



User Guide

**Wireless Access Point  
With Cloud Manager**

LAPAC1200C / LAPAC1750C

# Contents

Package Contents .....	4
Device Features .....	4
Mounting Guide .....	5
Access Point Setup Guide .....	6
Setup to manage your access point with Linksys cloud server .....	6
Setup to manage your access point locally with browser-based admin tool .....	7
Cloud Management Interface .....	8
Networks .....	8
Overview .....	10
Access Points .....	11
Wireless .....	16
Clients .....	21
Settings .....	23
Account settings .....	24
Inventory .....	27
Local Management Interface .....	28
Setup Wizard (Local Administration) .....	28
Administration .....	32
LAN .....	41
Wireless .....	47
Captive Portal .....	80
Cluster .....	89
System Status .....	96
Maintenance .....	106
Appendix A - Troubleshooting .....	112
Overview .....	112
General Problems .....	112
Appendix B - About Wireless LANs .....	114
Overview .....	114
Wireless LAN Terminology .....	114

Appendix C - PC and Server Configuration .....	118
Overview .....	118
Using WEP .....	118
Using WPA2-PSK .....	119
Using WPA2-Enterprise .....	119
802.1x Server Setup (Windows 2000 Server) .....	120
802.1x Client Setup on Windows XP .....	129
Using 802.1x Mode (without WPA) .....	135
Regulatory Approvals .....	136

# Package Contents

- Linksys Wireless Access Point
- Quick Start Guide
- Ethernet Cable
- AC Power Adapter
- CD with Documentation
- Mounting Bracket
- Mounting Kit
- Ceiling Mount Back Plate
- Drilling Layout Template

## Device Features

There is one indicator light on the front/top of the access point.

Light Color	Activity	Status
Green	Blinking	System is starting.
	Solid	System is normal; no wireless devices connected.
Blue	Blinking	Software upgrade in process.
	Solid	System is normal; at least one wireless device connected.
Red	Solid	Startup process or update failed; hard reset or service required.

## Ports and Button

**Power Port**—Connect the AC power adapter to this port.

**Note**—*Use only the adapter that came with your access point.*

**Ethernet Port**—Connect a wired network device to this port. This port supports PoE (Power over Ethernet) with a PoE switch or PoE injector. LAPAC1200C and LAPAC1750C can be powered on from an 802.3 af/at (PoE+) compliance source. Using CAT5e or better cable is highly recommended. The maximum power consumption of LAPAC1200C is 13W and LAPAC1750C is 15W.

**Note**—*When both PoE and AC power adapter are connected to access point, device will get power from PoE as higher precedence.*

**Reset Button**—Press and hold this button for less than 15 seconds to power cycle device. Press and hold for longer than 15 seconds to reset the device to factory default settings.

## Mounting Guide

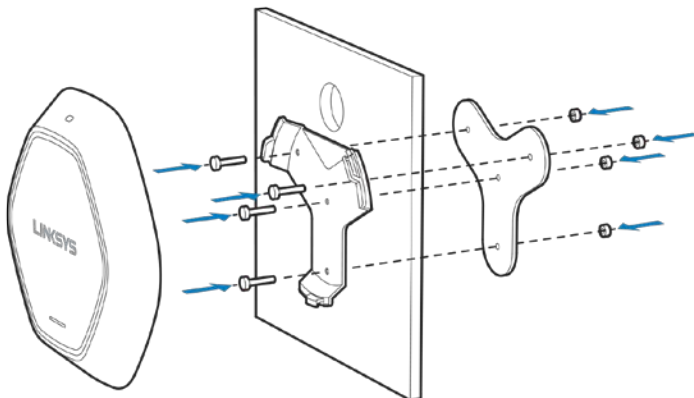
To avoid overheating, do not install your access point if ambient temperatures exceed 104°F (40°C). Install on a flat, stable surface, near the center of your wireless coverage area making sure not to block vents on the sides of the device enclosure.

### Wall Installation

1. Position drilling layout template at the desired location.
2. Drill four screw holes on the mounting surface. If your ethernet cable is routed behind the wall, mark ethernet cable hole as well.
3. Secure the mounting bracket on the wall with anchors and screws.
4. If your ethernet cable is routed behind the wall, cut or drill the ethernet cable hole you marked in Step 2. Feed the ethernet cable through the hole.
5. Connect the ethernet cable and/or AC power adapter to your device.
6. Slide the device into the bracket. Turn clockwise until it locks into place.

### Ceiling Installation

1. Select ceiling tile for mounting and remove tile.
2. Position drilling layout template at the desired location.
3. Drill four screw holes and ethernet cable hole on the surface of ceiling tile.
4. Place back plate on the opposite side of ceiling tile. Secure mounting bracket to the ceiling tile with flathead screw and nut. Route the ethernet cable through the ethernet cable hole.



5. Replace tile in ceiling.
6. Connect the ethernet cable and/or AC power adapter to your device
7. Slide the device into the bracket. Turn access point clockwise until it locks.

**IMPORTANT**—Improper or insecure mounting could result in damage to the device or personal injury. Linksys is not responsible for damages caused by improper mounting.

# Access Point Setup Guide

Once your Linksys access point is installed, choose which way you will manage it:

- Remotely, using the Linksys cloud server, or
- Locally, through a browser-based user interface

## Setup to manage your access point with Linksys cloud server

### Step 1

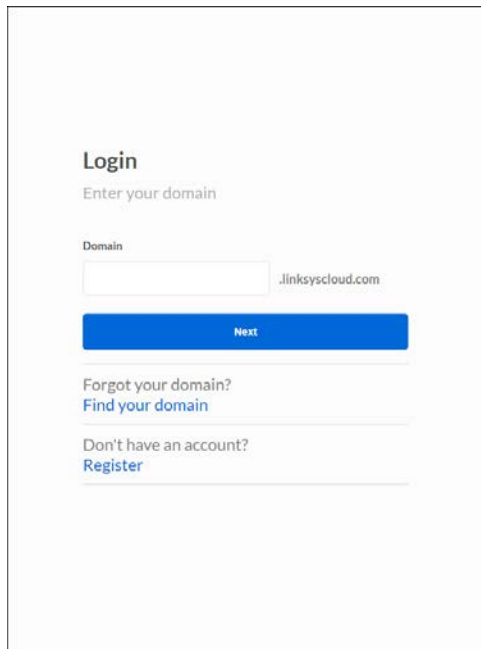
Make sure the access point is powered on and connected with an ethernet cable to your network with internet access. By factory default, the IP address is assigned by a DHCP server. If there is no DHCP server in your network, the default IP address is 192.168.1.252/255.255.255.0.

Log in to the access point's browser-based admin tool locally and click the Configure LAN Settings link. Change the IP address or VLAN so the access point can access the internet.

If the indicator light is off, check that the AC power adapter, or PoE cable, is properly connected on both ends.

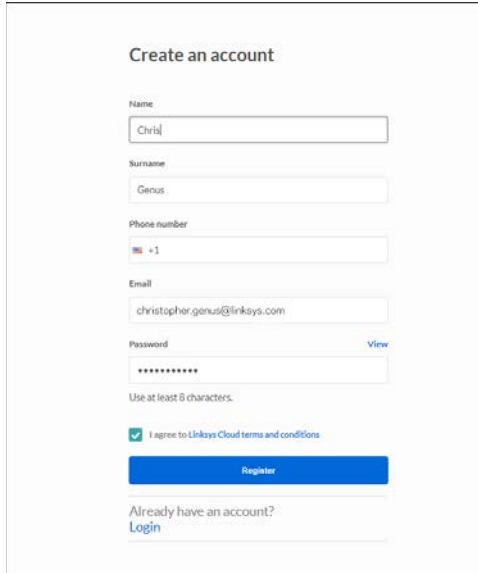
### Step 2

Enter <http://Business.Linksys.com> in a web browser to access the cloud dashboard. If you already have a Linksys Small Business Cloud server account, log in.



The screenshot shows the Linksys cloud dashboard login interface. At the top, it says "Login" followed by the instruction "Enter your domain". Below this is a "Domain" label and a text input field containing ".linksyscloud.com". A blue "Next" button is positioned below the input field. Underneath the button, there are two links: "Forgot your domain? Find your domain" and "Don't have an account? Register".

If not, create an account by completing the on-screen forms. Then, register the access point at the new account.



We'll send you a confirmation email. Click on the link and finish setting up your access point.

## Setup to manage your access point locally with browser-based admin tool

### Step 1

Make sure the access point is powered on and connected with an ethernet cable to your network. If the indicator light is off, check that the AC power adapter, or PoE cable, is properly connected on both ends.

### Step 2

Enter the IP address of your access point. By default, the IP address will be assigned by a DHCP server (usually the network router). If there is no DHCP server on your network, the default IP address is 192.168.1.252/255.255.255.0.

### Step 3

Type in default username: **admin**, and password: **admin**.

### Step 4

Click **Login** and disable the cloud management capability by clicking the **Disable Cloud Manager** button in the upper right corner of the screen.

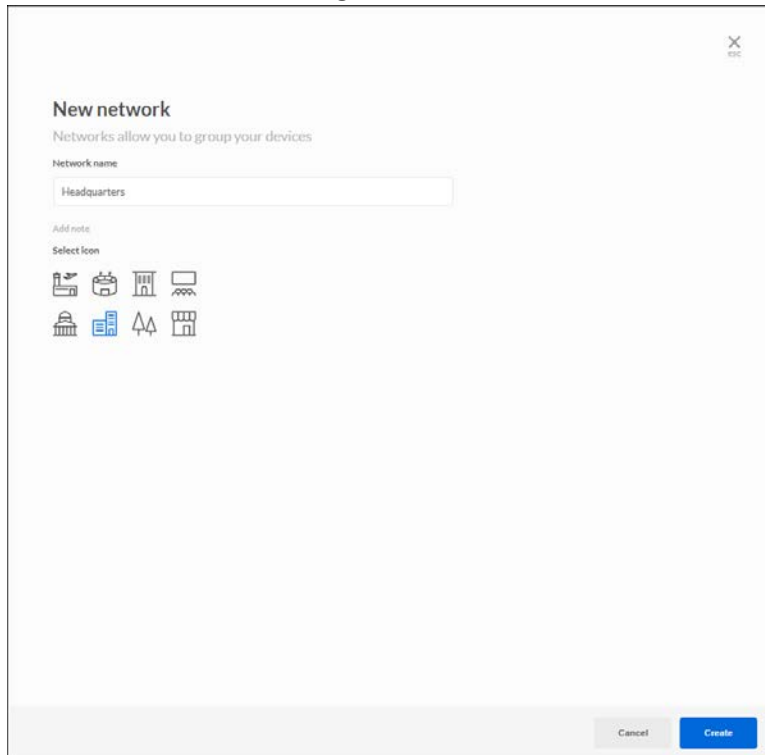
# Cloud Management Interface

Once you are logged in to Business.Linksys.com you can create and manage your networks.

## Networks

### Create network

To create a new network, go to *Networks* and click *New Network*



The screenshot shows a modal window titled "New network" with a close button (X) in the top right corner. Below the title is a subtitle: "Networks allow you to group your devices". There is a text input field labeled "Network name" containing the text "Headquarters". Below this is a section labeled "Add note" with a text area. Underneath is a section labeled "Select icon" with a grid of eight icons: a factory, a calendar, a building, a computer monitor, a classical building, a bar chart, a tree, and a storefront. At the bottom of the modal are two buttons: "Cancel" and "Create".



Choose a name for your network and add any descriptive notes about the network. Choose an icon to represent your network.

New network

Networks allow you to group your devices

Network name


Satellite


Note


Cancel


Five people in Townsvillid


Select icon


















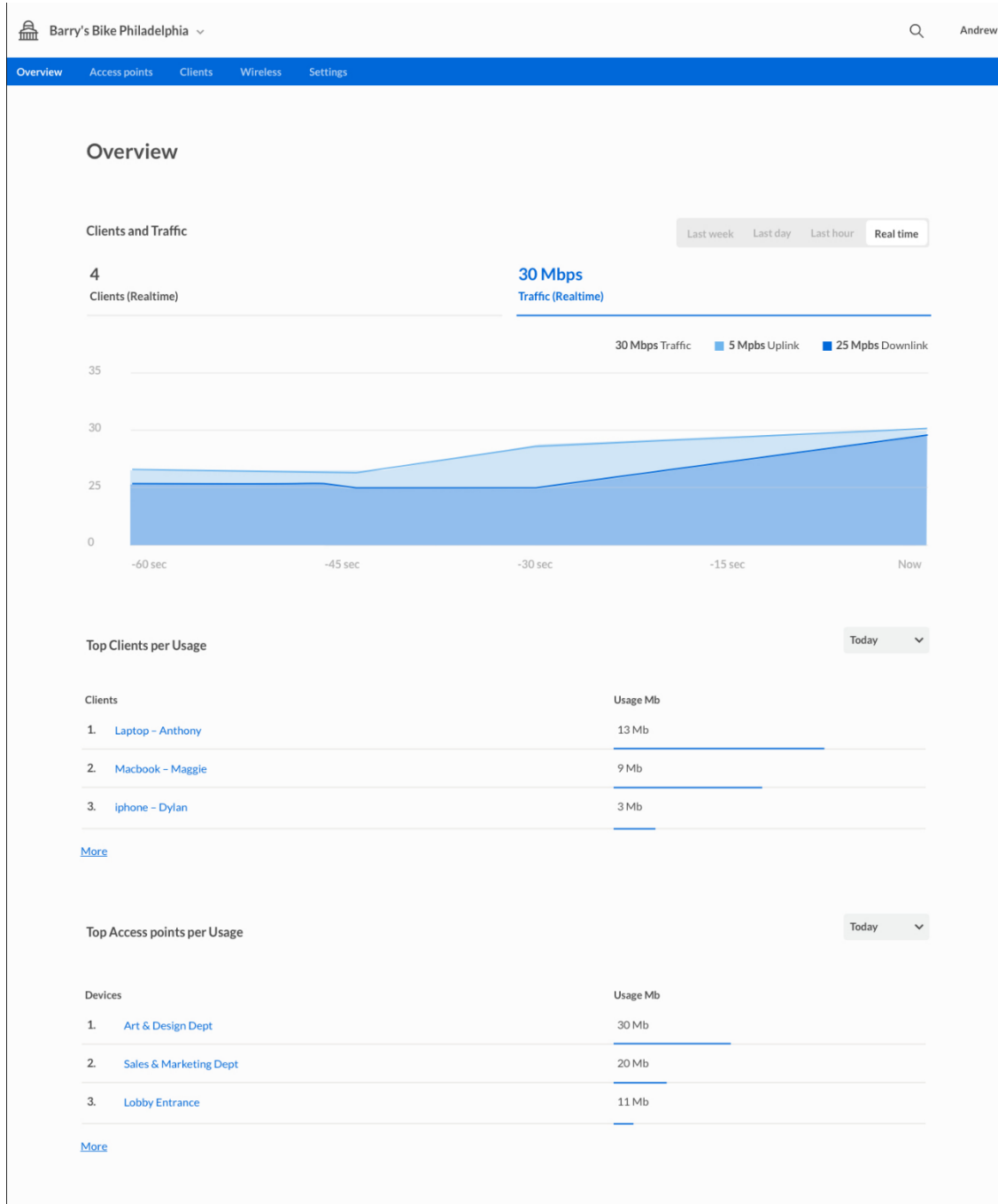


Cancel

Create

9

# Overview

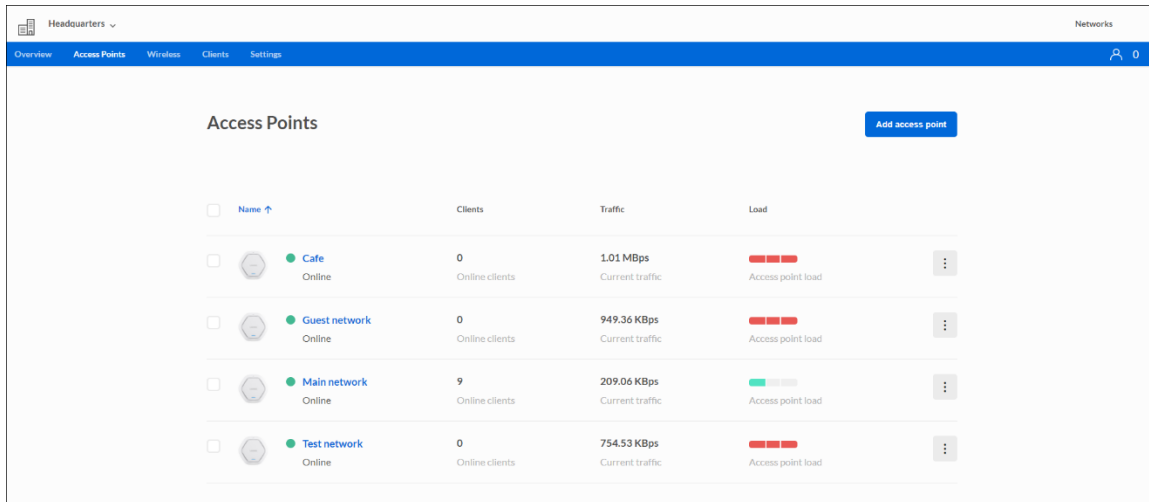






Overview provides information on a network, its access points and client devices:

- Clients and usage
- Top clients per usage
- Top devices per usage
- Channel
- Devices on map

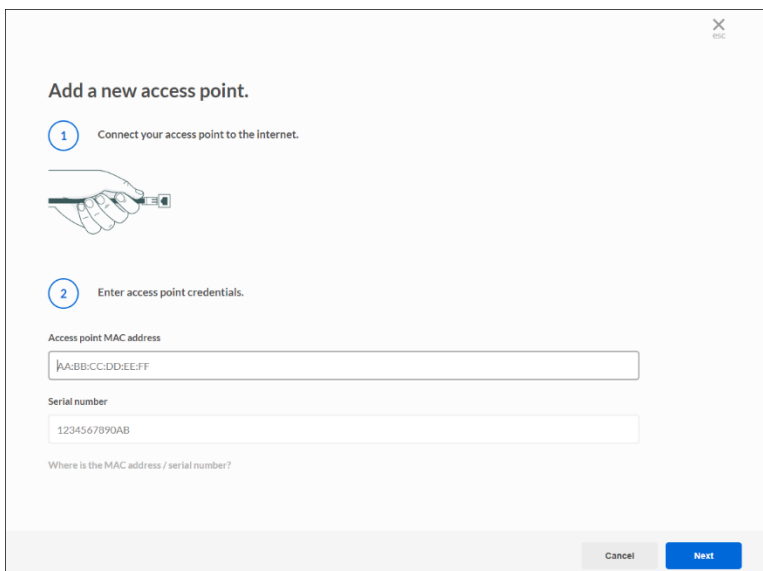
## Access Points

Go to *Networks* and click on a network name. Click on *Access Points* in the menu bar to manage access points on your network.



<input type="checkbox"/>	Name ↑	Clients	Traffic	Load	
<input type="checkbox"/>	 <b>Cafe</b> Online	0 Online clients	1.01 MBps Current traffic	<div><div></div></div> Access point load	⋮
<input type="checkbox"/>	 <b>Guest network</b> Online	0 Online clients	949.36 KBps Current traffic	<div><div></div></div> Access point load	⋮
<input type="checkbox"/>	 <b>Main network</b> Online	9 Online clients	209.06 KBps Current traffic	<div><div></div></div> Access point load	⋮
<input type="checkbox"/>	 <b>Test network</b> Online	0 Online clients	754.53 KBps Current traffic	<div><div></div></div> Access point load	⋮


To add a new access point to the network, click **Add access point**.



✕ ESC

Add a new access point.

1 Connect your access point to the Internet.



2 Enter access point credentials.

Access point MAC address

Serial number

Where is the MAC address / serial number?

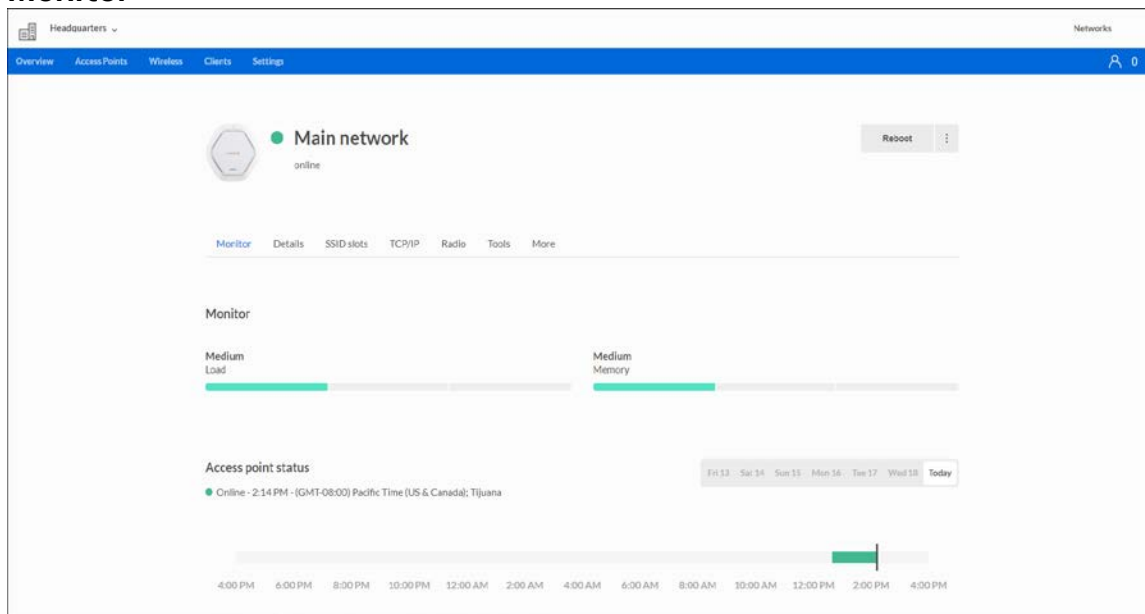
Cancel Next

1. Connect your access point to internet.
2. Enter the MAC address and serial number of the access point you want to add, then click **Next**.

