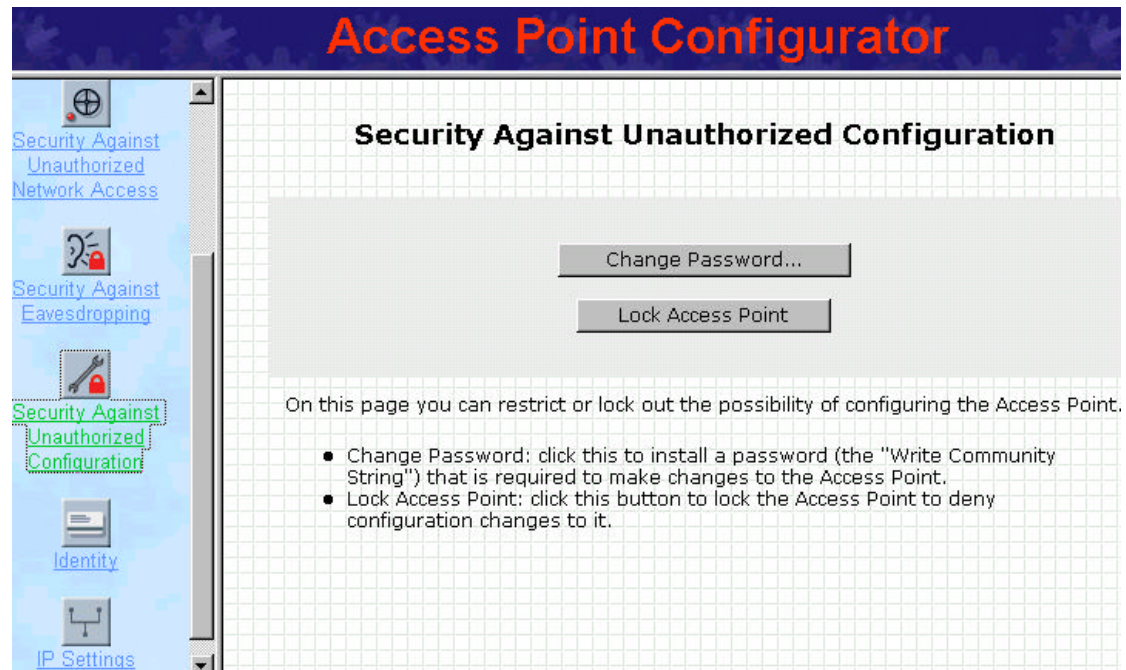
WEP 40:the password must contain exactly 10 characters,

WEP 128:the password must contain exactly 26 characters.

Note: Only the following alphanumeric characters are allowed in the password,
which is 0 to 9, a to f.

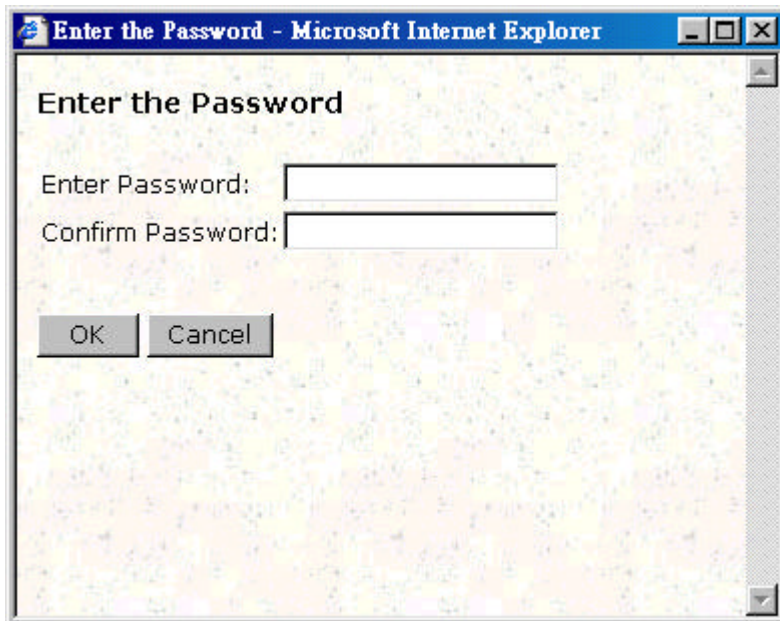
Click on **OK**.