Once the access point has been found, you can rename it and click the **Add device** button.

The screenshot shows a web interface for adding a new access point. At the top, there's a 'Back' button and a close icon. The main heading is 'Add access point'. Below it, a card displays the access point's details: a green dot indicating it's 'Online', the MAC address 'AE:23:0C:D0:90:BB', the vendor 'Linksys', and the firmware version '1.1.03.000'. Below this card, there's a section for 'Access point name' with a text input field containing 'AE:23:0C:D0:90:BB'. At the bottom right, there's a blue 'Add access point' button.

## Monitor



**Load**—Shows the access point's consumption of CPU load.

**Memory**—Shows the access point's consumption of memory.

**Status**—Shows the access point's status for the last seven days

**Clients and usage**—Shows data about clients and traffic for the last seven days.

**Connected clients**—Shows the list of connected clients.

## Details

View whether the access point is connected to the cloud. See the current firmware version and check for updates. You can also see the MAC address, model number, the name you gave it and any device notes or description.

The screenshot shows the 'Details' page for the 'Main Network'. The network is online. The details section includes:

- Connection status:** Connected to the cloud (indicated by a green dot).
- Hardware address:** 58:EF:68:B3:54:D4
- Serial:** 26F10503800052
- Vendor:** Linksys

## Wireless slot

The screenshot shows the 'Wireless slot' page for the 'Main Network'. It displays a table of wireless slots with the following data:

Wireless Name	Authentication	Broadcast	Splash page	Bandwidth limit
First Wireless Name Enabled	WPA2	1	Disabled	None upload / None download
Second Wireless Name Enabled	WPA2	1	Disabled	None upload / None download
Third Wireless Name Enabled	WPA2	1	Disabled	None upload / None download

To add a new wireless name to the device, click **Add wireless name** and select one from the list.

**Authentication**—Shows whether the wireless name is open or requires a password.

**Broadcast**—Shows how many access points in the network are broadcasting the wireless name.

**Splash page**—Shows whether a splash page is enabled or disabled.

**Bandwidth limit**—Shows the bandwidth limit set by the administrator.

# TCP/IP

The screenshot shows the 'Main Network' configuration page with the 'TCP/IP' tab selected. The network status is 'online'. The configuration table is as follows:

TCP/IP	
Configure IP	Server IP
DHCP	192.168.1.176
Gateway	Subnet mask
192.168.1.1	255.255.255.0
Primary DNS server	Secondary DNS server
192.168.1.1	0.0.0.0
VLAN tagging	Untagged VLAN

**Configure IP**—Select Automatic Configuration or Static IP Address.

**Server IP**—Enter an unused IP address from the address range used on your LAN.

**Gateway**—Enter the gateway for IP Server.

**Subnet mask**—Enter the subnet mask for the IP address.

**Primary DNS server**—Enter the DNS Address.

**Secondary DNS server**—Optional.

**VLAN Tagging**—Enter tag of your VLAN.

## Radio

The screenshot shows the 'Main Network' configuration page with the 'Radio' tab selected. The network status is 'online'. The configuration table is as follows:

Radio	
Radio 2.4 GHz	Radio 5 GHz
Radio mode	Radio mode
802.11 b/g/n	802.11 a/n/ac/ax
Channel	Channel
Auto	Auto
TX power	TX power
22 dBm	22 dBm

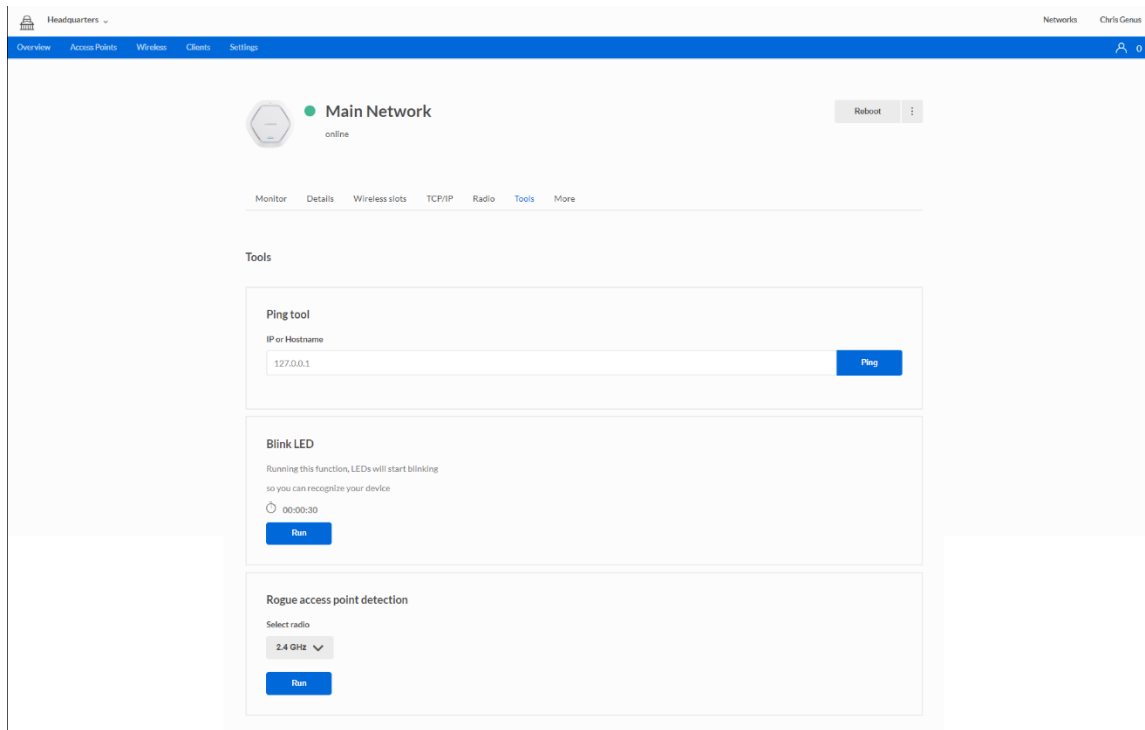
**Radio mode**—Choose a radio mode

**Channel width**--Choose 20 MHz, 40 MHz or 80 MHz

**Channel**—Choose Auto or a channel from 1-5

**TX Power**—Choose the strength of signal when access point is transmitting

## Tools

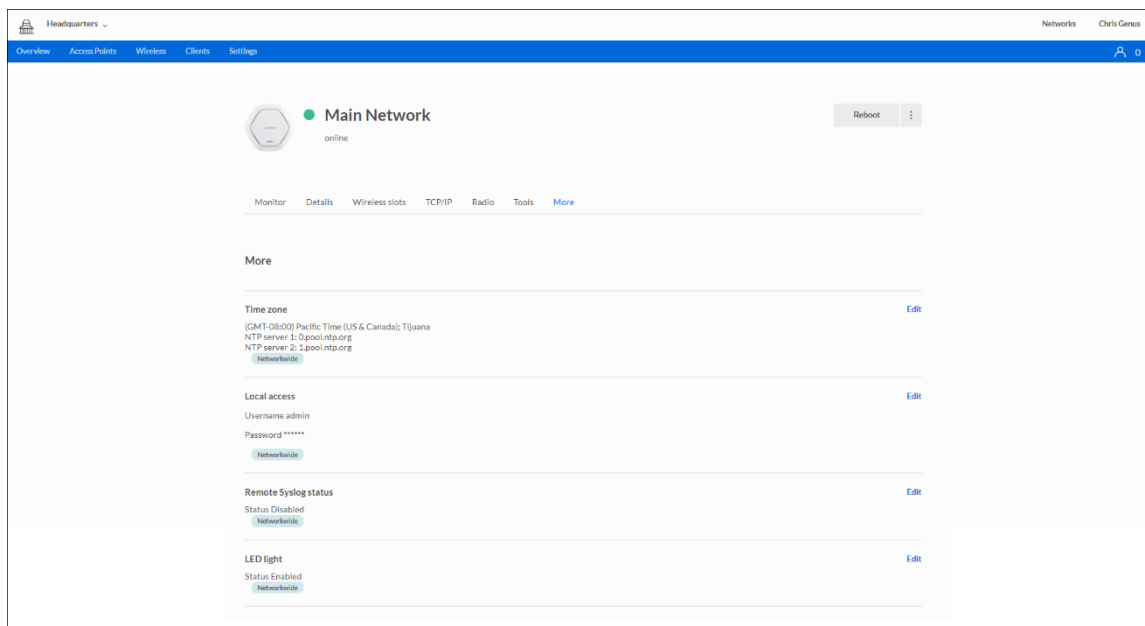


**Ping tool**—Determine the accessibility of a host on the network.

**Blink LED**—Make your device LED blink so you can identify it.

**Rogue access point detection**—Detect an unexpected or unauthorized access point installed in a secure network environment.

## More



**Time zone**—View and edit the device time zone.

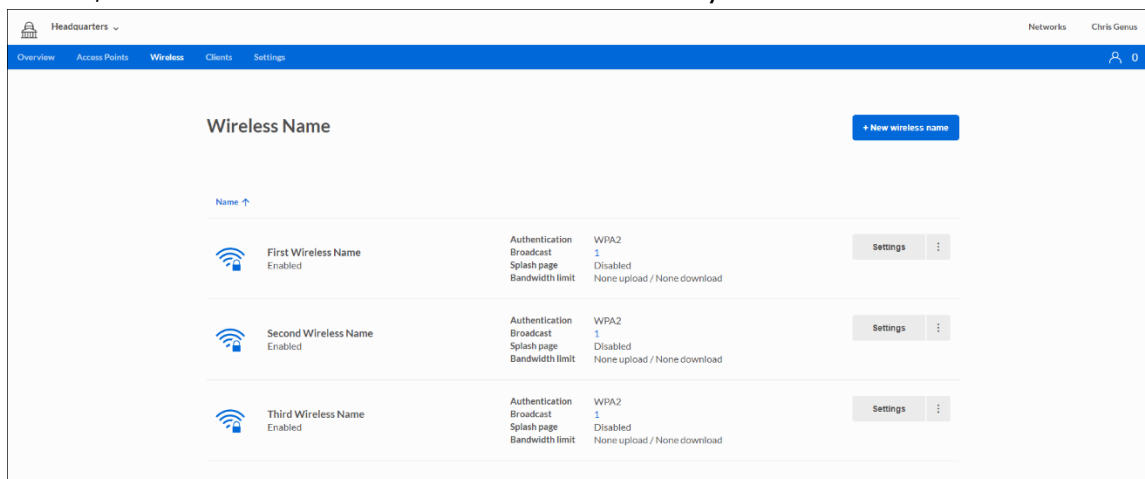
**Local access**—The username and password for local access to device. Default is “admin”.

**Remote syslog status**--Decide whether to send logs to a Syslog server and enter the server’s IP address.

**LED Light**—Device LED status.

## Wireless

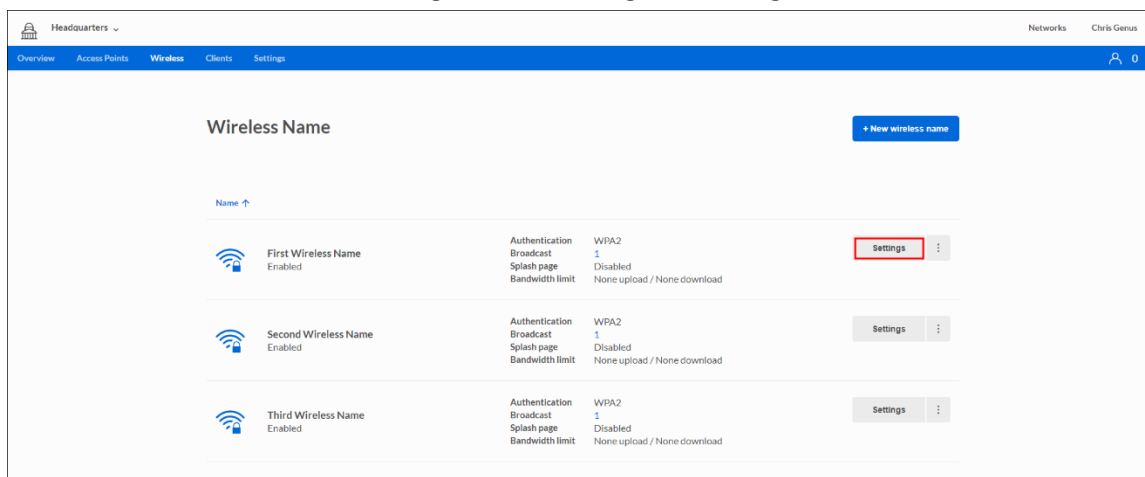
Create, view and edit names for the wireless names on your networks.



To create a new wireless name, choose a network, click *Wireless* and then **+ New wireless name**.

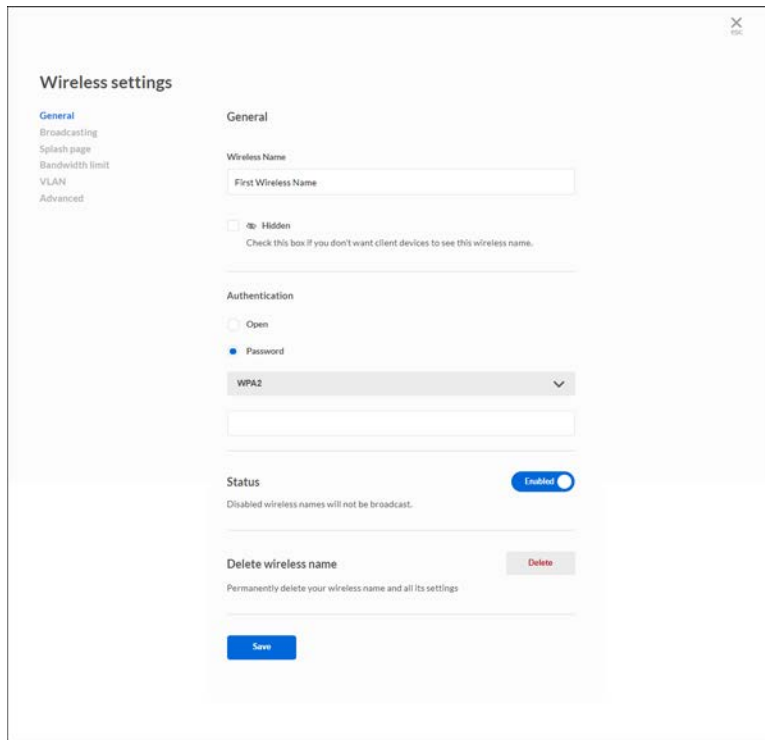
## Wireless Settings

To edit a wireless name’s settings, click settings to the right of a wireless name.





## General



The screenshot shows the 'Wireless settings' page with the 'General' tab selected. On the left, a sidebar lists 'General', 'Broadcasting', 'Splash page', 'Bandwidth limit', 'VLAN', and 'Advanced'. The main content area is titled 'General' and contains the following sections:

- Wireless Name:** A text input field with the placeholder 'First Wireless Name'.
- Hidden:** A checkbox labeled 'Hidden' with a note: 'Check this box if you don't want client devices to see this wireless name.'
- Authentication:** Two radio buttons, 'Open' and 'Password' (which is selected). Below the radio buttons is a dropdown menu currently showing 'WPA2'.
- Status:** A toggle switch labeled 'Enabled' which is currently turned on. Below it, a note states: 'Disabled wireless names will not be broadcast.'
- Delete wireless name:** A section with a 'Delete' button and a note: 'Permanently delete your wireless name and all its settings'.

A 'Save' button is located at the bottom of the form.

**Wireless Name**—Choose a name and decide whether to broadcast or hide that name.

**Authentication**—Choose whether to protect the wireless name with a password or allow all devices to connect. If using a password, choose a security type - either WEP or WPA2.

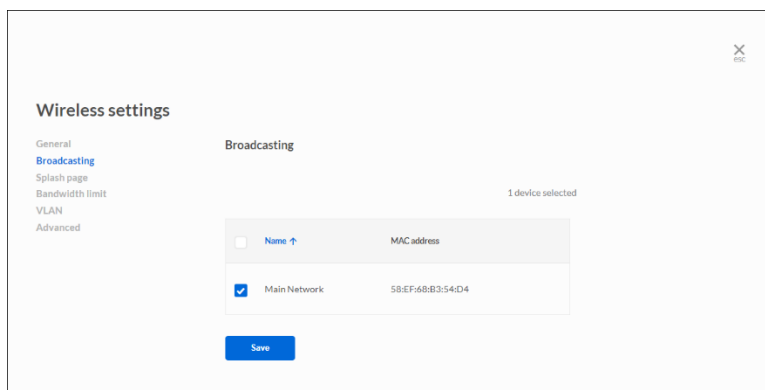
**Status**—Enable or disable the wireless name. Disabled wireless names will not be broadcast.

**Delete wireless name**—Remove the wireless name and all settings from the cloud.

*Be sure to click the Save button when you are finished making changes.*

## Broadcasting

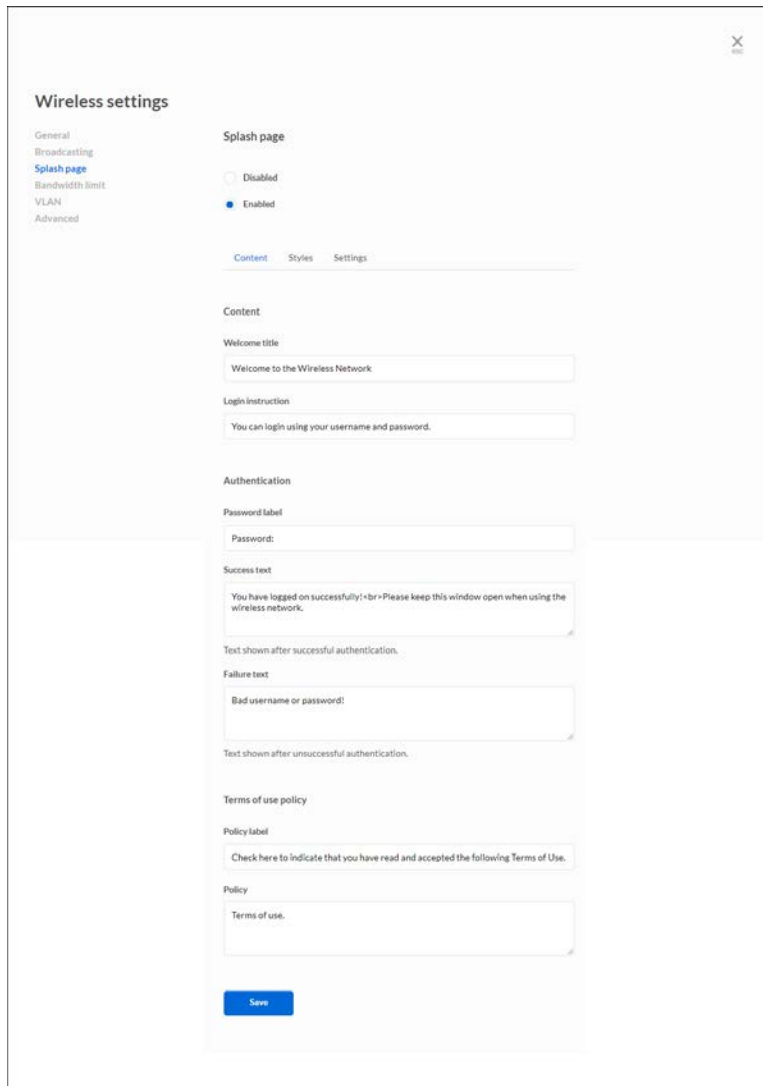
Choose whether to broadcast the wireless names available on an access point.



The screenshot shows the 'Wireless settings' page with the 'Broadcasting' tab selected. The sidebar on the left now highlights 'Broadcasting'. The main content area is titled 'Broadcasting' and includes the following elements:

- A status indicator: '1 device selected'.
- A table with two columns: 'Name' and 'MAC address'. The 'Name' column has a sort arrow pointing up.
- The table contains one entry: 'Main Network' with the MAC address '58:EF:68:B3:54:D4'. The entry is selected, indicated by a checked checkbox in the 'Name' column.
- A 'Save' button is located at the bottom of the table.

## Splash page



The screenshot shows a web interface for configuring wireless settings. On the left is a sidebar with a list of settings: General, Broadcasting, **Splash page** (highlighted in blue), Bandwidth limit, VLAN, and Advanced. The main area is titled 'Wireless settings' and contains a 'Splash page' section. In this section, the 'Enabled' radio button is selected. Below this are three tabs: 'Content', 'Styles', and 'Settings'. The 'Content' tab is active, showing several text input fields: 'Welcome title' (containing 'Welcome to the Wireless Network'), 'Login instruction' (containing 'You can login using your username and password.'), 'Authentication' section with a 'Password label' field (containing 'Password:'), 'Success text' (containing 'You have logged on successfully!<br>Please keep this window open when using the wireless network.'), 'Text shown after successful authentication.' (empty), 'Failure text' (containing 'Bad username or password:'), and 'Text shown after unsuccessful authentication.' (empty). Below these is a 'Terms of use policy' section with a 'Policy label' field (containing 'Check here to indicate that you have read and accepted the following Terms of Use.') and a 'Policy' field (containing 'Terms of use.'). At the bottom of the form is a blue 'Save' button.

**Enabled/Disabled**—Choose whether to send users to a splash page when connecting to the wireless name.

### Content

- Content
  - Welcome title—Create a greeting.
  - Login Instruction—Tell users how to log in.
- Authentication
  - Password label—Label the password field.
  - Success text—Create a message for users who log in successfully.
  - Failure text—Create a message for users who are unsuccessful logging in.

- Term of use policy
  - Policy label—Create message to instruct users to confirm they have read your terms of use.
  - Policy—Create terms of use.

*Be sure to click the Save button when you are finished making changes.*

## Styles

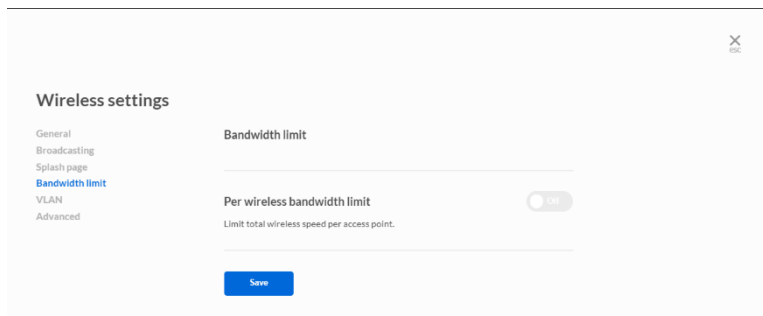
- Style
  - Logo—Upload a file as a logo for your wireless name.
  - Colors—Choose colors for background, text and buttons.

*Be sure to click the Save button when you are finished making changes.*

## Settings

- Client session time out—Set the amount of time (in minutes) that clients can remain connected to the wireless name. Allowed range is 0-1440 minutes.
- Authentication type—Choose whether to require users to enter a password to move beyond the splash page.
- Set password—Choose a password for users to enter.
- Custom landing page (Promotional URL)—Turn on to redirect users to a specific website after authentication.
- URL—Enter the URL of the website users will be redirected to after authentication.

## Bandwidth limit



Wireless settings

- General
- Broadcasting
- Splash page
- Bandwidth limit**
- VLAN
- Advanced

Bandwidth limit

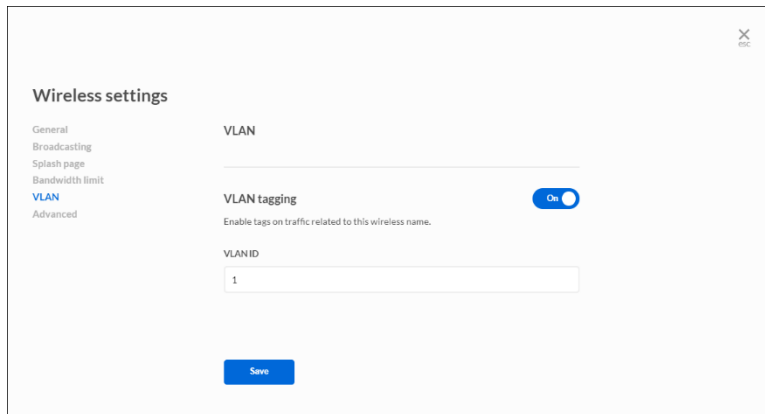
Per wireless bandwidth limit ☐

Limit total wireless speed per access point.

Save

**Per wireless bandwidth limit**—Turn on bandwidth limit and use the slider to set the maximum bandwidth (in Mbps) for devices on the wireless band.

## VLAN

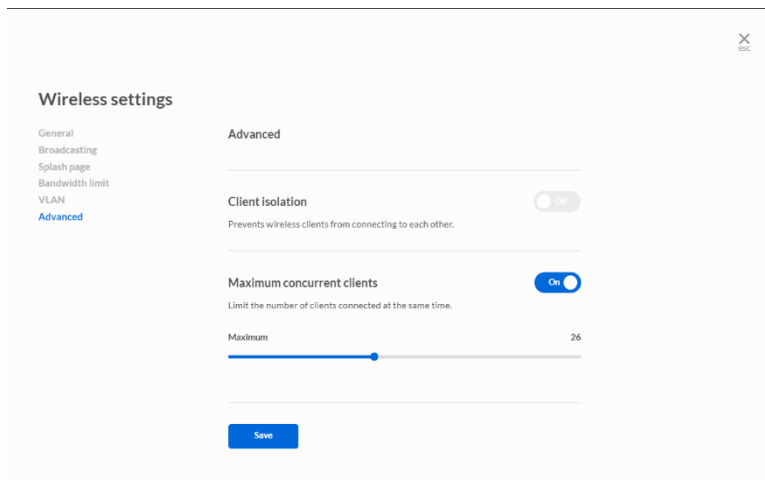


The screenshot shows the 'Wireless settings' page with the 'VLAN' tab selected. On the left sidebar, the menu items are: General, Broadcasting, Splash page, Bandwidth limit, VLAN (highlighted), and Advanced. The main content area is titled 'VLAN' and contains a 'VLAN tagging' toggle switch set to 'On'. Below it, a text input field for 'VLAN ID' contains the number '1'. A 'Save' button is at the bottom.

**VLAN tagging**—Turn on to enable tags on traffic related to this wireless name.

**VLAN ID**—Choose a VLAN ID.

## Advanced



The screenshot shows the 'Wireless settings' page with the 'Advanced' tab selected. On the left sidebar, the menu items are: General, Broadcasting, Splash page, Bandwidth limit, VLAN, and Advanced (highlighted). The main content area is titled 'Advanced' and contains two settings: 'Client isolation' with a toggle switch set to 'Off', and 'Maximum concurrent clients' with a toggle switch set to 'On' and a slider set to '26'. A 'Save' button is at the bottom.

**Client isolation**—When turned on, prevents wireless clients from connecting to each other.

**Maximum concurrent clients**—When turned on, limits the number of clients that can be connected at the same time.

# Clients

Headquarters

Overview

Access Points

Wireless

Clients

Settings

Networks


Chris Genus

0

Clients

Name	Last seen	Wireless Name	Device	Signal	Bandwidth	Policy	
<div><div></div><div>F4:1B:A1:07:44:29</div></div>	31 May - 16:44	First Wireless Name	Main Network	<div></div>	150 Bps	Normal	<div></div>
<div><div></div><div>AC:5F:3E:67:3A:C5</div></div>	31 May - 16:44	First Wireless Name	Main Network	<div></div>	36 Bps	Normal	<div></div>
<div><div></div><div>18:65:9D:DA:89:59</div></div>	31 May - 16:44	First Wireless Name	AccessPoint1	<div></div>	44 Bps	Normal	<div></div>
<div><div></div><div>14:7D:C5:77:1E:90</div></div>	31 May - 16:44	First Wireless Name	AccessPoint1	<div></div>	65 Bps	Normal	<div></div>
<div><div></div><div>04:52:F3:07:5A:9D</div></div>	31 May - 13:32	First Wireless Name	AccessPoint1	<div></div>	866 Bps	Normal	<div></div>

Click the settings icon in the far column to view information about a specific client. You also can change the client's name.

Headquarters

Overview

Access Points

Wireless

Clients

Settings

Networks

Chris Genus

## Details

The screenshot shows the 'Details' tab for a client. At the top, the MAC address 'F4:1B:A1:07:44:29' is displayed with a green dot and the status 'connected'. To the right is a 'Rename' button and a vertical ellipsis menu. Below this is a tab bar with 'Details' (selected) and 'Connection'. The main content area is titled 'Details' and contains several fields: 'MAC address' (F4:1B:A1:07:44:29), 'Name', 'Notes', 'First seen' (31 May - 13:22), and 'Last seen' (31 May - 16:50).

**MAC address**—Client MAC address

**Name**—Custom client label

**Notes**—Client note or description

**First seen**—The first time the client connected

**Last seen**—Last seen client date

## Connection

The screenshot shows the 'Connection' tab for the same client. The top header is identical. The tab bar now has 'Details' and 'Connection' (selected). The main content area is titled 'Connection' and contains three boxes: 'Duration' (2:31:39), 'Traffic' (150 Bps), and 'Signal' (with a Wi-Fi icon). Below these are fields for 'Last seen' (31 May - 16:52), 'Wireless Name' (First Wireless Name), and 'Device' (Main Network).

**Duration**—How long the client has been connected

**Traffic**—The speed of the connection

**Signal**—The strength of the connection

**Last seen**—The last time the client was connected

**Wireless Name**—The Wi-Fi SSID the client connected to

**Device IP address**—The client's IP address

# Settings

Select a network and click on the *Settings* tab. Choose a setting to view or edit.

The screenshot shows a web interface for network management. At the top, there's a header with 'Headquarters' and a dropdown arrow, and 'Networks' on the right. Below the header is a navigation bar with tabs: 'Overview', 'Access Points', 'Wireless', 'Clients', and 'Settings'. The 'Settings' tab is active. The main content area is titled 'Settings' and has three sub-sections: 'General' (selected), 'Access point configuration', and 'Notifications'. The 'General' section contains three rows, each with a label, a value, and an 'Edit' link. The first row is 'Icon' with a building icon and an 'Edit' link. The second row is 'Name' with the value 'Headquarters' and an 'Edit' link. The third row is 'Note' with an empty text area and an 'Edit' link. At the bottom of the 'General' section, there is a 'Delete network.' button with a red 'Delete' label and a warning message: 'Permanently delete your network and all settings.'

Settings		
<b>General</b>		
Icon		<a href="#">Edit</a>
Name	Headquarters	<a href="#">Edit</a>
Note		<a href="#">Edit</a>
Delete network.		<a href="#">Delete</a>
Permanently delete your network and all settings.		

## General

View or edit a network's icon, name and any notes. You can also delete a network from cloud management.

## Access point configuration

View or edit a network's time zone, local login information, remote syslog status and turn the access point's light on or off.

## Notifications

Decide whether to send email notifications to network members when an access point goes offline.

## Account settings

To view or edit your account settings, click on your account name and choose Account settings from the drop-down menu.

The screenshot shows the Linksys Networks dashboard. At the top, there's a navigation bar with the Linksys logo and a user profile section. The user profile section includes a dropdown menu with the following options: christopher.keough@belkin.com, Account settings, Inventory, and Logout. The main content area is titled 'Networks' and contains a table with columns for Status, Clients, and Traffic. The table lists four networks: Headquarters, Satellite, Annex, and Outpost. Each network row shows its status (e.g., 4 Devices for Headquarters), the number of online clients (16 for Headquarters), and the current traffic (3.11 MBps for Headquarters).

Status	Clients	Traffic
<b>Headquarters</b> 4 Devices	16 Online clients	3.11 MBps Current traffic
<b>Satellite</b> 0 Device	0 Online clients	0 Bps Current traffic
<b>Annex</b> 0 Device	0 Online clients	0 Bps Current traffic
<b>Outpost</b> 0 Device	0 Online clients	0 Bps Current traffic

## Account

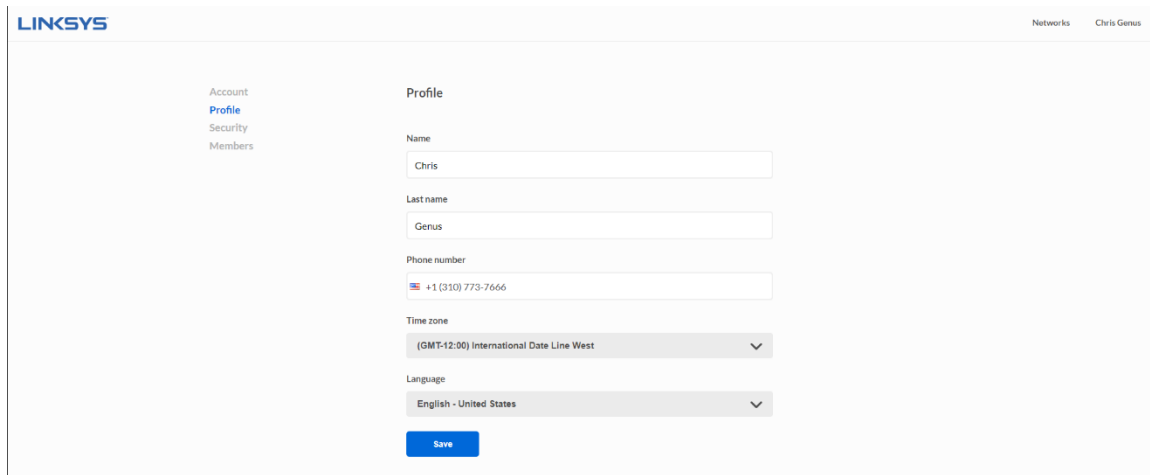
The screenshot shows the Linksys Account settings page. On the left, there's a sidebar with the following options: Account, Profile, Security, and Members. The main content area is titled 'Account' and contains two dropdown menus: 'Time zone' (set to (GMT-12:00) International Date Line West) and 'Language' (set to English - United States). Below these menus is a 'Save' button.

**Time zone**—Set the time zone for your account.

**Language**—Set the language for the user interface.



# Profile



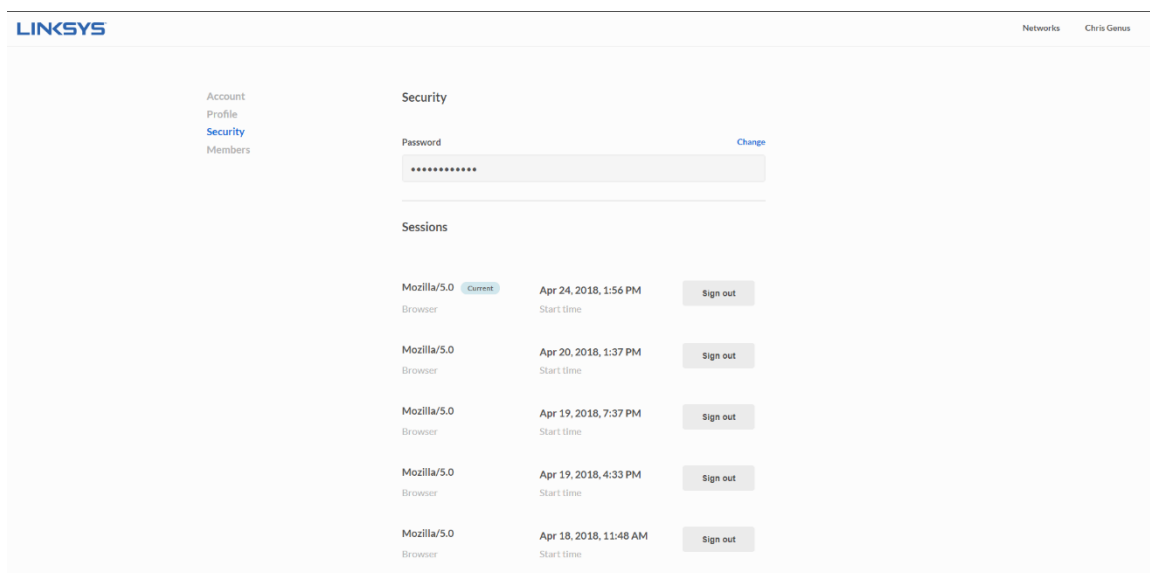
The screenshot shows the Linksys web interface. At the top left is the Linksys logo. At the top right are links for 'Networks' and 'Chris Genus'. On the left side, there is a vertical menu with 'Account', 'Profile' (highlighted in blue), 'Security', and 'Members'. The main content area is titled 'Profile'. It contains several input fields: 'Name' with the value 'Chris', 'Last name' with the value 'Genus', 'Phone number' with a dropdown for country (US) and the value '+1 (310) 773-7666', 'Time zone' with a dropdown showing '(GMT-12:00) International Date Line West', and 'Language' with a dropdown showing 'English - United States'. At the bottom of the form is a blue 'Save' button.

The profile screen shows your personal data:

- Name
- Last name
- Email
- Phone number
- Time zone
- Language

## Security

Change your account password and view information about users logged in to the cloud management account.

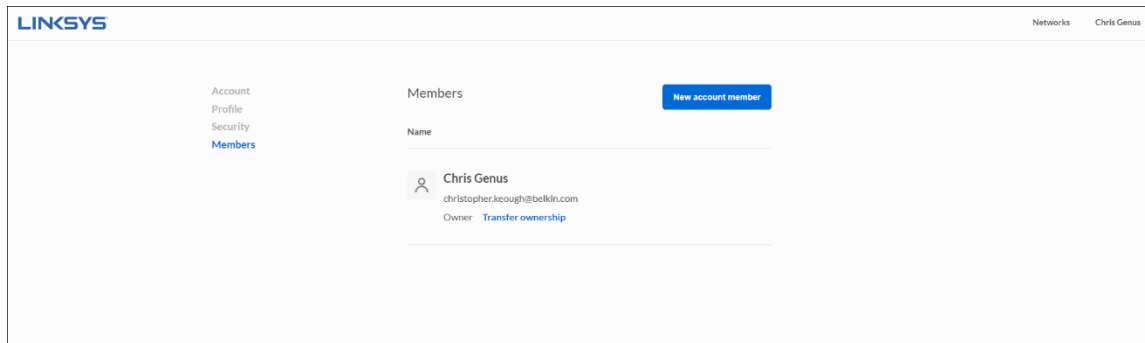


The screenshot shows the Linksys web interface. At the top left is the Linksys logo. At the top right are links for 'Networks' and 'Chris Genus'. On the left side, there is a vertical menu with 'Account', 'Profile', 'Security' (highlighted in blue), and 'Members'. The main content area is titled 'Security'. It has two sections. The first section is 'Password', which shows a masked password field and a blue 'Change' link. The second section is 'Sessions', which displays a table of active sessions. The table has three columns: browser information, start time, and a 'Sign out' button. There are five sessions listed.

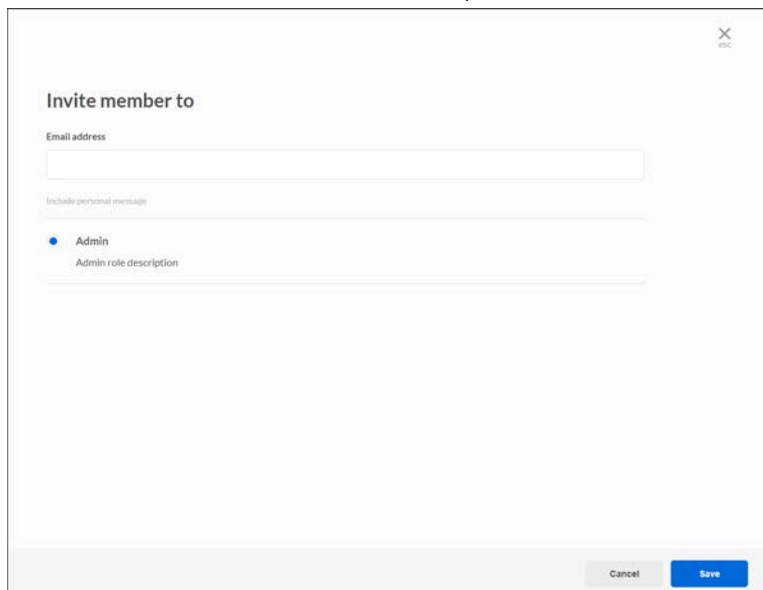
Browser	Start time	Sign out
Mozilla/5.0 Browser	Apr 24, 2018, 1:56 PM	Sign out
Mozilla/5.0 Browser	Apr 20, 2018, 1:37 PM	Sign out
Mozilla/5.0 Browser	Apr 19, 2018, 7:37 PM	Sign out
Mozilla/5.0 Browser	Apr 19, 2018, 4:33 PM	Sign out
Mozilla/5.0 Browser	Apr 18, 2018, 11:48 AM	Sign out

## Members

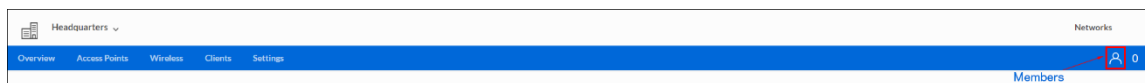
Lists all the members of the account.



To add a new member to an account, click on **New account member**.