Security Against Unauthorized Configuration :On this page you can manage the Write Community String for the Access Point and lock the management of the Access Point.



On this page you can install a password, the so-called “Write Community String”, that is required to make changes to the Access Point and lock the Access Point.

Click on the button of “**Change password**”.

A screenshot of a Microsoft Internet Explorer window. The title bar reads "Enter the Password - Microsoft Internet Explorer". The main content area has a title "Enter the Password". Below the title, there are two text input fields. The first is labeled "Enter Password:" and the second is labeled "Confirm Password:". Below these fields are two buttons: "OK" and "Cancel".

You can enter a password that is required to edit the settings of the Access Point with the Web Interface.

Click **OK**

Lock Access Point: Click on the button Lock Access Point to lock it.

A warning appears: “Are you sure to lock the Access Point? This will immediately prevent making configuration changes. You will still be able to view the current settings.”

Click on **OK** to lock the Access Point. No more configuration changes to the Access Point are allowed.

To unlock the Access Point:

- 1.You can reset the Access Point’ s settings to factory defaults by pushing a paperclip in the little hole next to the UTP port while the Access Point is on.
- 2.Release the reset button when the LED has stopped burning.
All settings are deleted.

Identity : Here the identity data of the Access Point are displayed, and you can edit some of these data.

The screenshot shows a web-based configuration interface titled "Access Point Configurator" in a red banner. On the left is a vertical navigation menu with icons and links: "Security Against Unauthorized Network Access", "Security Against Eavesdropping", "Security Against Unauthorized Configuration", "Identity" (highlighted in green), and "IP Settings". The main content area is titled "Identity" and contains a form with the following fields: "Location:" with the value "FAE-2nd Floor", "Contact:" with the value "faeteam@gemtek.com.tw", "MAC Address:" with the value "00:90:4B:08:8B:DB", "Access Point Type:" with the value "WLAN Access Point", and "Firmware Version:" with the value "3.2.28". Below the form are "Cancel" and "Apply" buttons. At the bottom of the main area, there is explanatory text: "This page gives information that will help you to identify the Access Point and its basic properties: The Location field can be used to indicate the physical location of the device (for example 2nd floor, room 3). The Contact field can be used to indicate the person responsible for the device, this can be an email address (for example: someone@company.com). Both fields do not influence the behavior of the Access Point."

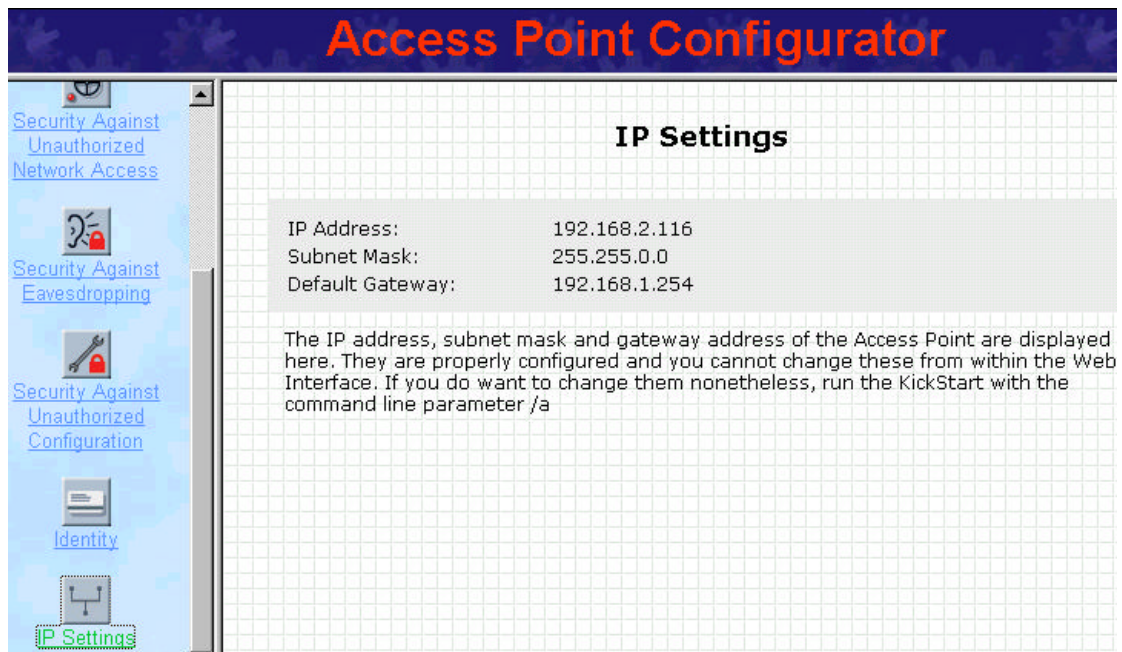
Location : This is a text field in which you can enter e.g. where the Access Point is installed (e.g. 2nd floor, room 3).