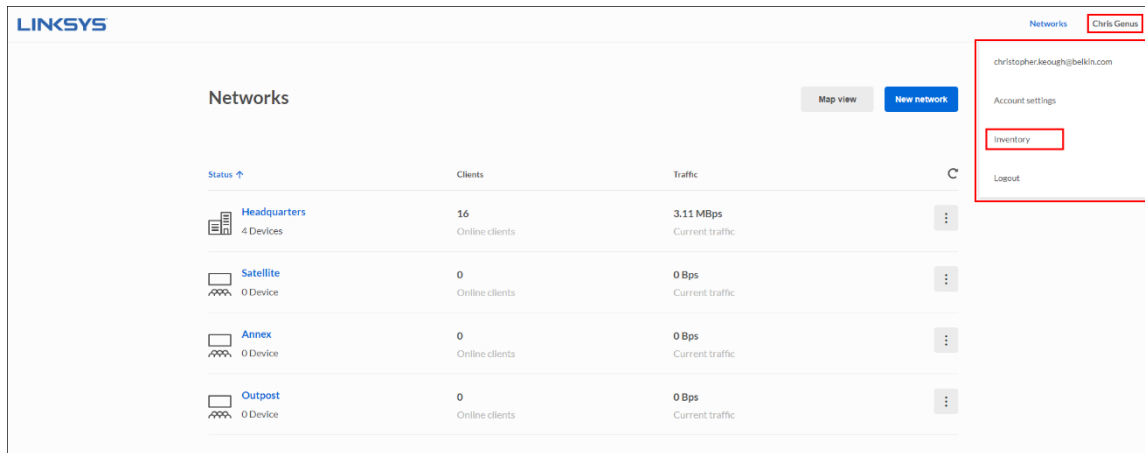


You can also add a new member to your network by clicking the person icon on the far right of the menu bar. Click *Invite Member* and enter an email address and assign permissions (Manager or Viewer).



To transfer ownership of your account, click *Transfer ownership* and enter the email address of the member you would like to give ownership.

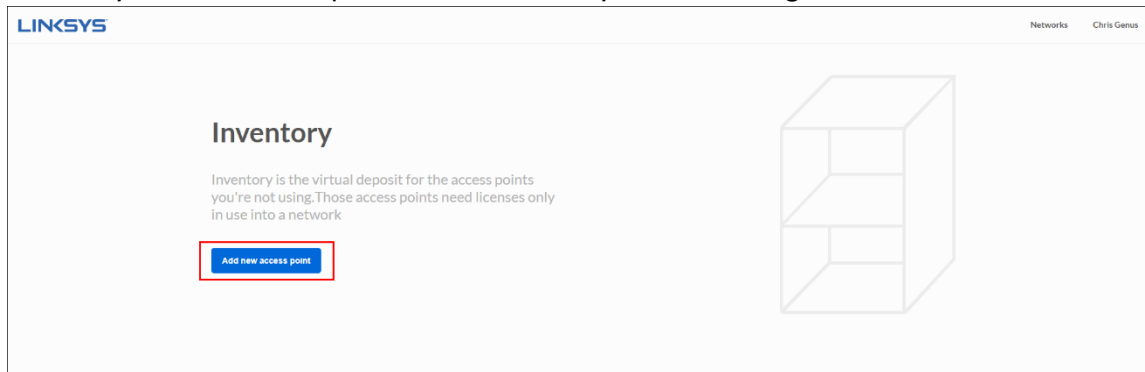
# Inventory



The screenshot shows the Linksys Networks dashboard. The main content area is titled "Networks" and features a table with columns for "Status", "Clients", and "Traffic". The table lists four networks: Headquarters (4 Devices, 16 Online clients, 3.11 MBps Current traffic), Satellite (0 Device, 0 Online clients, 0 Bps Current traffic), Annex (0 Device, 0 Online clients, 0 Bps Current traffic), and Outpost (0 Device, 0 Online clients, 0 Bps Current traffic). A sidebar on the right contains a user profile for "Chris Genus" with the email "christopher.keough@belkin.com", and links for "Account settings", "Inventory" (highlighted with a red box), and "Logout".

Status	Clients	Traffic
<b>Headquarters</b> 4 Devices	16 Online clients	3.11 MBps Current traffic
<b>Satellite</b> 0 Device	0 Online clients	0 Bps Current traffic
<b>Annex</b> 0 Device	0 Online clients	0 Bps Current traffic
<b>Outpost</b> 0 Device	0 Online clients	0 Bps Current traffic

Inventory is the virtual deposit for the devices you're not using.



The screenshot shows the Linksys Inventory page. The main heading is "Inventory". Below it, a text block explains: "Inventory is the virtual deposit for the access points you're not using. Those access points need licenses only in use into a network". A blue button labeled "Add new access point" is highlighted with a red box. To the right of the text is a 3D wireframe illustration of a storage bin.

To add a device, click the **Add new access point** button.

Connect your device to the internet

Enter the MAC address and serial number of the device you want to add. Click the **Next** button.

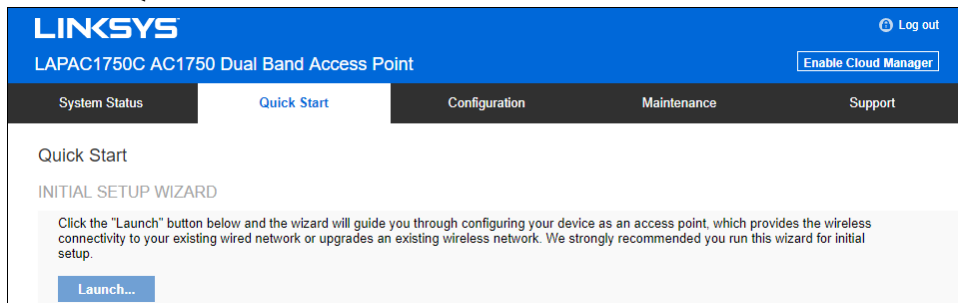
Once the device has been found, rename it and click the **Add access point** button.

# Local Management Interface

## Setup Wizard (Local Administration)

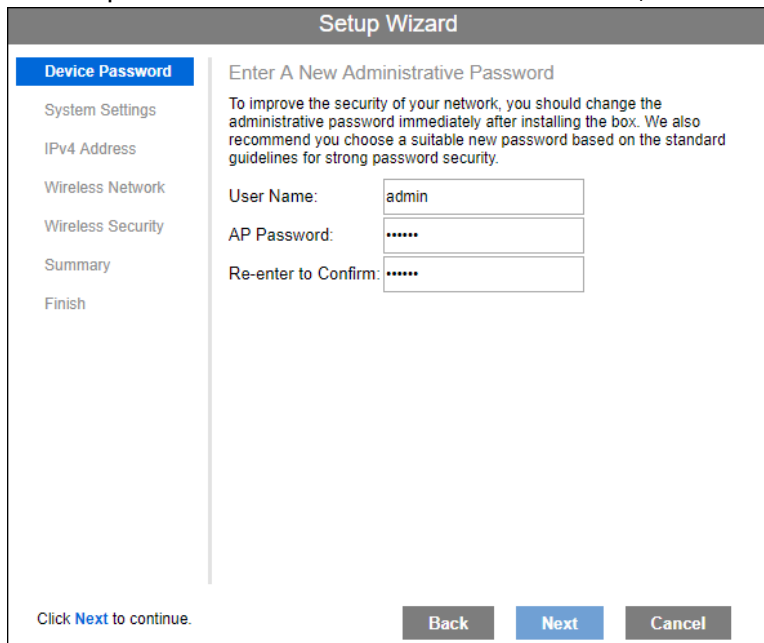
If you are setting up the access point as a standalone device, run the Setup Wizard. If the access point will be part of a cluster – master or slave - go to *Configuration > Cluster > Settings & Status* page instead.

1. Click the *Quick Start* tab on the main menu.



The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start' (selected), 'Configuration', 'Maintenance', and 'Support'. The 'Quick Start' section contains the 'INITIAL SETUP WIZARD' with a description and a 'Launch...' button.

2. On the first screen, click **Launch...**
3. Set the password on the *Device Password* screen, if desired.



The screenshot shows the 'Setup Wizard' screen with the 'Device Password' tab selected. It prompts the user to 'Enter A New Administrative Password' and provides instructions on password security. The form includes fields for 'User Name' (pre-filled with 'admin'), 'AP Password', and 'Re-enter to Confirm'. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

4. Configure the time zone, date and time for the device on *System Settings* screen.

The screenshot shows the 'Setup Wizard' window with the 'System Settings' tab selected. The left sidebar lists 'Device Password', 'System Settings' (highlighted), 'IPv4 Address', 'Wireless Network', 'Wireless Security', 'Summary', and 'Finish'. The main content area is titled 'Enter Device Name And System Time' and includes instructions to 'Set a meaningful name for this box, and configure time.' The 'Host Name' field contains 'lap354d4'. The 'Current Clock' shows '2018/06/01 Fri 11:51:03 (-08:00)'. There are two radio buttons: 'Configure Manually' (unselected) and 'Sync with NTP server Automatically' (selected). The 'Date' is set to 'Jan 1 2013' and the 'Time' is '00:00:00'. The 'Time Zone' is '(GMT-08:00) Pacific Time (US & Canad...)'. There is an unchecked checkbox for 'Automatically adjust clock for daylight saving changes'. The 'Start Time' and 'End Time' are both set to 'First Sun Jan 00:00'. The 'Offset' is '15 Minutes'. The 'NTP Server' is '0.pool.ntp.org'. At the bottom, there is a link 'Click Next to continue.' and three buttons: 'Back', 'Next' (highlighted), and 'Cancel'.

5. On the *IPv4 Address* screen configure the IP address of the device (*Static* or *Automatic*) then click **Next**.

The screenshot shows the 'Setup Wizard' window with the 'IPv4 Address' tab selected. The left sidebar lists 'Device Password', 'System Settings', 'IPv4 Address' (highlighted), 'Wireless Network', 'Wireless Security', 'Summary', and 'Finish'. The main content area is titled 'Enter Device IPv4 Address' and includes instructions to 'Select IP address type either dynamic or static IP Address.' The 'IP Settings' dropdown is set to 'Automatic Configuration'. The 'Local IP Address' is '192.168.1.176', the 'Subnet Mask' is '255.255.255.0', the 'Default Gateway' is '192.168.1.1', the 'Primary DNS' is '192.168.1.1', and the 'Secondary DNS' is '0.0.0.0'. At the bottom, there is a link 'Click Next to continue.' and three buttons: 'Back', 'Next' (highlighted), and 'Cancel'.

6. Set the SSID information on the *Wireless Network* screen. Click **Next**. If you want to configure more than four SSIDs, go to *Configuration > Wireless > Basic Settings*. The access point supports up to eight SSIDs per radio.

7. On the *Wireless Security* screen, configure the wireless security settings for the device. Click **Next**. If you are looking for security options that are not available in the wizard, go to *Configuration > Wireless Security* page. The access point supports more sophisticated security options there.

8. On the *Summary* screen, check the data to make sure they are correct and then click **Submit** to save the changes.

**Setup Wizard**

- ✓ Device Password
- ✓ System Settings
- ✓ IPv4 Address
- ✓ Wireless Network
- ✓ Wireless Security
- Summary**
- Finish

**Summary**

Review your wireless security settings. If data is correct, you may like to write it down or copy and paste to a file as you need this data when you add wireless clients into your wireless network.

Select Your Radio: Radio 1

SSID	Wireless Network	Security Type	Security Key
1	First Wireless Name	Disabled	
2		Disabled	
3		Disabled	
4		Disabled	

Click **Submit** to save changes.

**Back** **Submit** **Cancel**


9. Click **Finish** to leave the wizard.

**Setup Wizard**

- ✓ Device Password
- ✓ System Settings
- ✓ IPv4 Address
- ✓ Wireless Network
- ✓ Wireless Security
- ✓ Summary
- Finish**

**Completing Your Setup Wizard**

You have successfully set up your device as an access point.



Click **Finish** to close this wizard.

**Back** **Finish** **Cancel**

# Administration

## User Accounts

Go to *Configuration > Administration* and select *User Accounts* to manage user accounts. The access point supports up to five users: one administrator and four normal users.

The screenshot shows the Linksys web interface for the LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. The left sidebar shows the 'Administration' menu with 'User Accounts' selected. The main content area is titled 'User Accounts' and contains a 'User Account Table' with the following data:

	User Name	User Level	New Password	Confirm New Password
<input type="checkbox"/>	admin	Read/Write Access		

Below the table are 'Add' and 'Delete' buttons. At the bottom right of the table are 'Save' and 'Cancel' buttons.

### User Account Table

#### User Name

Enter the User Name to connect to the access point's admin interface. User Name is effective once you save settings.

User Name can include up to 63 characters. Special characters are allowed.

#### User Level

Only administrator account has Read/Write permission to the access point's admin interface. All other accounts have Read Only permission.



<b>New Password</b>	Enter the Password to connect to the access point's admin interface.  Password must be between 4 and 63 characters. Special characters are allowed.
<b>Confirm New Password</b>	Re-enter password.

## Time

Go to *Configuration > Administration* and select *Time* to configure system time of the device.

The screenshot shows the Linksys configuration interface for a LAPAC1750C AC1750 Dual Band Access Point. The 'Configuration' tab is active, and the 'Time' sub-tab is selected in the left sidebar. The main content area displays the 'Time' configuration page. At the top, it shows the 'Current Clock' as 2018/06/01 Fri 12:18:17 (-08:00). Below this, there are two radio buttons: 'Manually' (unselected) and 'Sync with NTP server Automatically' (selected). The 'Manually' section includes fields for 'Date' (Jan 1, 2013) and 'Time' (00:00:00). The 'Sync with NTP server Automatically' section includes a 'Time Zone' dropdown set to '(GMT-08:00) Pacific Time (US & Canada); Tijuana'. Below this is a checkbox for 'Automatically adjust clock for daylight saving changes' which is unchecked. Further down are fields for 'Start Time' and 'End Time', both set to 'First Sun Jan 00:00'. An 'Offset' field is set to '60 Minutes'. At the bottom, there are two 'NTP Server' fields: 'NTP Server 1' set to '0.pool.ntp.org' and 'NTP Server 2' set to '1.pool.ntp.org'. Both have a '(Max 128 characters)' note. 'Save' and 'Cancel' buttons are at the bottom right.

Time	
<b>Current Time</b>	Display current date and time of the system.
<b>Manually</b>	Set date and time manually.
<b>Automatically</b>	When enabled (default setting) the access point will get the current time from a public time server.

<b>Time Zone</b>	Choose the time zone for your location from the drop-down list. If your location observes daylight saving time, enable "Automatically adjust clock for daylight saving changes."
<b>Start Time</b>	Specify the start time of daylight saving.
<b>End Time</b>	Specify the end time of daylight saving.
<b>Offset</b>	Select the adjusted time of daylight saving.
<b>NTP</b>	
<b>NTP Server 1</b>	<p>Enter the primary NTP server. It can be an IPv4 address or a domain name.</p> <p>Valid characters include alphanumeric characters, "_", "-", and ".". Maximum length is 64 characters.</p>
<b>NTP Server 2</b>	<p>Enter the secondary NTP server. It can be an IPv4 address or a domain name.</p> <p>Valid characters include alphanumeric characters, "_", "-", and ".". Maximum length is 64 characters.</p>

## Log Settings

Go to *Configuration > Administration* and select *Log Settings* to configure logs. Logs record various types of activity on the access point. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

The screenshot shows the Linksys web interface for the LAPAC1750C AC1750 Dual Band Access Point. The 'Log Settings' page is displayed under the 'Configuration' tab. The left sidebar shows the 'Administration' menu with options like User Accounts, Time, Log Settings, Management Access, SSL Certificate, and LED Lighting. The main content area is titled 'Log Settings' and contains three main sections: 'Log Types' with checkboxes for 'Unauthorized Login Attempt', 'Authorized Login', 'System Error Messages', and 'Configuration Changes'; 'Email Alert' with fields for 'SMTP Server', 'Port', 'Username', 'Password', and 'E-Mail Address for Logs'; and 'Syslog Notification' with a checkbox for 'Syslog Notification', a dropdown for 'IP Address Type', and a field for 'Server IP Address'. There are 'Save' and 'Cancel' buttons at the bottom right.

### Log Types

#### Log Types

Select events to log. Checking all options increase the size of the log, so enable only events you believe are required.

### Email Alert

#### Email Alert

Enable email alert function.

#### SMTP Server

Enter the e-mail server that is used to send logs. It can be an IPv4 address or a domain name.

Valid characters include alphanumeric characters, "\_", "-" and ".".

Maximum length is 64 characters.

#### Data Encryption

Enable if you want to use data encryption.

#### Port

Enter the port for the SMTP server. The port is a value from 1 to 65535 and default is 25.

<b>Username</b>	Enter the Username to login to your SMTP server. The Username can include up to 32 characters. Special characters are allowed.
<b>Password</b>	Enter the Password to login to your SMTP server. The Password can include up to 32 characters. Special characters are allowed.
<b>Email Address for Logs</b>	Enter the email address the log messages are to be sent to. Valid characters include alphanumeric characters, "_", "-", "." and "@". Maximum length is 64 characters.
<b>Log Queue Length</b>	Enter the length of the queue: up to 500 log messages. The default is 20 messages. When messages reach the set length the queue will be sent to the specified email address.
<b>Log Time Threshold</b>	Enter the time threshold (in seconds) used to check if the queue is full. It's a value from 1 to 600 and default is 600 seconds.
<b>Syslog</b>	
<b>Syslog Notification</b>	Enable Syslog notification.
<b>IP Type</b>	Select the IP type of the syslog server: IPv4 or IPv6.
<b>Server IP Address</b>	Enter the IPv4 or IPv6 address of syslog server here.

Go to *Configuration > Administration* and select *Management Access* page to configure the management methods of the access point.

37

<b>Web Access</b>	
<b>HTTP</b>	<p>HTTP (Hyper Text Transfer Protocol) is the standard for transferring files (text, graphic images and other multimedia files) on the World Wide Web.</p> <p>Enable to allow Web access by HTTP protocol.</p>
<b>HTTP Port</b>	Specify the port for HTTP. It can be 80 (default) or from 1024 to 65535.
<b>HTTP to HTTPS Redirect</b>	<p>Enable to redirect Web access of HTTP to HTTPS automatically.</p> <p>This field is available only when HTTP access is disabled.</p>
<b>HTTPS</b>	<p>HTTPS (Hypertext Transfer Protocol Secure) can provide more secure communication with the SSL/TLS protocol, which support data encryption to HTTP clients and servers.</p> <p>Enable to allow Web access by HTTPS protocol.</p>
<b>HTTPS Port</b>	Specify the port for HTTPS. It can be 443 (default) or from 1024 to 65535.
<b>From Wireless</b>	Enable wireless devices to connect to access point's admin page. Disabled by default.
<b>Access Control</b>	By default, no IP addresses are prohibited from accessing the device's admin page. You can enable access control and enter specified IP addresses for access. Four IPv4 and four IPv6 addresses can be specified.
<b>SNMP Settings</b>	
<b>SNMP</b>	<p>Simple Network Management Protocol (SNMP) is a network monitoring and management protocol.</p> <p>Enable or disable SNMP function here. Disabled by default.</p>
<b>Contact</b>	<p>Enter contact information for the access point.</p> <p>The contact includes 1 to 32 characters. Special characters are allowed.</p>
<b>Location</b>	<p>Enter the area or location where the access point resides.</p> <p>The location includes 1 to 32 characters. Special characters are allowed.</p>

SNMP v1/v2 Settings	
<b>Get Community</b>	<p>Enter the name of Get Community. Get Community is used to read data from the access point and not for writing data into the access point.</p> <p>Get Community includes 1 to 32 characters. Special characters are allowed.</p>
<b>Set Community</b>	<p>Enter the name of Set Community. Set Community is used to write data into the access point.</p> <p>The Set Community includes 1 to 32 characters. Special characters are allowed.</p>
SNMP v3 Settings	
<b>SNMP v3 Settings</b>	<p>Configure the SNMPv3 settings if you want to use SNMPv3.</p> <p>Username: Enter the username. It includes 0 to 32 characters. Special characters are allowed.</p> <p>Authentication Protocol: None or HMAC-MD5.</p> <p>Authentication Key: 8 to 32 characters. Special characters are allowed.</p> <p>Privacy Protocol: None or CBC-DES.</p> <p>Privacy Key: 8 to 32 characters. Special characters are allowed.</p>
Access Control	
<b>Access Control</b>	<p>When SNMP is enabled, any IP address can connect to the access point MIB database through SNMP. You can enable access control to allow specified IP addresses. Two IPv4 and two IPv6 addresses can be specified.</p>
SNMP Trap	
<b>Trap Community</b>	<p>Enter the Trap Community server. It includes 1 to 32 characters. Special characters are allowed.</p>
<b>Trap Destination</b>	<p>Two Trap Community servers are supported: can be IPv4 or IPv6.</p>

## SSL Certificate

Go to *Configuration > Administration* and select *SSL Certificate* to manage the SSL certificate used by HTTPS.

The screenshot shows the Linksys configuration interface for the LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. The left sidebar lists various configuration categories, with 'Administration' expanded to show 'User Accounts', 'Time', 'Log Settings', 'Management Access', 'SSL Certificate' (selected), and 'LED Lighting'. Below 'Administration' are 'LAN', 'Wireless', 'Captive Portal', and 'Cluster'. The main content area is titled 'SSL Certificate' and contains two sections: 'EXPORT/INSTALL TO/FROM LOCAL PC' and 'EXPORT/INSTALL TO/FROM TFTP SERVER'. The first section has buttons for 'Export Certificate' and 'Install Certificate', with a file selection interface for the latter. The second section has buttons for 'Export' and 'Install', with input fields for 'Destination File' and 'Source File' and a 'TFTP Server' IP address field.

### Export/Restore to/from Local PC

#### Export SSL Certificate

Click to export the SSL certificate.

#### Install Certificate

Browse to choose the certificate file. Click Install Certificate.

### Export to TFTP Server

#### Destination File

Enter the name of the destination file.

#### TFTP Server

Enter the IP address for the TFTP server. Only support IPv4 address here.

#### Export

Click to export the SSL certificate to the TFTP server.



Restore from TFTP Server	
Source File	Enter the name of the source file.
TFTP Server	Enter the IP address for the TFTP server. Only support IPv4 address here.
Install	Click to install the file to the device.

## LED Lighting

Go to *Configuration > Administration* and select *LED Lighting* to turn off/on the LED on the front/top of the access point.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. The left sidebar shows the 'Administration' menu with options like 'User Accounts', 'Time', 'Log Settings', 'Management Access', 'SSL Certificate', and 'LED Lighting' (highlighted). Below the sidebar, the 'LED Lighting' configuration page is displayed. It features a toggle switch for 'LED Lighting' which is currently set to 'Enable'. There are 'Save' and 'Cancel' buttons at the bottom right of the configuration area.

# LAN

## Network Setup

Go to *Configuration > LAN > Network Setup* to configure basic device settings, VLAN settings and settings for the LAN interface, including static or dynamic IPv4/IPv6 address assignment.

### TCP/IP

#### Host Name

Assign a host name to this access point. Host name consists of 1 to 15 characters. Valid characters include A-Z, a-z, 0-9 and -. Character cannot be first and last character of hostname and hostname cannot be composed of all digits.

#### VLAN

Enables or disables VLAN function.

<b>Untagged VLAN</b>	<p>Enables or disables VLAN tagging. If enabled (default), traffic from the LAN port is untagged when the following conditions are met: 1) VLAN ID is equal to Untagged VLAN ID and 2) untagged traffic can be accepted by LAN port. If disabled, traffic from the LAN port is always tagged and only tagged traffic can be accepted from LAN port.</p> <p>By default all traffic on the access point uses VLAN 1, the default untagged VLAN. All traffic will be untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a SSID.</p>
<b>Untagged VLAN ID</b>	<p>Specifies a number between 1 and 4094 for the untagged VLAN ID. The default is 1. Traffic on the VLAN that you specify in this field is not be tagged with a VLAN ID when forwarded to the network.</p> <p>Untagged VLAN ID field is active only when untagged VLAN is enabled.</p> <p>VLAN 1 is the default for both untagged VLAN and management VLAN.</p>
<b>Management VLAN</b>	<p>The VLAN associated with the IP address you use to connect to the access point. Provide a number between 1 and 4094 for the Management VLAN ID. The default is 1.</p>
<b>IPv4/v6</b>	
<b>IP Settings</b>	Select Automatic Configuration or Static IP Address.
<b>IP Address</b>	Enter an unused IP address from the address range used on your LAN.
<b>Subnet Mask</b>	Enter the subnet mask for the IP address above.
<b>Default Gateway</b>	Enter the gateway for the IP address above.
<b>Primary DNS</b>	Enter the DNS address.
<b>Secondary DNS</b>	Optional. If entered, this DNS will be used if the Primary DNS does not respond.

## Advanced

Go to *Configuration > LAN > Advanced* this screen to configure advanced network settings of the access point.

The screenshot shows the Linksys web interface for the LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. The left sidebar shows a tree view with 'Administration' expanded, containing 'LAN' (selected), 'Network Setup', 'Advanced' (selected), 'Wireless', 'Captive Portal', and 'Cluster'. The main content area is titled 'Advanced' and contains several sections:

- PORT SETTINGS**
  - Auto Negotiation: ☒ Enable. Operational Auto Negotiation: Enabled.
  - Port Speed: 100M (dropdown). Operational Port Speed: 1000Mbps.
  - Duplex Mode: Full (dropdown). Operational Duplex Mode: Full.
  - Flow Control: ☐ Enable.
- 802.1X SUPPLICANT**
  - 802.1X Supplicant: ☐ Enable.
  - Authentication Type: ☒ Authentication via MAC Address, ☐ Authentication via Name and Password.
  - Name: (Range: 1~63 characters).
  - Password: (Range: 4~63 characters).
- DISCOVERY SETTINGS**
  - Bonjour: ☒ Enable.
  - LLDP: ☒ Enable.
  - LLDP-MED: ☒ Enable.
- IGMP/MLD SNOOPING**
  - IGMP Snooping: ☒ Enable.
  - MLD Snooping: ☒ Enable.

At the bottom right, there are 'Save' and 'Cancel' buttons.

### Port Settings

<b>Auto Negotiation</b>	If enabled, Port Speed and Duplex Mode will become grey and cannot be configured. If disabled, Port Speed and Duplex Mode can be configured.
<b>Operational Auto Negotiation</b>	Current Auto Negotiation mode of the ethernet port.
<b>Port Speed</b>	Select the speed of the ethernet port. Available only when Auto Negotiation is disabled. The option can be 10M, 100M or 1000M (default).
<b>Operational Port Speed</b>	Displays the current port speed of the ethernet port.

<b>Duplex Mode</b>	Select the duplex mode of the ethernet port. Available only when Auto Negotiation is disabled. The option can be Half or Full (default).
<b>Operational Duplex Mode</b>	Displays the current duplex mode of the ethernet port.
<b>Flow Control</b>	Enable or disable flow control of the ethernet port.
<b>802.1x Supplicant</b>	
<b>802.1x Supplicant</b>	Enable if your network requires this access point to use 802.1X authentication in order to operate.
<b>Authentication</b>	<p>This feature supports following two kinds of authentication:</p> <ul style="list-style-type: none"> <li>• <b>Authentication via MAC Address</b> Select this if you want to use MAC Address for authentication. The access point uses lowercase MAC address for Name and Password, like xxxxxxxxxxxx.</li> <li>• <b>Authentication via Name and Password</b> Select this if you want to use name and password for authentication.  Name - Enter the login name. The name includes 1 to 63 characters. Special characters are allowed.  Password - Enter the desired login password. The password includes 4 to 63 characters. Special characters are allowed.</li> </ul>
<b>Discovery Settings</b>	
<b>Bonjour</b>	Enable if administrator wants the access point to be discovered by Bonjour enabled devices automatically. If VLAN is enabled, the discovery packets will be sent out via management VLAN only. The access point supports http and https services.
<b>LLDP</b>	Enable if administrator wants the access point to be discovered by switch by LLDP protocol. Information such as product name, device name, firmware version, IP address, MAC address and so on will be advertised.
<b>LLDP-MED</b>	Enable if administrator wants the access point to be discovered by switch by LLDP-MED protocol. Information such as product name, device name, firmware version, IP address, MAC address and so on will be advertised.

<b>IGMP/MLD Snooping</b>	
<b>IGMP Snooping</b>	<p>IGMP (Internet Group Management Protocol) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast.</p> <p>IGMP snooping streamlines multicast traffic handling by examining (snooping) IGMP membership report messages from interested hosts, multicast traffic is limited to the subset of ports on which the hosts reside.</p> <p>IGMP snooping is enabled by default in the access point</p> <p>The access point supports IGMPv1, IGMPv2 and IGMPv3 in IGMP Snooping.</p>
<b>MLD Snooping</b>	<p>MLD (Multicast Listener Discovery) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.</p> <p>Multicast Listener Discovery (MLD) Snooping provides multicast containment by forwarding traffic only to those clients that have MLD receivers for a specific multicast group (destination address). The access point maintains the MLD group membership information by processing MLD reports and generating messages so traffic can be forwarded to ports receiving MLD reports.</p> <p>MLD snooping is enabled by default in the access point</p> <p>The access point supports MLDv1 and MLDv2 in MLD Snooping.</p>

# Wireless

## Basic Settings

Go to *Configuration > Wireless > Basic Settings* to configure your wireless radio and SSIDs. Advanced wireless settings such as Band Steering, Channel Bandwidth, are on the *Advanced Settings* screen.

LINKSYS

LAPAC1750C AC1750 Dual Band Access Point

Help Log out

Enable Cloud Manager

System Status

Quick Start

Configuration

Maintenance

Support

Administration

LAN

Wireless

Basic Settings

Security

Rogue AP Detection

Scheduler

Scheduler Association

Connection Control

Rate Limit

QoS

WDS

Workgroup Bridge

Advanced Settings

Captive Portal

Cluster

Basic Wireless Settings

Select Your Radio

Wireless Radio: Radio 1

Radio Settings

Enable Radio: ☒ Enable

Network Mode: B/G/N-Mixed

Wireless Channel: Auto

SSID Settings

SSID	SSID Name	Enable	Broadcast	Isolation	VLAN	Max Clients
SSID 1	LinksysSMB24G	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 2		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 3		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 4		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 5		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 6		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 7		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0
SSID 8		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	0

Save Cancel

### Basic Wireless Settings

Wireless Radio	Select the wireless radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.
Enable Radio	Enable or disable the wireless radio.

<b>Wireless Mode</b>	<p>Select the desired option for radio 1:</p> <p>G only - allow connection by 802.11G wireless stations only.</p> <p>N only - allow connection by 802.11N wireless stations only.</p> <p>B/G-Mixed - allow connection by 802.11B and G wireless stations only.</p> <p>B/G/N-Mixed (Default) - allow connections by 802.11N, 802.11B and 802.11G wireless stations.</p> <p>Select the desired option for radio 2:</p> <p>N/A-Mixed - allow connection by 802.11A and N wireless stations only.</p> <p>N only - allow connection by 802.11N wireless stations only.</p> <p>AC only - allow connection by 802.11AC wireless stations only.</p> <p>A/N/AC-Mixed - allow connection by 802.11A, 802.11N and 802.11AC wireless stations.</p>
<b>Wireless Channel</b>	<p>Select wireless channel of the radio.</p> <p>If Auto is selected, the access point will select the best available channel when device boots up.</p> <p>If you experience lost connections and/or slow data transfers, experiment with manually setting different channels to see which is the best.</p>
<b>SSID Settings</b>	
<b>SSID Name</b>	Enter the desired SSID Name. Each SSID must have a unique name. The name includes 1 to 32 characters
<b>Broadcast</b>	<p>Enable or disable the broadcast of the SSID.</p> <p>When the access point does not broadcast its SSID, the network name is not shown in the list of available networks on a client station. Instead, you must enter the exact network name manually into the wireless connection utility on the client so that it can connect.</p>
<b>Isolation</b>	<p>Enable or disable isolation among clients of the SSID. If enabled, wireless clients cannot communicate with others in the same SSID.</p> <p>It's disabled by default.</p>



<b>VLAN ID</b>	<p>Enter the VLAN ID of the SSID.</p> <p>Used to tag packets which are received from the wireless clients of the SSID and sent from Ethernet or WDS interfaces.</p> <p>Applicable only when VLAN function is enabled. VLAN function can be configured in Configuration -&gt; LAN -&gt; Network Setup screen.</p>
<b>Max Clients</b>	<p>Enter the number of clients that can connect to the SSID. The range is from 0 to 32 and 0 means no limit.</p>

## Security

Go to *Configuration > Wireless > Security* to configure security settings of SSIDs to provide data protection over the wireless network.

Security	
<b>Select SSID</b>	Select the desired SSID from the drop-down list.
<b>Security Mode</b>	Select the desired security method from the list.

### Security Mode

- Disabled - No security. Anyone using the correct SSID can connect to your network.
- WEP - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.

- WPA2-Personal - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method.
- WPA/WPA2-Personal - This method, sometimes called Mixed Mode, allows clients to use either WPA-Personal (with TKIP) or WPA2-Personal (with AES).
- WPA2-Enterprise - Requires a RADIUS Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.

If this option is selected:

- This access point must have a client login on the RADIUS Server.
- Each user must authenticate on the RADIUS Server. This is usually done using digital certificates.
- Each user's wireless client must support 802.1x and provide the RADIUS authentication data when required.
- All data transmission is encrypted using the WPA2 AES standard. Keys are automatically generated, so no key input is required.
- WPA/WPA2-Enterprise - This method, sometimes called Mixed Mode, allows clients to use either WPA-Enterprise (with TKIP) or WPA2-Enterprise (with AES).
- RADIUS - RADIUS mode utilizes RADIUS server for authentication and dynamic WEP key generation for data encryption.

## WEP

This is the 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.

LINKSYS  
LAPAC1750G AC1750 Dual Band Access Point

Help Log out  
Enable Cloud Manager

System Status Quick Start Configuration Maintenance Support

Administration  
LAN  
Wireless  
Basic Settings  
Security  
Rogue AP Detection  
Scheduler  
Scheduler Association  
Connection Control  
Rate Limit  
QoS  
WDS  
Workgroup Bridge  
Advanced Settings  
Captive Portal  
Cluster

Wireless Security

Select Your SSID  
SSID: Radio 1:SSID 1 (LinksysSMB24G)

Security Settings  
Security Mode: WEP  
Authentication Type: Open System  
Default Transmit Key: 1 2 3 4  
WEP Encryption: 64-bit (10 hex digits)  
Passphrase: (Range: 1~30 characters) Generate  
Key 1: (10 HEX characters)  
Key 2: (10 HEX characters)  
Key 3: (10 HEX characters)  
Key 4: (10 HEX characters)  
Save Cancel

### WEP

<b>Authentication</b>	Select Open System or Shared Key. All wireless stations must use the same method.
<b>Default Transmit Key</b>	Select a transmit key.
<b>WEP Encryption</b>	Select an encryption option, and ensure your wireless stations have the same setting: 64-Bit Encryption - Keys are 10 Hex characters. 128-Bit Encryption - Keys are 26 Hex characters.
<b>Passphrase</b>	Generate a key or keys, instead of entering them directly. Enter a word or group of printable characters in the Passphrase box and click the Generate button. It consists of 1 to 30 characters.
<b>Key Value</b>	Enter a key in hexadecimal format. <i>Note--Due to hardware limitation, one set of WEP key is supported per radio.</i>

## WPA2-Personal

This is a further development of WPA-Personal and offers even greater security.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The 'Configuration' tab is selected, and the 'Wireless Security' page is displayed. The left sidebar shows a navigation menu with 'Wireless' expanded. The main content area has the following settings:

- Select Your SSID:** Radio 1:SSID 1 (LinksysSMB24G)
- Security Settings:**
  - Security Mode:** WPA2-Personal
  - WPA Algorithm:** AES
  - Pre-shared Key:** (Empty field, with a note: (Range: 8-63 ASCII or 64 HEX characters))
  - Key Renewal:** 3600 seconds (Range: 600-36000, Default: 3600)

At the bottom right of the settings area are 'Save' and 'Cancel' buttons.

WPA2-Personal	
WPA Algorithm	The encryption method is AES. Wireless stations must also use AES.
Pre-shared Key	Enter the key value. It is 8 to 63 ASCII characters or 64 HEX characters. Other wireless stations must use the same key.
Key Renewal	<p>Specify the value of Group Key Renewal. It's a value from 600 to 36000 and default is 3600.</p> <p>WPA automatically changes secret keys after a certain period of time. The group key interval is the period of time in between automatic changes of the group key, which all devices on the network share.</p> <p>Constantly keying the group key protects your network against intrusion, as the would-be intruder must cope with an ever-changing secret key.</p>

## WPA/WPA2-Personal

This method, sometimes called Mixed Mode, allows clients to use either WPA-Personal or WPA2-Personal.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The 'Configuration' tab is selected, and the 'Wireless' section is expanded. The 'Wireless Security' page is displayed, showing the following settings:

- Select Your SSID:** Radio 1:SSID 1 (LinksysSMB24G)
- Security Settings:**
  - Security Mode:** WPA/WPA2-Personal
  - WPA Algorithm:** TKIP or AES
  - Pre-shared Key:** (Range: 8-63 ASCII or 64 HEX characters)
  - Key Renewal:** 3600 seconds (Range: 600-36000, Default: 3600)

Buttons for 'Save' and 'Cancel' are located at the bottom right of the configuration area.

### WPA/WPA2-Personal

<b>WPA Algorithm</b>	The encryption method is TKIP or AES.
<b>Pre-shared Key</b>	Enter the key value. It is 8 to 63 ASCII characters or 64 HEX characters. Other wireless stations must use the same key.
<b>Key Renewal</b>	<p>Specify the value of Group Key Renewal. It's a value from 600 to 36000, and default is 3600.</p> <p>WPA automatically changes secret keys after a certain period of time. The group key interval is the period of time in between automatic changes of the group key, which all devices on the network share.</p> <p>Constantly keying the group key protects your network against intrusion, as the would-be intruder must cope with an ever-changing secret key.</p>

## WPA2-Enterprise

This version of WPA2-Enterprise requires a RADIUS Server on your LAN to provide the client authentication. Data transmissions are encrypted using the WPA2 AES standard.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The 'Configuration' tab is active, and the 'Wireless Security' section is selected in the left sidebar. The 'Security Settings' for 'Radio 1:SSID 1 (LinksysSMB24G)' are displayed. The 'Security Mode' is set to 'WPA2-Enterprise'. The 'Primary Server' is set to '0.0.0.0' and the 'Primary Server Port' is '1812'. The 'Primary Shared Secret' is masked with dots. The 'Backup Server' is also set to '0.0.0.0' and the 'Backup Server Port' is '1812'. The 'Backup Shared Secret' is also masked. The 'WPA Algorithm' is set to 'AES' and the 'Key Renewal Timeout' is '3600' seconds. 'Save' and 'Cancel' buttons are at the bottom right.

Wireless Security	
Select Your SSID	
SSID:	Radio 1:SSID 1 (LinksysSMB24G)
Security Settings	
Security Mode:	WPA2-Enterprise
Primary Server:	0 . 0 . 0 . 0
Primary Server Port:	1812 (Range: 1~65534, Default: 1812)
Primary Shared Secret:	***** (Range: 1~64 characters)
Backup Server:	0 . 0 . 0 . 0
Backup Server Port:	1812 (Range: 1~65534, Default: 1812)
Backup Shared Secret:	***** (Range: 1~64 characters)
WPA Algorithm:	AES
Key Renewal Timeout:	3600 seconds (Range: 600~36000, Default: 3600)
<div>Save Cancel</div>	

### WPA2-Enterprise

Primary Server	Enter the IP address of the RADIUS Server on your network.
Primary Server Port	Enter the port number used for connections to the RADIUS Server. It is a value from 1 to 65534, and default is 1812.
Primary Shared Secret	Enter the key value to match the RADIUS Server. It consists of 1 to 64 characters.
Backup Server	The Backup Authentication Server will be used when the Primary Authentication Server is not available.
Backup Server Port	Enter the port number used for connections to the Backup RADIUS Server. It's a value from 1 to 65534, and default is 1812.

<b>Backup Shared Secret</b>	Enter the key value to match the Backup RADIUS Server. It consists of 1 to 64 characters.
<b>WPA Algorithm</b>	The encryption method is AES.
<b>Key Renewal Timeout</b>	<p>Specify the value of Group Key Renewal. It is a value from 600 to 36000, and default is 3600.</p> <p>WPA automatically changes secret keys after a certain period of time. The group key interval is the period of time in between automatic changes of the group key, which all devices on the network share.</p> <p>Constantly keying the group key protects your network against intrusion, as the would-be intruder must cope with an ever-changing secret key.</p>

## WPA/WPA2-Enterprise

WPA/WPA2-Enterprise requires a RADIUS Server on your LAN to provide the client authentication. Data transmissions are encrypted using WPA/WPA2 standard.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The 'Configuration' tab is active, and the 'Wireless Security' section is selected in the left sidebar. The 'Security Settings' for 'Radio 1:SSID 1 (LinksysSMB24G)' are displayed. The 'Security Mode' is set to 'WPA/WPA2-Enterprise'. The 'Primary Server' is set to '0.0.0.0' and the 'Primary Server Port' is '1812'. The 'Primary Shared Secret' is masked with dots. The 'Backup Server' is also set to '0.0.0.0' and the 'Backup Server Port' is '1812'. The 'Backup Shared Secret' is also masked. The 'WPA Algorithm' is set to 'TKIP or AES' and the 'Key Renewal Timeout' is '3600' seconds. 'Save' and 'Cancel' buttons are at the bottom right.

Wireless Security	
Select Your SSID	
SSID:	Radio 1:SSID 1 (LinksysSMB24G)
Security Settings	
Security Mode:	WPA/WPA2-Enterprise
Primary Server:	0 . 0 . 0 . 0
Primary Server Port:	1812 (Range: 1~65534, Default: 1812)
Primary Shared Secret:	..... (Range: 1~64 characters)
Backup Server:	0 . 0 . 0 . 0
Backup Server Port:	1812 (Range: 1~65534, Default: 1812)
Backup Shared Secret:	..... (Range: 1~64 characters)
WPA Algorithm:	TKIP or AES
Key Renewal Timeout:	3600 seconds (Range: 600~36000, Default: 3600)
<div>Save Cancel</div>	

### WPA/WPA2-Enterprise

Primary Server	Enter the IP address of the RADIUS Server on your network.
Primary Server Port	Enter the port number used for connections to the RADIUS Server. It is a value from 1 to 65534, and default is 1812.
Primary Shared Secret	Enter the key value to match the RADIUS Server. It consists of 1 to 64 characters.
Backup Server	The Backup Authentication Server will be used when the Primary Authentication Server is not available.
Backup Server Port	Enter the port number used for connections to the Backup RADIUS Server. It is a value from 1 to 65534, and default is 1812.