You can put any text into this field, the text has no influence on how the Access Point works.

Contact: This is a text field in which you can enter e.g. the name of the systems administrator responsible for the Access Point (“admin@domain.com”).

You can put any text into this field, the text has no influence on how the Access Point works.

IP Settings: The IP, subnet and gateway addresses of the Access Point are displayed here.



It is not possible to change these addresses from within the Web Interface.

If you want to change the IP settings of an Access Point that has already proper IP settings, you need to run KickStart and change them manually.

Note: If you would like to assign new IP address to AP, please run the command line from **Start** → **Run** windows with “**kickstart/a**” command to procedure process.

5 Troubleshooting

Q: If KickStart does not find the Access Point you are looking for.

A: There are several possible causes depending on the way the Access Point is connected to the network.

a. Problems on the wireless side

Always check the status of the LEDs to see whether you have:

- electricity problems,
- radio signal problems,
- networking problems.

1. Possible cause: Is the Access Point powered up ?

Solution: Check the power LED. Check if the Access Point is connected.

2. Possible cause: Is the Access Point in range of the WLAN card on your computer?

Solution: Check the ACT signal LED. Check for possible problems with respect to range.

3. Possible cause: Is there a network connection? Check the network LINK LED.

Solution: The Access Point may take up to a minute to find an IP address it can use if Auto IP is used to assign an IP address.

4. Possible cause: Client cannot make connection. A wireless client is not (yet) connected to the Access Point.

Solution: Refer to the manual of the wireless client on how to connect.

b. Problems on the wired side

Always check if your cables and connections are in good order and properly installed.

1. Possible cause: Has the proper cable been used?

Solution:

- If the Access Point is connected to a hub, a ‘ normal ’ (not a crossover) cable must be used.
- If the Access Point is connected directly to a computer , a crossover cable must be used.

6 Technical Specifications of WX-1500 Series

Standards supported

- IEEE 802.11 standard for Wireless LAN
- All major networking standards (including IP, IPX)

Environmental

Operating temperature (ambient):

- -10 ~ 50° C

Humidity:

- Max. 95% Non-condensing

Power specifications

DC power supply

- Input : DC 100-240 50-60 Hz 1A
- Output: 5V DC 1A converter incl.

Radio specifications

Range:

- per cell indoors approx. 35-100 meters
- per cell outdoors up to 100-300 meters

Transmit power:

- Nominal Temp Range: 14 dBm, 12min.
- Extend Temp Range: 14 dBm, 11 dBm min.
- Transmit Power, 2.7 v to 3v: 14 dBm max, 11 dBm min.

Frequency range:

- 2.4-2.4835 GHz, direct sequence spread spectrum

Number of Channels:

- Most European countries: 13 (1-13)
- US and Canada: 11 (1-11) (3 non-overlapping)
- France: 4 (10-13) (1 non-overlapping)
- Japan : 14 (1-14)

Antenna system:

- Dual antenna diversity system; 2dB gain with swivel neck

Specific features

Supported bit rates:

- 11 Mbps : CCK
- 5.5 Mbps : CCK
- 1 Mbps : DBSK
- 2 Mbps : DQPSK

Data encryption:

- 40-bits WEP Encryption
- 128-bits WEP Encryption

Utility Software:

- KickStart program & web management

Physical Dimensions

136 x 126 x 40 mm, 227 x 126 x 40 mm with antennas extended