<b>Backup Shared Secret</b>	Enter the key value to match the Backup RADIUS Server. It consists of 1 to 64 characters.
<b>WPA Algorithm</b>	The encryption method is TKIP or AES.
<b>Key Renewal Timeout</b>	<p>Specify the value of Group Key Renewal. It is a value from 600 to 36000, and default is 3600 second.</p> <p>WPA automatically changes secret keys after a certain period of time. The group key interval is the period of time between automatic changes of the group key, which all devices on the network share.</p> <p>Constantly keying the group key protects your network against intrusion, as the would-be intruder must cope with an ever-changing secret key.</p>

## RADIUS

Use RADIUS server for authentication and dynamic WEP key generation for data encryption.

The screenshot shows the Linksys configuration web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. On the left, a sidebar menu lists 'Administration', 'LAN', 'Wireless' (selected), 'Basic Settings', 'Security', 'Rogue AP Detection', 'Scheduler', 'Scheduler Association', 'Connection Control', 'Rate Limit', 'QoS', 'WDS', 'Workgroup Bridge', and 'Advanced Settings'. The main content area is titled 'Wireless Security' and contains the following fields:

- Select Your SSID:** A dropdown menu showing 'Radio 1:SSID 1 (LinksysSMB24G)'.
- Security Settings:**
  - Security Mode:** A dropdown menu showing 'RADIUS'.
  - Primary Server:** IP address input fields (0, 0, 0, 0).
  - Primary Server Port:** 1812 (Range: 1~65534, Default: 1812).
  - Primary Shared Secret:** A text field with masked characters (Range: 1~64 characters).
  - Backup Server:** IP address input fields (0, 0, 0, 0).
  - Backup Server Port:** 1812 (Range: 1~65534, Default: 1812).
  - Backup Shared Secret:** A text field with masked characters (Range: 1~64 characters).

At the bottom right of the configuration area are 'Save' and 'Cancel' buttons.

### Authentication Server

<b>Primary Server</b>	Enter the IP address of the RADIUS Server on your network.
<b>Primary Server Port</b>	Enter the port number used for connections to the RADIUS Server. It is a value from 1 to 65534, and default is 1812.
<b>Primary Shared Secret</b>	Enter the key value to match the RADIUS Server. It consists of 1 to 64 characters.
<b>Backup Server</b>	The Backup Authentication Server will be used when the Primary Authentication Server is not available.
<b>Backup Server Port</b>	Enter the port number used for connections to the Backup RADIUS Server. It is a value from 1 to 65534, and default is 1812.
<b>Backup Shared Secret</b>	Enter the key value to match the Backup RADIUS Server. It consists of 1 to 64 characters.

# Rogue AP Detection

Go to *Configuration > Wireless > Rogue AP Detection* to detect an unexpected or unauthorized access point installed in a secure network environment.

LINKSYS

LAPAC1750C AC1750 Dual Band Access Point

HelpLog out

Enable Cloud Manager

System StatusQuick StartConfigurationMaintenanceSupport

Administration

LAN

Wireless

Basic Settings

Security

Rogue AP Detection

Scheduler

Scheduler Association

Connection Control

Rate Limit

QoS

WDS

Workgroup Bridge

Advanced Settings

Captive Portal

Cluster

Rogue AP Detection

Select Your Radio

Wireless Radio:Radio 1

Rogue AP Detection

Rogue AP Detection:☐ Enable

Detected Rogue AP List

Action	MAC Address	SSID	Channel	Security	Signal (dBm)
Trusted AP List					
Action	MAC Address	SSID	Channel	Security	Signal (dBm)
New MAC Address: <input type="text"/> <input type="button" value="Add"/>					
<input type="button" value="Save"/> <input type="button" value="Refresh"/>					

Radio	
Wireless Radio	Select the desired radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.
Rogue AP	Enable or disable Rogue AP Detection on the selected radio.
Detected Rogue AP List	
Action	Click Trust to move the AP to the Trusted AP List.
MAC Address	The MAC address of the Rogue AP.
SSID	The SSID of the Rogue AP.
Channel	The channel of the Rogue AP.
Security	The security method of the Rogue AP.
Signal	The signal level of the Rogue AP.

Trusted AP List	
<b>Action</b>	Click Untrust to move the AP to the Rogue AP List.
<b>MAC Address</b>	The MAC address of the Trusted AP.
<b>SSID</b>	The SSID of the Trusted AP.
<b>Channel</b>	The channel of the Trusted AP.
<b>Security</b>	The security method of the Trusted AP.
<b>Signal</b>	The signal level of the Trusted AP.
<b>New MAC Address</b>	Add one trusted AP by MAC address.

## Scheduler

Go to *Configuration > Wireless > Scheduler* to configure a rule with a specific time interval for SSIDs to be operational. Automate enabling or disabling SSIDs based on the profile definition. Support up to 16 profiles and each profile can include four time rules.

### Scheduler

#### Wireless Scheduler

Enable or disable wireless scheduler on the radio. It is disabled by default.

If disabled, even if some SSIDs are associated with profiles, they will be always active.

Scheduler Operational Status	
<b>Status</b>	The operational status of the scheduler.
<b>Reason</b>	<p>The detailed reason for the scheduler operational status. It includes the following situations.</p> <ul style="list-style-type: none"> <li>• System time is outdated. Scheduler is inactive because system time is outdated.</li> <li>• Administrative Mode is disabled. Scheduler is disabled by administrator.</li> <li>• Active Scheduler is active.</li> </ul>
Scheduler Profile configuration	
<b>New Profile Name</b>	Enter the name for new profile.
<b>Profile Name</b>	Select the desired profile from the list to configure.
<b>Day of the Week</b>	<p>Select the desired day from the list.</p> <p>Option "None" means this time rule is disabled.</p>
<b>Start Time</b>	Choose the start time.
<b>Finish Time</b>	Choose the finish time.

## Scheduler Association

Go to *Configuration > Wireless > Scheduler Association* to associate defined scheduler profiles with SSIDs.

### Radio

#### Wireless Radio

Select the desired radio from the list.  
Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.

### Scheduler Association

#### SSID

The index of SSID.

#### SSID Name

The name of the SSID.

#### Profile Name

Choose the profile that is associated with the SSID.  
If the profile associated with the SSID is deleted, then the association will be removed.  
Option "None" means no scheduler profile is associated.

#### Interface Status

The status of the SSID. It can be Enabled or Disabled.  
Scheduler only works when the SSID is enabled.

## Connection Control

Go to *Configuration > Wireless > Connection Control* to define whether listed client stations may authenticate with the access point.

The screenshot displays the Linksys web management interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar is blue with the Linksys logo, a 'Help' icon, a 'Log out' icon, and an 'Enable Cloud Manager' button. Below this is a dark grey navigation bar with tabs for 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. On the left, a sidebar menu shows categories: 'Administration' (with sub-items 'LAN' and 'Wireless'), 'Basic Settings' (with sub-items 'Security', 'Rogue AP Detection', 'Scheduler', and 'Scheduler Association'), 'Connection Control' (selected), 'Rate Limit', 'QoS', 'WDS', 'Workgroup Bridge', 'Advanced Settings', 'Captive Portal', and 'Cluster'. The main content area is titled 'Wireless Connection Control'. It features a 'Select Your SSID' section with a dropdown menu showing 'Radio 1: SSID 1 (LinksysSMB24G)'. Below this is a 'Control Type' section with three radio buttons: 'Local', 'RADIUS', and 'Disabled' (which is selected). At the bottom right of the configuration area are 'Save' and 'Cancel' buttons.



<b>SSID</b>	Select the desired SSID from the list.
<b>Control Type</b>	<p>Select the option from the drop-down list as desired.</p> <ul style="list-style-type: none"> <li>Local: Choose either "Allow only following MAC addresses to connect to wireless network" or "Prevent following MAC addresses from connection to wireless network." You can enter up to 20 MAC addresses of wireless stations or choose the MAC address.</li> <li>RADIUS <ul style="list-style-type: none"> <li>Primary/Backup RADIUS Server - Enter the IP address of the RADIUS Server.</li> <li>Primary/Backup RADIUS Server Port - Enter the Port number of the RADIUS Server.</li> <li>Primary/Backup Shared Secret - This is shared between the wireless access point and the RADIUS Server while authenticating the device attempting to connect.</li> </ul> </li> <li>Disabled</li> </ul>

## Rate Limit

Go to *Configuration > Wireless > Rate Limit* to limit downstream and upstream rate of SSIDs.

Radio	
<b>Wireless Radio</b>	Select the desired radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.
Rate Limit	
<b>SSID</b>	The index of SSID.
<b>SSID Name</b>	The name of the SSID.
<b>Upstream Rate</b>	Enter a maximum upstream rate for the SSID. The range is from 0 to 200 Mbps for Radio 1 and from 0 to 600 Mbps for Radio 2; 0 means no limitation.
<b>Downstream Rate</b>	Enter a maximum downstream rate for the SSID. The range is from 0 to 200 Mbps for Radio 1 and from 0 to 600 Mbps for Radio 2; 0 means no limitation.

## QoS

Go to *Configuration > Wireless > QoS (Quality of Service)* to specify priorities for different traffic coming from your wireless client. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic.

**LINKSYS** LAPAC1750C AC1750 Dual Band Access Point

System Status Quick Start **Configuration** Maintenance Support

Administration  
LAN  
**Wireless**  
Basic Settings  
Security  
Rogue AP Detection  
Scheduler  
Scheduler Association  
Connection Control  
Rate Limit  
QoS  
WDS  
Workgroup Bridge  
Advanced Settings  
Captive Portal  
Cluster

QoS

Select Your Radio  
Wireless Radio: Radio 1

QoS Settings

SSID	SSID Name	VLAN ID	Priority	WMM
SSID 1	LinksysSMB24G	1	0	<input checked="" type="checkbox"/>
SSID 2		1	0	<input checked="" type="checkbox"/>
SSID 3		1	0	<input checked="" type="checkbox"/>
SSID 4		1	0	<input checked="" type="checkbox"/>
SSID 5		1	0	<input checked="" type="checkbox"/>
SSID 6		1	0	<input checked="" type="checkbox"/>
SSID 7		1	0	<input checked="" type="checkbox"/>
SSID 8		1	0	<input checked="" type="checkbox"/>

Save Cancel

### QoS Setting

<b>Wireless Radio</b>	Select the desired radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.
-----------------------	--

### QoS Settings

<b>SSID</b>	The index of SSID.
<b>SSID Name</b>	The name of the SSID.
<b>VLAN ID</b>	The VLAN ID of the SSID.

<b>Priority</b>	<p>Select the priority level from the list. VLAN must be enabled in order to set priority.</p> <p>The 802.1p will be included in the VLAN header of the packets which are received from the SSID and sent from Ethernet or WDS interface.</p>
<b>WMM</b>	<p>Enable or disable WMM.</p> <p>WMM (Wi-Fi Multimedia) is a component of the IEEE 802.11e wireless LAN standard for QoS.</p> <p>WMM provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled.</p> <p>Legacy applications that do not support WMM and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.</p> <p>WMM is enabled by default.</p>

## WDS

Go to *Configuration > Wireless > WDS (Wireless Distribution System)* to expand a wireless network through multiple access points instead of linking them with a wired backbone.

The access point can act as WDS Root or WDS Station:

- WDS Root - Receives WDS connections from remote WDS Stations.
- WDS Station - Connects to remote WDS Root. Supports up to 4 WDS Stations on each wireless radio.

**LINKSYS**  
LAPAC1750C AC1750 Dual Band Access Point

System Status Quick Start **Configuration** Maintenance Support

Administration  
LAN  
**Wireless**  
Basic Settings  
Security  
Rogue AP Detection  
Scheduler  
Scheduler Association  
Connection Control  
Rate Limit  
QoS  
WDS  
Workgroup Bridge  
Advanced Settings  
Captive Portal  
Cluster

**WDS**

SPANNING TREE

Spanning Tree Mode: ☐ Enable

SELECT YOUR RADIO

Radio: Radio 1

**WDS ROOT**

WDS Root AP Interface

Interface Status: ☐ Enable

Local SSID: LinksysSMB24G-WDSRoot

Local MAC Address: 7A:EF:68:83:54:D5

Local Channel: 11

Allowed VLAN List: 1 (Format: xxx,xxx,xxx, Default: 1)

Security Mode: Disabled

**WDS STATION**

**WDS Interface 1**

Interface Status: ☐ Enable

Local MAC Address: 8A:EF:68:83:54:D5

Remote SSID: Site Survey

Remote MAC Address: 00:00:00:00:00:00 (xxxxxx,xxx,xxx) (Optional)

VLAN List: 1 (Format: xxx,xxx,xxx, Default: 1)

Security Mode: Disabled

Status: Not Connected

**WDS Interface 2**

Interface Status: ☐ Enable

Local MAC Address: 9A:EF:68:83:54:D5

Remote SSID: Site Survey

Remote MAC Address: 00:00:00:00:00:00 (xxxxxx,xxx,xxx) (Optional)

VLAN List: 1 (Format: xxx,xxx,xxx, Default: 1)

Security Mode: Disabled

Status: Not Connected

**WDS Interface 3**

Interface Status: ☐ Enable

Local MAC Address: AA:EF:68:83:54:D5

Remote SSID: Site Survey

Remote MAC Address: 00:00:00:00:00:00 (xxxxxx,xxx,xxx) (Optional)

VLAN List: 1 (Format: xxx,xxx,xxx, Default: 1)

Security Mode: Disabled

Status: Not Connected

**WDS Interface 4**

Interface Status: ☐ Enable

Local MAC Address: 8A:EF:68:83:54:D5

Remote SSID: Site Survey

Remote MAC Address: 00:00:00:00:00:00 (xxxxxx,xxx,xxx) (Optional)

VLAN List: 1 (Format: xxx,xxx,xxx, Default: 1)

Security Mode: Disabled

Status: Not Connected

Save Cancel

Spanning Tree (recommended if you configure WDS connections)	
Spanning Tree	When enabled, STP helps prevent switching loops.
WDS Settings	
Radio	Select the desired radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.
WDS Root	
Interface Status	<p>Enable or Disable the WDS Root.</p> <p>Be sure the following settings on WDS Root device are determined and configured. The WDS Station must use the same settings as Root afterwards.</p> <ul style="list-style-type: none"> <li>• Radio</li> <li>• IEEE 802.11 Mode</li> <li>• Channel Bandwidth</li> <li>• Channel</li> </ul> <p><i>Note-It is highly recommended that static channel is configured on both APs. Do not use Auto channel option when you enable WDS, as both APs in a WDS link must be on the same radio channel. If Auto option is configured, there is chance two access points run on different channels and WDS link cannot establish.</i></p> <p>Workgroup Bridge and WDS will not work at the same time on one wireless radio. When Workgroup Bridge is enabled, WDS will be disabled automatically on the same radio.</p>
Local SSID	Enter name of the WDS Root SSID (used when connected by WDS Stations).
Local MAC Address	MAC address of the WDS Root SSID.
Local Channel	<p>The channel used by WDS Root SSID. WDS stations must use same channel as the WDS Root.</p> <p>Channel can be changed in "Basic Settings" page.</p>

<b>Allowed VLAN List</b>	<p>Enter the list of VLANs accepted by the WDS Root.</p> <p>When VLAN is enabled, WDS Root receives from WDS Stations only packets in the VLAN list. Packets not in the list will be dropped.</p> <p>The VLAN list is only applicable when VLAN is enabled.</p> <p>The VLAN list includes 1 to 16 VLAN IDs separated by "," such as "100,200,300,400,500,600,700,800".</p>
<b>Security Settings</b>	<p>Setting can be Disabled, WPA-Personal, WPA2-Personal, WPA2-Enterprise or WPA/WPA2-Enterprise.</p>
<b>WDS Station</b>	
<b>Interface Status</b>	<p>Enable or disable the WDS Station.</p> <p>Before configuring a WDS Station, be sure the following settings of the device are identical to the WDS Root that will be connected.</p> <ul style="list-style-type: none"> <li>• Radio</li> <li>• IEEE 802.11 Mode</li> <li>• Channel Bandwidth</li> <li>• Channel</li> </ul> <p><i>Note-It is highly recommended that static channel is configured on both APs. Do not use Auto channel option when you enable WDS, as both APs in a WDS link must be on the same radio channel. If Auto option is configured, there is chance two access points run on different channels and WDS link cannot establish.</i></p> <p>Workgroup Bridge and WDS will not work at the same time on one wireless radio. When Workgroup Bridge is enabled, WDS will be disabled automatically on the same radio.</p>
<b>Remote SSID</b>	<p>Enter the name of the Root's SSID. Click Site Survey button and choose from the list. You must do this for WDS Station to connect to a remote WDS Root.</p>

<b>Remote MAC Address</b>	<p>MAC address of the access point on the other end of the WDS link. Optional</p> <p>WDS Station connects to remote WDS Root by matching SSIDs. When there is more than one remote WDS Root with the same SSID, the WDS Station can differentiate them by MAC address.</p> <p>The format is xx:xx:xx:xx:xx:xx.</p>
<b>VLAN List</b>	<p>Enter the list of VLANs that are accepted by the WDS Station.</p> <p>When VLAN is enabled, the WDS Station forwards to the remote WDS Root only packets in the VLAN list. Packets not in the VLAN list cannot be forwarded to the remote WDS Root.</p> <p>The VLAN List is only applicable when VLAN is enabled.</p> <p>The VLAN list includes 1 to 8 VLAN IDs separated by "," such as "100,200,300,400,500,600,700,800".</p>
<b>Security Mode</b>	<p>The type of encryption to use on the WDS link. It must be unique to the access point on the other end of the WDS link.</p> <p>The options are Disabled, WPA Personal, WPA2 Personal, WPA Enterprise or WPA2 Enterprise.</p>
<b>Status</b>	<p>Status of the WDS interface. It can be Disabled, Connected or Not Connected.</p>



## Workgroup Bridge

Go to *Configuration > Wireless > Workgroup Bridge* to extend the accessibility of a remote network. In Workgroup Bridge mode, the access point acts as a wireless station (STA) on the wireless LAN. It can bridge traffic between a remote wired network and a wireless LAN.

When Workgroup Bridge is enabled, SSID configuration still works to provide wireless services to clients.

All access points participating in Workgroup Bridge must have the identical settings for Radio interface, IEEE 802.11 mode, Channel Bandwidth, Channel (Auto is not recommended).

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. The left sidebar lists various configuration categories: Administration, LAN, Wireless (selected), Basic Settings, Security, Rogue AP Detection, Scheduler, Scheduler Association, Connection Control, Rate Limit, QoS, WDS, Workgroup Bridge (highlighted), Advanced Settings, Captive Portal, and Cluster. The main content area is titled 'Workgroup Bridge' and contains the following settings:

- Select Your Radio:** Radio: Radio 1 (dropdown), Status: ☐ Enable
- Remote AP Settings:** SSID: [text input] Site Survey (button), Remote MAC Address: 00:00:00:00:00:00 (xxxx:xxxx:xx) (Optional), Security Mode: Disabled (dropdown), Connection Status: Not Connected

At the bottom right of the settings area are 'Save' and 'Cancel' buttons.

Workgroup Bridge	
Radio	<p>Select the desired radio from the list.</p> <p>Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.</p>
Workgroup Bridge Status	
Status	<p>Enable or disable Workgroup Bridge function.</p> <p>Before configuring Workgroup Bridge, make sure all devices in Workgroup Bridge have the following identical settings.</p> <ul style="list-style-type: none"> <li>• Radio</li> <li>• IEEE 802.11 Mode</li> <li>• Channel Bandwidth</li> <li>• Channel</li> </ul> <p><i>Note-It is highly recommended that static channel is configured on both APs. Do not use Auto channel option when you enable Workgroup Bridge, as both APs in a Workgroup Bridge link must be on the same radio channel. If Auto option is configured, there is chance two access points run on different channels and Worgroup Bridge link cannot establish.</i></p>
Remote AP Settings	
SSID	<p>Enter the name of the SSID to which Workgroup Bridge will connect. Click Site Survey button to choose from the list. You must do this for Workgroup Bridge to connect to a remote access point.</p>
Remote MAC Address	<p>Normally, Workgroup Bridge connects to a remote access point by matching SSID. When more than one remote access point has the same SSID, Workgroup Bridge can connect to different remote access points.</p> <p>Optional: You can specify the MAC address of the remote access point to limit Workgroup Bridge's connection to a specific remote access point.</p> <p>The format is xx:xx:xx:xx:xx:xx.</p>

<b>Security Mode</b>	<p>Select the desired mode from the list.</p> <ul style="list-style-type: none"><li>• Disabled</li><li>• WPA-Personal</li><li>• WPA2-Personal</li><li>• WPA-Enterprise</li><li>• WPA2-Enterprise</li></ul>
----------------------	--

## Advanced Settings

Go to *Configuration > Wireless > Workgroup Bridge* to configure advanced parameters of wireless radios.

### Band Steering

#### Band Steering

Enable or disable Band Steering function.

Band Steering is a technology that detects whether the wireless client is dual-band capable. If it is, band steering pushes the client to connect to the less-congested 5 GHz network. It does this by actively blocking the client's attempts to connect with the 2.4GHz network.

### Isolation

#### Isolation between SSIDs

Define whether to isolate traffic between SSIDs. If enabled, wireless clients in different SSIDs cannot communicate with each other. Enabled by default.

### Advanced Parameters

<b>Wireless Radio</b>	Select the desired radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.
<b>Worldwide Mode (802.11d)</b>	Worldwide Mode (802.11d) enables the access point to direct connected wireless devices to radio settings specific to where in the world the devices are in use.
<b>Channel Bandwidth</b>	Select the designed channel bandwidth for the wireless radio. 20MHz - Select if you are not using any 802.11n wireless devices. 20/40MHz - Select if you are using both 802.11n and non-802.11n wireless devices. 20/40/80MHz - Select if you are using 802.11ac, 802.11n and non-802.11n wireless devices.
<b>Guard Interval</b>	Select the guard interval manually for Wireless-N connections. The two options are Short (400 nanoseconds) and Long (800 nanoseconds). The default is Auto.
<b>CTS Protection Mode</b>	CTS (Clear-To-Send) Protection Mode boosts the access point's ability to catch all Wireless-G transmissions, but it severely decreases performance. By default, CTS Protection Mode is disabled, but the access point will automatically enable this feature when Wireless-G devices are not able to transmit to the access point in an environment with heavy 802.11b traffic.
<b>Beacon Interval</b>	The access point transmits beacon frames at regular intervals to announce the existence of the wireless network. Enter the interval between the transmissions of beacon frames. The value range is between 40 and 1000 milliseconds and default is 100 milliseconds.

<b>DTIM Interval</b>	<p>Enter the Delivery Traffic Information Map (DTIM) period, an integer from 1 to 255 beacons. The default is 1 beacon.</p> <p>The DTIM message is an element included in some beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pickup.</p> <p>The DTIM period that you specify indicates how often the clients served by this WAP device should check for buffered data still on the access point awaiting pickup.</p> <p>For example, if you enter 1, clients check for buffered data on the access point at every beacon. If you enter 10, clients check on every 10th beacon.</p>
<b>RTS Threshold</b>	<p>Enter the Request to Send (RTS) Threshold value, an integer from 1 to 2347. The default is 2347 octets.</p> <p>The RTS threshold indicates the number of octets in a Medium Access Control Protocol Data Unit (MPDU) below which an RTS/CTS handshake is not performed.</p> <p>Changing the RTS threshold can help control traffic flow through the access point, especially one with a lot of clients. If you specify a low threshold value, RTS packets are sent more frequently, which consumes more bandwidth and reduces the throughput of the packet. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network, or on a network experiencing electromagnetic interference.</p>

<b>Fragmentation Threshold</b>	<p>Enter the fragmentation threshold, an integer from 256 to 2346. The default is 2346.</p> <p>The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold you set, the fragmentation function is activated and the packet is sent as multiple 802.11 frames.</p> <p>If the packet being transmitted is equal to or less than the threshold, fragmentation is not used. Setting the threshold to the largest value (2,346 bytes, which is the default) effectively disables fragmentation.</p> <p>Fragmentation involves more overhead because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured.</p>
<b>Output Power</b>	<p>Select the output power of the access point. If many access points exist, lower power can reduce the signal interference among them.</p>

# Captive Portal

Captive Portal is a method of securing access to the Internet from within a wireless network. Users must enter authentication credentials before their wireless client devices can access the Internet.

## Global Configuration

Go to *Configuration > Captive Portal > Global Configuration* to change settings and modify captive portal authentication access port number if needed.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance', and 'Support'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories: Administration, LAN, Wireless, and Captive Portal. Under 'Captive Portal', the 'Global Configuration' option is selected. The main content area displays the 'Global Configuration' settings for the Captive Portal. These settings include: 'Captive Portal' (a checkbox currently unchecked), 'Authentication Timeout' (a text input field set to '300' with a range of 60-600 and a default of 300), 'Additional HTTP Port' (a checkbox currently unchecked), 'HTTP Port' (a text input field set to '80' with a range of 80-1024-65535 and a default of 80), 'Additional HTTPS Port' (a checkbox currently unchecked), and 'HTTPS Port' (a text input field set to '443' with a range of 443-1024-65535 and a default of 443). At the bottom right of the settings area are 'Save' and 'Cancel' buttons.

<b>Captive Portal</b>	Enable or Disable Captive Portal function globally. Captive Portal is disabled by default.
<b>Authentication Timeout</b>	The number of seconds the access point keeps an authentication session open with a wireless client. If the client fails to enter authentication credentials within the timeout period, the client may need to refresh the web authentication page. The range is from 60 to 600 seconds. Default is 300.
<b>Additional HTTP Port</b>	HTTP portal authentication uses the HTTP management port by default. You can configure an additional port for that process.



<b>HTTP Port</b>	Once Additional HTTP Port is enabled, define an additional port for HTTP protocol. The value can be 80 or 1024 to 65535 and is 80 by default. The HTTP Port must be different from the HTTP port in <i>Administration &gt; Management Access</i> page.
<b>Additional HTTPS Port</b>	HTTPS portal authentication uses the HTTPS management port by default. You can configure an additional port for that process.
<b>HTTPS Port</b>	Once Additional HTTPS Port is enabled, define an additional port for HTTPS protocol. The value can be 443 or 1024 to 65535 and is 443 by default. The additional HTTPS Port must be different from the HTTPS port in <i>Administration &gt; Management Access</i> page.

## Portal Profiles

Go to *Configuration > Captive Portal > Portal Profiles* to define detailed settings for Captive Portal profile. Create up to two profiles.

**LINKSYS** LAPAC1750C AC1750 Dual Band Access Point

Help Log out

Enable Cloud Manager

System Status Quick Start Configuration Maintenance Support

Administration  
LAN  
Wireless  
Captive Portal  
Global Configuration  
Portal Profiles  
Local User  
Local Group  
Web Customization  
Profile Association  
Client Information  
Cluster

**Portal Profiles**

Select Your Profile

Captive Portal Profile: Profile 1

Profile Settings

Protocol: HTTP

Authentication: Local

Group Name: Default

Landing Page: ☐ Enable

Redirect to Original URL: ☐ Enable

Promotion URL: (Max 128 characters)

Session Timeout: 0 minutes (Range: 0~1440, Default: 0)

Save Cancel

Portal Profiles	
<b>Captive Portal Profile</b>	Select a profile to configure.
<b>Protocol</b>	Select the protocol used to access the Portal Authentication web server. It can be HTTP or HTTPS.
<b>Authentication</b>	<p>Select an authentication method for clients.</p> <p>Local - The access point uses a local database to authenticated wireless clients.</p> <p>Radius - The access point uses a database on a remote RADIUS server to authenticate wireless clients. The RADIUS server must support EAP-MD5.</p> <p>Password Only - Wireless clients only need a password. Username is unnecessary.</p> <p>No Password - Wireless clients accept defined terms to access the wireless network. Password and username both are unnecessary.</p>
<b>Landing Page</b>	Enable Landing Page to determine where authenticated wireless clients will be directed after logging in at Captive Portal. Choose <i>Original URL</i> or <i>Promotion URL</i> .
<b>Redirect to Original URL</b>	If Landing Page is enabled, this setting redirects authenticated wireless clients from the Captive Portal login screen to the URL the user typed in.
<b>Promotion URL</b>	Enter a URL to which authenticated clients will be redirected from the Captive Portal login page. Landing Page must be enabled and Redirect to Original URL must be disabled.
<b>Session Timeout</b>	Set the session time in minutes. The access point will disconnect authenticated clients when the session time expires. Session time can range from 0 to 1440 minutes. The default is 0 minutes, which means no timeout.
Local Authentication	
<b>Group Name</b>	Assigns an existing group to the profile. All users who belong to the group are permitted to access the network through this portal. The option 'Default' means a group which includes all users.

Radius Authentication	
<b>Primary Server</b>	Enter the IP address of the RADIUS Server on your network.
<b>Primary Server Port</b>	Enter the port number used for connections to the RADIUS Server.
<b>Primary Shared Secret</b>	Enter the key value to match the RADIUS Server.
<b>Backup Server</b>	The Backup Authentication Server will be used when the Primary Authentication Server is not available.
<b>Backup Server Port</b>	Enter the port number used for connections to the Backup RADIUS Server.
<b>Backup Shared Secret</b>	Enter the key value to match the Backup RADIUS Server.
Password Only Authentication	
<b>Password</b>	The password for the profile. Wireless clients only need one password to access the wireless network.

## Local User

Go to *Configuration > Captive Portal > Local User* to configure user settings for Captive Portal. Up to 128 users are supported.

The screenshot shows the Linksys web interface for the LAPAC1750C AC1750 Dual Band Access Point. The navigation menu on the left is expanded to show the 'Captive Portal' section, which includes 'Local User'. The main content area is titled 'User' and contains a 'Local User Table' with columns for 'User Name', 'New Password', and 'Confirm New Password'. There are 'Add' and 'Delete' buttons below the table, and 'Save' and 'Cancel' buttons at the bottom right.

<b>User Name</b>	Enter the name of the user account.  The user name includes 1 to 32 characters. Special characters except ':' and ';' are allowed.
<b>Password</b>	Enter the password of the user account.  The password must be between 4 and 32 characters in length. Special characters except ':' and ';' are allowed.
<b>Confirm Password</b>	Re-enter the password to confirm it.

## Local Group

Go to *Configuration > Captive Portal > Local Group* to configure group settings. Groups include multiple local users and are mapped to Captive Portal profiles. Up to two groups are supported.

The screenshot displays the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration' (selected), 'Maintenance', and 'Support'. The left sidebar shows a tree view with 'Administration' expanded, containing 'LAN', 'Wireless', 'Captive Portal' (selected), 'Global Configuration', 'Portal Profiles', 'Local User', 'Local Group' (selected), 'Web Customization', 'Profile Association', 'Client Information', and 'Cluster'. The main content area is titled 'Group' and contains a 'New Group' section with a 'Group Name' input field (range: 1-32 characters) and an 'Add' button. Below this is the 'Group Members' section, which includes a 'Group Selection' dropdown, a 'Delete' button, and two list boxes: 'Members' and 'Other Users'. Both list boxes are currently empty and marked with 'End of List' at the bottom. Navigation arrows '<<' and '>>' are positioned between the two list boxes.

<b>Group Name</b>	<p>Enter the name of the new group.</p> <p>The group name includes 1 to 32 characters. Special characters except ':' and ';' are allowed.</p> <p>Click <b>Add</b>.</p>
<b>Group Selection</b>	<p>Select one group to delete or configure its user members.</p>
<b>Members</b>	<p>User members of the selected group. You can select one user and click "&gt;&gt;" button to remove it.</p>
<b>Other Users</b>	<p>Other users which don't belong to the selected group. You can select one user and click "&lt;&lt;" button to add it into the group.</p>

## Web Customization

Go to *Configuration > Captive Portal > Web Customization* to customize the authentication web page of Captive Portal.

**LINKSYS**  
LAPAC1750C AC1750 Dual Band Access Point

Help Log out  
Enable Cloud Manager

System Status Quick Start **Configuration** Maintenance Support

Administration  
LAN  
Wireless  
▼ **Captive Portal**  
Global Configuration  
Portal Profiles  
Local User  
Local Group  
Web Customization  
Profile Association  
Client Information  
Cluster

**Web Customization**

Profile: Profile 1

New Logo Upload: Choose File No file chosen Upload

Logo Selection: Default Delete

Background Color: #0073BA (Format: #xxxxxx, Default: #0073BA)

Font Color: #FFFFFF (Format: #xxxxxx, Default: #FFFFFF)

Welcome Title: Welcome to the Wireless Network (Range: 1-64 Characters)

Login Instruction: You can login using your username and password. (Range: 1-96 Characters)

User Label: Username: (Range: 1-16 Characters)

Password Label: Password: (Range: 1-16 Characters)

Button Name: Connect (Range: 1-12 Characters)

Button Color: #70A0D4 (Format: #xxxxxx, Default: #70A0D4)

Term of Use Label: Check here to indicate that you have read and a (Range: 1-128 Characters)

Terms of use

Term of Use: (Max 1024 characters)

Success Text: You have logged on successfully!<br>Please keep (Range: 1-128 Characters)

Failure Text: Bad username or password! (Range: 1-128 Characters)

Preview Save Cancel

<b>Profile</b>	Select a profile to configure.
<b>New Logo Upload</b>	<p>Logos display in the web page. Select an image file from your local PC and click Upload.</p> <p>Formats .gif, .png and .jpg are supported. File size cannot exceed 5KB.</p> <p>One profile can support one default and one new logo image. If a second new logo is uploaded, it will replace the first new logo.</p>
<b>Logo Selection</b>	Select a logo image from the list.
<b>Background Color</b>	The HTML code for the background color in 6-digit hexadecimal format. The default is #0073BA.
<b>Font Color</b>	The HTML code for the font color in 6-digit hexadecimal format. The default is #FFFFFF.
<b>Welcome Title</b>	Customize text to go with your logo. The default is <i>Welcome to the Wireless Network.</i>
<b>Login Instruction</b>	<p>Customize text to go with the login box. Default text for different authentication options:</p> <p>Local Authentication/Radius Authentication You can log in using your username and password."</p> <p>Password Only Authentication You can log in using your password.</p> <p>Local Authentication Click Connect to log in.</p>
<b>User Label</b>	Customize the username text box. Enter up to 16 characters. The default is "Username".
<b>Password Label</b>	Customize the user password text box. Enter up to 16 characters. The default is "Password".
<b>Button Name</b>	Customize the text that appears in the log in button. Enter up to 12 characters. The default is "Connect".
<b>Button Color</b>	The HTML code for the background color of the button in 6-digit hexadecimal format. The default is #70A0D4.
<b>Terms of Use Label</b>	Customize the text to go with the checkbox. Enter up to 128 characters. The default is "Check here to indicate that you have read and accepted the following Terms of Use."

<b>Terms of Use</b>	Customize the text to go with Terms of Use. Enter up to 512 characters. The default is "Terms of Use".
<b>Success Text</b>	Customize the text that shows when the client has been authenticated. The default is "You have logged on successfully! Please keep this window open when using the wireless network."
<b>Failure Text</b>	Customize the text that shows when authentication fails. Enter up to 128 characters. The default is "Bad username or password"

## Profile Association

Go to *Configuration > Captive Portal > Profile Association* to associate defined Captive Portal profiles with SSIDs.

**LINKSYS** LAPAC1750C AC1750 Dual Band Access Point

Help Log out Enable Cloud Manager

System Status Quick Start **Configuration** Maintenance Support

Administration  
LAN  
Wireless  
**Captive Portal**  
Global Configuration  
Portal Profiles  
Local User  
Local Group  
Web Customization  
Profile Association  
Client Information  
Cluster

### Profile Association

Select Your Radio

Wireless Radio: Radio 1

SSID	SSID Name	Profile
SSID 1	LinksysSMB24G	None
SSID 2		None
SSID 3		None
SSID 4		None
SSID 5		None
SSID 6		None
SSID 7		None
SSID 8		None

Save Cancel

<b>SSID</b>	A list of available SSIDs.
<b>SSID Name</b>	The name of the SSID.
<b>Profile Name</b>	Choose the profile that is associated with the SSID. If the profile associated with the SSID is deleted, then the association will be removed. If <i>None</i> is selected, it means no profile is associated.

## Client Information

Go to *Configuration > Captive Portal > Client Information* to view the status of wireless clients that are authenticated by Captive Portal.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The navigation menu on the left includes Administration, LAN, Wireless, and Captive Portal. The Captive Portal section is expanded, showing options like Global Configuration, Portal Profiles, Local User, Local Group, Web Customization, Profile Association, and Client Information. The Client Information page is active, displaying a table of authenticated clients. The table has columns for MAC Address, IP Address, User Name, SSID, Online Time (sec), Away Timeout (sec), Session Timeout (sec), and Operation. A Refresh button is located below the table.

<b>MAC Address</b>	MAC address of the client.
<b>IP Address</b>	IP address of the client.
<b>User Name</b>	User name used by the client to log in.
<b>SSID Name</b>	Name of the SSID to which the client is connected.
<b>Online Time</b>	How long the client has been online. Measured in seconds.



<b>Away Timeout</b>	An authenticated client that has been disconnected from the access point has a specific amount of time within which it may reconnect without re-authentication. The timer starts when the client disconnects from the SSID. After the time reaches zero, the client is de-authenticated. If the timeout is set to 0, the client is not de-authenticated. Measured in seconds.
<b>Session Timeout</b>	The remaining time of the authenticated session. The timer starts when the client is authenticated. After the time reaches zero, the client is de-authenticated. If the value is fixed to 0, the session won't time out. Measured in seconds.

## Cluster

The cluster function provides a centralized method to administer and control wireless services across multiple devices. When access points are clustered, you can view, deploy, configure, and secure the wireless network as a single entity.

**Note**-Firmware version 1.1.0 or above support cluster feature. If your device has legacy firmware installed, download the latest one from [www.linksys.com/support](http://www.linksys.com/support).

The access points within a cluster must have the same management VLAN configured. A cluster can support 16 LAPAC1200C/LAPAC1750C access points, as long as they are same model number.

In each cluster, one access point must be manually configured as the master access point. There can only be one master in a cluster. This master will propagate configuration information, such as wireless settings, time settings etc. to the other team members within a cluster. Log in to the master access point to change sharable parameter settings instead of slaves.

When firmware is upgraded on the master, all slaves within the same cluster will receive the upgrade.

Clustered access points share these configurations:

- User Accounts
- Time Settings
- Log Settings
- Management Access
- Discovery Settings
- IGMP/MLD Snooping
- Wireless Network Mode
- SSID Settings
- Wireless Security
- Rogue AP Detection
- Wireless Scheduler
- Wireless Scheduler Association
- Wireless Connection Control
- Rate Limit
- QoS
- Advanced Wireless Settings
- Captive Portal Settings
- Ethernet Port Settings
- VLAN Settings

These configurations are not shared by clustered access points:

- IP Settings
- WDS
- Output Power
- Hostname
- Workgroup Bridge
- Wireless Channel
- 802.1x Supplicant

## Settings & Status

Go to *Configuration > Cluster > Settings & Status* to manage the AP cluster function.

Choose a member type.

The screenshot displays the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance', and 'Support'. The left sidebar shows a tree view with 'Cluster' selected. The main content area is titled 'Cluster Settings' and contains a 'Member Type' section with three radio buttons: 'Master', 'Slave', and 'Disabled' (which is selected). Below the radio buttons are 'Save', 'Refresh', and 'Cancel' buttons.

<b>Type</b>	<p>Disabled—Disable the cluster function.</p> <p>Master—Enable the cluster function and assign the access point to be the master.</p> <p><b>Note</b>— <i>If system detects there is one Master already existed in the same cluster, the new access point that likes to become master will be assigned to slave automatically.</i></p> <p>Slave—Enable the cluster function and assign the access point to be the slave.</p> <p><b>Note</b>— <i>When the cluster function is enabled, WDS and workgroup bridge will be disabled automatically.</i></p>
-------------	---

## Master

**LINKSYS** LAPAC1750C AC1750 Dual Band Access Point

Help Log out

Enable Cloud Manager

System Status Quick Start **Configuration** Maintenance Support

Administration  
LAN  
Wireless  
Captive Portal  
**Cluster**  
Settings & Status  
Client Sessions  
Channel Management

### Cluster Settings

**Member Type**

☒ Master ☐ Slave ☐ Disabled

**Cluster Status**

Status: Disabled

Member Number: 0

**Cluster Settings**

Location:  (Range: 0-32 characters)

Cluster Name:  (Range: 4-32 characters)

**Cluster Members**

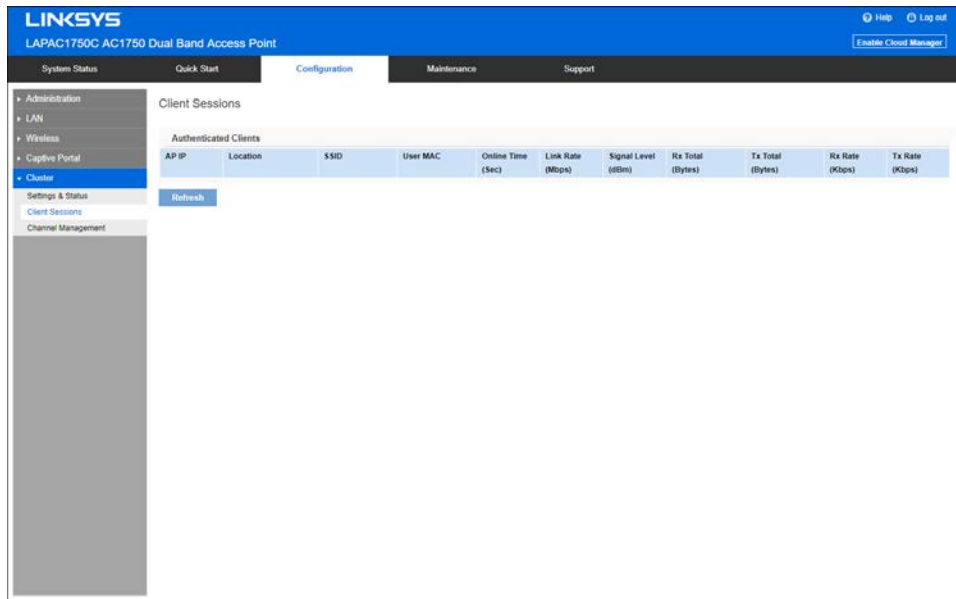
Type	Location	MAC Address	IP Address	Firmware Version

Save Refresh Cancel

<b>Status</b>	<p>Disabled—Cluster function is disabled.</p> <p>Active—Cluster function is enabled and master is active.</p> <p>Active (Backup Master)—Cluster function is enabled and backup master is active.</p> <p>Inactive (Cannot reach the master)—Cluster function is enabled but it's inactive because device cannot reach the master.</p>
<b>Member Number</b>	Number of the members active in the cluster. If an access point joins the cluster but is powered off or cannot reach the master, it is not counted.
<b>Location (Optional)</b>	Where the access point is physically located; for example, Reception. Length is from 0 to 32 bytes.
<b>Cluster Name</b>	<p>Name of the cluster for the LAP device to join; for example, "lab cluster".</p> <p>All access points with the same cluster name belong to the same cluster. Length of this value is from 4 to 32 bytes and special characters are allowed. This is a mandatory field if the cluster function is turned on.</p>
<b>Backup Master</b>	<p>When an access point works as a cluster slave, it can be enabled as a backup master. When master gets offline, it will take the role of master.</p> <p>When the backup master begins to work, it will send advertisements and slaves will send keep-alive and report sessions to it. When shareable settings are modified in it, it will share them to all slaves.</p> <p>When master gets online again, this backup master AP will stop the master function and let original master AP take over master role.</p>

## Client Sessions

Go to *Configuration > Cluster > Client Sessions* to see the status of wireless clients within the cluster.



The session is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the WLAN client logs on to the network, and the session ends when the WLAN client either logs off intentionally or loses the connection for some other reason.

When one wireless client of Captive Portal roams from one access point to another in the same cluster, it need not re-authenticate.

<b>IP Address</b>	IP address of the access point to which the client connects.
<b>Location</b>	Location of the access point to which the client connects.
<b>SSID</b>	SSID name of the access point to which the client connects.
<b>User MAC</b>	MAC address of the client.
<b>Online Time</b>	Displays how long this client has been online since it is authenticated. Unit is second.
<b>Link Rate</b>	Indicates the link rate of the client. Unit is Mbps.
<b>Signal</b>	The signal strength of the client is displayed. Unit is dBm.
<b>Rx Total</b>	The total bytes which are received from the client by the access point. Unit is Byte.

<b>Tx Total</b>	The total bytes which are sent to the client by the access point. Unit is Byte.
<b>Rx Rate</b>	Current transfer rate of the data which are received from the client by the access point. Unit is Kbps.
<b>Tx Rate</b>	Current transfer rate of the data which are sent to the client by the access point. Unit is Kbps.

## Channel Management

Go to *Configuration > Cluster > Channel Management* to manage the channel assignments for access points within a cluster.

**LINKSYS** LAPAC1750C AC1750 Dual Band Access Point

Help Log out Enable Cloud Manager

System Status Quick Start **Configuration** Maintenance Support

Administration  
LAN  
Wireless  
Captive Portal  
**Cluster**  
Settings & Status  
Client Sessions  
Channel Management

### Channel Management

**Auto Channel**

Auto Channel: ☐ Enable

Scan Date: Daily

Scan Time: 00 : 00 (Hour : Minute)

Scan Trigger: Immediately

**Current Channels**

Type	Location	IP Address	Wireless Radio	Status	Channel	Locked

Save Refresh Cancel

When channel management is enabled, the access point automatically assigns radio channels within a cluster. Auto channel assignment reduces mutual interference (or interference with other access points outside of its cluster) and maximizes Wi-Fi bandwidth to help maintain efficient communication over the wireless network.

<b>Auto Channel</b>	
<b>Auto Channel</b>	Access point scans available Wi-Fi channels and changes the channel if better network performance is possible. Disabled by default.
<b>Scan Day</b>	Choose the day of the week when Auto Channel scans Wi-Fi channels. You may choose specific days or have the access point scan and select the best channel daily.
<b>Scan Time</b>	Choose the time of day when Auto Channel performs scan.
<b>Scan Trigger</b>	<p>Because Auto Channel will change the channel if it finds a better one, you can choose when to allow a scan.</p> <ul style="list-style-type: none"> <li>• Immediately – Scan according to the day/time specified.</li> <li>• No Clients – Scan only if no clients are connected to the wireless radio. If there are clients connected, the access point will complete the Auto Channel operation the next scheduled time when no clients are connected.</li> </ul>
<b>Current Channels</b>	
<b>Type</b>	Member type of the access point. It can be Master, Slave or Backup Master.
<b>Location</b>	Where the access point is physically located
<b>IP Address</b>	IP address of the access point.
<b>Wireless Radio</b>	1 stands for 2.4Ghz radio, and 2 stands for 5Ghz radio.
<b>Status</b>	Status of the wireless radio. It can be Active or Inactive.
<b>Channel</b>	Current channel number of the wireless radio.
<b>Locked</b>	Select if you feel the current channel is the best for that radio.

# System Status

## Status

### System Summary

Go to *System Status* > *Status* > *System Summary* for status of the access point.

LINKSYS

LAPAC1750C AC1750 Dual Band Access Point

Help Log out

Enable Cloud Manager

System Status

Quick Start

Configuration

Maintenance

Support

Status

System Summary

LAN Status

Wireless Status

Wireless Clients

Statistics

Log View

System Summary

Device SKU: LAPAC1750C

Firmware Version: V1.0.00.003

Firmware Checksum: 083ee0a566ff1e64

Hardware Version: V01

Local MAC Address: 58:EF:68:B3:54:D4

Serial Number: 26F10S03800052

Host Name: lap354d4

System Up Time: 2 days, 22 hours, 48 minutes, 41 seconds

System Time: 2018/06/04 Mon 08:21:32 (-08:00)

Power Source: PoE

Cloud Status: Disabled

Refresh

### System Summary

Device SKU	The SKU is often used to identify device model number and region.
Firmware Version	The version of the firmware currently installed.
Firmware Checksum	The checksum of the firmware running in the access point.
Hardware Version	The version of the hardware.
Local MAC Address	The MAC (physical) address of the wireless access point.
Serial Number	The serial number of the device.



<b>Host Name</b>	The host name assigned to the access point.
<b>System Up Time</b>	How long the system has been running since the last restart or reboot.
<b>System Time</b>	The current date and time.
<b>Power Source</b>	The power source of the access point. It can be Power over Ethernet (PoE) or Power Adapter. When two power sources are plugged in, Power Adaptor will be displayed.
<b>Cloud Status</b>	Whether cloud management is enabled or disabled.

## LAN Status

Go to *System Status > Status > LAN Status* to see settings and status of LAN interface.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes links for Help, Log out, and an 'Enable Cloud Manager' button. The main menu has tabs for System Status, Quick Start, Configuration, Maintenance, and Support. The left sidebar shows a tree view with 'Status' expanded, containing System Summary, LAN Status (selected), Wireless Status, Wireless Clients, Statistics, and Log View. The main content area is titled 'LAN Status' and displays the following settings:

VLAN	
VLAN:	Disabled
Untagged VLAN:	Enabled
Untagged VLAN ID:	1
Management VLAN:	1
IPv4	
IP Address:	192.168.1.176
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
Primary DNS:	192.168.1.1
Secondary DNS:	0.0.0.0
IPv6	
IP Address:	
Default Gateway:	
Primary DNS:	
Secondary DNS:	

A 'Refresh' button is located at the bottom right of the settings area.

VLAN	
<b>VLAN</b>	Enabled or disabled (default).
<b>Untagged VLAN</b>	<p>Enabled (default) or disabled.</p> <p>When enabled, and if its VLAN ID is equal to Untagged VLAN ID, all traffic is untagged when sent from LAN ports. Untagged traffic can be accepted by LAN ports. If disabled, traffic is always tagged when sent from LAN port and only tagged traffic can be accepted from LAN port.</p> <p>By default all traffic on the access point uses VLAN 1, the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a SSID.</p>
<b>Untagged VLAN ID</b>	Displays the untagged VLAN ID. Traffic on the VLAN that you specify in this field is not be tagged with a VLAN ID when forwarded to the network. VLAN 1 is the default ID for untagged VLAN and management VLAN.
<b>Management VLAN</b>	<p>Displays the Management VLAN ID. The VLAN associated with the IP address you use to connect to the access point. Provide a number between 1 and 4094 for the Management VLAN ID. The default is 1.</p> <p>This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the access point.</p>
IPv4	
<b>IP Address</b>	The IP address of the wireless access point.
<b>Subnet Mask</b>	The Network Mask (Subnet Mask) for the IP address above.
<b>Default Gateway</b>	Enter the gateway for the LAN segment to which the wireless access point is attached (the same value as the PCs on that LAN segment).
<b>Primary DNS</b>	The primary DNS address provided by the DHCP server or configured manually.
<b>Secondary DNS</b>	The secondary DNS address provided by the DHCP server or configured manually.

IPv6	
IP Address	The IP address of the wireless access point.
Default Gateway	Enter the gateway for the LAN segment to which the wireless access point is attached (the same value as the PCs on that LAN segment).
Primary DNS	The primary DNS address provided by the DHCP server or configured manually.
Secondary DNS	The secondary DNS address provided by the DHCP server or configured manually.

## Wireless Status

Go to *System Status > Status > Wireless Status* to see settings and status of wireless radios and SSIDs.

LINKSYS

LAPAC1750C AC1750 Dual Band Access Point

[Help](#)
[Log out](#)

[Enable Cloud Manager](#)

System Status

Quick Start

Configuration

Maintenance

Support

▼ Status

System Summary

LAN Status

Wireless Status

Wireless Clients

Statistics

Log View

Wireless Status

Select Your Radio

Wireless Radio: Radio 1

Radio Status

Radio Status: Enabled

Mode: B/G/N-Mixed

Current Channel: 11

Channel Bandwidth: 20MHz

SSID Status

Interface	SSID Name	Status	MAC Address	VLAN ID	Priority	Scheduler State
SSID 1	First Wireless Name	Enabled	58:EF:68:B3:54:D5	1	0	N/A
SSID 2		Disabled	0A:EF:68:B3:54:D5	1	0	N/A
SSID 3		Disabled	1A:EF:68:B3:54:D5	1	0	N/A
SSID 4		Disabled	2A:EF:68:B3:54:D5	1	0	N/A
SSID 5		Disabled	3A:EF:68:B3:54:D5	1	0	N/A
SSID 6		Disabled	4A:EF:68:B3:54:D5	1	0	N/A
SSID 7		Disabled	5A:EF:68:B3:54:D5	1	0	N/A
SSID 8		Disabled	6A:EF:68:B3:54:D5	1	0	N/A

WDS Root

Status	Local MAC	Local SSID	VLAN List
Disabled	7A:EF:68:B3:54:D5	LinksysSMB24G-WDSRoot	1

WDS Station

Interface	Status	Local MAC	Remote SSID	Remote MAC	Connection Status
1	Disabled	8A:EF:68:B3:54:D5		00:00:00:00:00:00	Not Connected
2	Disabled	9A:EF:68:B3:54:D5		00:00:00:00:00:00	Not Connected
3	Disabled	AA:EF:68:B3:54:D5		00:00:00:00:00:00	Not Connected
4	Disabled	BA:EF:68:B3:54:D5		00:00:00:00:00:00	Not Connected

Workgroup Bridge

Status	Local MAC	Remote SSID	Remote MAC	Connection Status
Disabled	CA:EF:68:B3:54:D5		00:00:00:00:00:00	Not Connected

Refresh

Radio Status	
<b>Mode</b>	Current 802.11mode (a/b/g/n/ac) of the radio.
<b>Current Channel</b>	The channel currently in use.
<b>Channel Bandwidth</b>	Current channel bandwidth of the radio. When set to 20 MHz, only the 20 MHz channel is in use. When set to 20/40 MHz, Wireless-N connections will use 40 MHz channel, but Wireless-B and Wireless-G will still use 20 MHz channel.
SSID Status	
<b>Interface</b>	SSID index.
<b>SSID Name</b>	Name of the SSID.
<b>Status</b>	Status of the SSID: Enabled or Disabled.
<b>MAC Address</b>	MAC Address of the SSID.
<b>VLAN ID</b>	VLAN ID of the SSID.
<b>Priority</b>	The 802.1p priority of the SSID.
<b>Scheduler State</b>	<ul style="list-style-type: none"> <li>• N/A—No scheduler is enabled on the SSID, or the SSID is disabled by administrator.</li> <li>• Active—The SSID is enabled.</li> <li>• Inactive—The SSID is disabled.</li> </ul>

WDS Root	
<b>Status</b>	Status of the WDS Root: Enabled or Disabled.
<b>Local MAC</b>	MAC Address of the WDS Root.
<b>Local SSID</b>	Name of the WDS Root.
<b>VLAN List</b>	<p>VLAN List of the WDS Root.</p> <p>When VLAN function is enabled, WDS Root only receives packets in the VLAN list from WDS Stations and packets not in the list will be dropped.</p>
WDS Station	
<b>Interface</b>	The index of WDS Station.
<b>Status</b>	Status of the WDS Station: Enabled or Disabled.
<b>Local MAC</b>	MAC Address of the WDS Root.
<b>Remote SSID</b>	SSID of the destination access point which is on the other end of the WDS link to which data is sent or handed-off and from which data is received.
<b>Remote MAC</b>	MAC Address of the destination access point which is on the other end of the WDS link to which data is sent or handed-off and from which data is received.
<b>Connection Status</b>	Status of the WDS Station: Disabled, Connected or Not Connected.
Workgroup Bridge	
<b>Status</b>	Status of the Workgroup Bridge: Enabled or Disabled.
<b>Local MAC</b>	MAC address of the Workgroup Bridge.
<b>Remote SSID</b>	SSID of the destination access point on the other end of the Workgroup Bridge link to which data is sent and from which data is received.
<b>Remote MAC</b>	MAC address of the destination access point on the other end of the Workgroup Bridge link to which data is sent and from which data is received.
<b>Connection Status</b>	Status of the Workgroup Bridge: Disabled, Connected or Not Connected.

## Wireless Clients

Go to *System Status > Status > Wireless Clients* to see connected clients based on each wireless interface.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance', and 'Support'. The left sidebar shows 'Status' expanded with options like 'System Summary', 'LAN Status', 'Wireless Status', 'Wireless Clients', 'Statistics', and 'Log View'. The main content area is titled 'Wireless Clients' and includes a 'Select Your Wireless Interface' dropdown menu set to 'Radio 1'. Below this is a table of connected clients.

SSID Name	Client MAC	SSID MAC	Link Rate (Mbps)	RSSI (dBm)	Online Time (sec)
First Wireless Name	18:65:90:DA:89:59	58:EF:68:B3:54:D5	164	-37	50
First Wireless Name	AC:5F:3E:67:3A:C5	58:EF:68:B3:54:D5	123	-33	10

A 'Refresh' button is located at the bottom right of the table.

Wireless Interface	Select the desired interface from the list. The interfaces include eight SSIDs per radio.
SSID Name	Name of the SSID to which the client connects.
Client MAC	The MAC address of the client.
SSID MAC	MAC of the SSID to which the client connects.
Link Rate	The link rate of the client. Unit is Mbps.
RSSI	The signal strength of the client. Unit is dBm.
Online Time	How long this client has been online. Unit is seconds.

## Interface Statistics

Go to *System Status > Status > Statistics* to see real-time statistics on data transmitted and received based on each SSID per Radio, and LAN interface.

LINKSYS

LAPAC1750C AC1750 Dual Band Access Point

Help Log out

Enable Cloud Manager

System Status

Quick Start

Configuration

Maintenance

Support

Status

System Summary

LAN Status

Wireless Status

Wireless Clients

Statistics

Log View

Interface Statistics

Select Your Radio

Wireless Radio: Radio 1

Transmit

Interface	Total Packets	Total Bytes	Total Dropped Packets	Total Dropped Bytes	Errors
LAN	224,737	32,854,591	0	0	0
SSID 1	25,447	34,900,239	0	0	0
SSID 2	0	0	0	0	0
SSID 3	0	0	0	0	0
SSID 4	0	0	0	0	0
SSID 5	0	0	0	0	0
SSID 6	0	0	0	0	0
SSID 7	0	0	0	0	0
SSID 8	0	0	0	0	0
WDS Root	0	0	0	0	0
WDS Station 1	0	0	0	0	0
WDS Station 2	0	0	0	0	0
WDS Station 3	0	0	0	0	0
WDS Station 4	0	0	0	0	0
WGB	0	0	0	0	0

Receive

Interface	Total Packets	Total Bytes	Total Dropped Packets	Total Dropped Bytes	Errors
LAN	891,948	714,845,992	0	0	146
SSID 1	51,761	6,354,950	0	0	28,222
SSID 2	0	0	0	0	0
SSID 3	0	0	0	0	0
SSID 4	0	0	0	0	0
SSID 5	0	0	0	0	0
SSID 6	0	0	0	0	0
SSID 7	0	0	0	0	0
SSID 8	0	0	0	0	0
WDS Root	0	0	0	0	0
WDS Station 1	0	0	0	0	0
WDS Station 2	0	0	0	0	0
WDS Station 3	0	0	0	0	0
WDS Station 4	0	0	0	0	0
WGB	0	0	0	0	0

Refresh

Interface	The name of the interface.
Wireless Radio	Select the desired radio from the list. Radio 1 is for 2.4 GHz, and Radio 2 is for 5 GHz.

## Transmit/Receive

- **Total Packets**—The total packets sent (in Transmit table) or received (in Received table) by the interface.
- **Total Bytes**—The total bytes sent (in Transmit table) or received (in Received table) by the interface.
- **Total Dropped Packets**—The total number of dropped packets sent (in Transmit table) or received (in Received table) by the interface.
- **Total Dropped Bytes**—The total number of dropped bytes sent (in Transmit table) or received (in Received table) by the interface.
- **Errors**—The total number of errors related to sending and receiving data on this interface.

## Log View

Go to **System Status > Status > Log View** to see a list of system events such as login attempts and configuration changes.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes links for Help, Log out, and Enable Cloud Manager. The main navigation menu has tabs for System Status, Quick Start, Configuration, Maintenance, and Support. The left sidebar shows the Status section expanded, with options for System Summary, LAN Status, Wireless Status, Wireless Clients, Statistics, and Log View. The Log View page displays a list of log messages, including:

- May 31 07:42:54 [CLOUD] Linksys cloud is enabled.
- May 31 07:43:01 [CLOUD] Linksys cloud is enabled.
- May 31 07:43:15 [CLOUD] Linksys cloud is connected.
- May 31 07:44:22 [CLOUD] Linksys cloud is disconnected.
- May 31 07:44:38 [CLOUD] Linksys cloud is connected.
- May 31 09:15:01 [WEB\_LOGIN] Authorized Login from 192.168.1.217
- May 31 09:24:06 [CONFIG\_CHANGE] lan\_ipaddr was changed to "192.168.1.252".
- May 31 09:24:06 [CONFIG\_CHANGE] lan\_gateway was changed to "255.255.255.255".
- May 31 09:24:06 [CONFIG\_CHANGE] lan\_dns1 was changed to "0.0.0.0".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile1\_name was changed to "default".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile1\_rule1 was changed to "default,0\_08:00-17:00".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile1\_rule2 was changed to "default,0\_08:00-17:00".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile1\_rule3 was changed to "default,0\_08:00-17:00".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile1\_rule4 was changed to "default,0\_08:00-17:00".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile2\_name was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile2\_rule1 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile2\_rule2 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile2\_rule3 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile2\_rule4 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile3\_name was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile3\_rule1 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile3\_rule2 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile3\_rule3 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile3\_rule4 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile4\_name was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile4\_rule1 was changed to "".
- May 31 09:24:06 [CONFIG\_CHANGE] wlan\_profile4\_rule2 was changed to "".



<b>Log Messages</b>	
<b>Log Messages</b>	Show the log messages.
<b>Buttons</b>	
<b>Refresh</b>	Update the data on screen.
<b>Save</b>	Save the log to a file on your PC.
<b>Clear</b>	Delete the existing logs from device.

# Maintenance

## Maintenance

### Firmware Upgrade

Go to *Maintenance > Maintenance > Firmware Upgrade* to upgrade the firmware in the wireless access point by using HTTP/HTTPS, or TFTP.

Check the Linksys support website (<http://www.linksys.com/support>) and download the latest firmware release to a storage device or PC. Perform the firmware upgrade by following the steps below.

If an access point works as master of an AP cluster, all slaves within the same cluster will be updated, as well.

Do not power off the device or disconnect the ethernet cable during the upgrade. The access point will reboot automatically after the upgrade is complete.

The screenshot displays the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance' (selected), and 'Support'. The 'Maintenance' section is expanded, showing 'Firmware Upgrade' as the active option. The main content area is titled 'Firmware Upgrade' and contains three sections: 'UPGRADE FIRMWARE FROM LOCAL PC', 'UPGRADE FIRMWARE FROM TFTP SERVER', and 'UPGRADE FIRMWARE FROM INTERNET'. The 'LOCAL PC' section has a 'Select a file to upgrade.' prompt, a 'Firmware File:' label, a 'Choose File' button, and an 'Upgrade' button. The 'TFTP SERVER' section has a 'Source File:' label, a text input field, a 'TFTP Server:' label, and four IP address input fields, followed by an 'Upgrade' button. The 'INTERNET' section has a 'Check for Upgrade' button.

**To perform the firmware upgrade from local PC:**

1. Click **Choose File** to navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear next to the **Choose File** button.
3. Click **Upgrade**.

### To perform the firmware upgrade from TFTP server:

1. Enter the IP address of the TFTP server and the source file. The source file is the firmware filename you stored in your TFTP server. Only IPv4 addresses are supported.
2. Click **Upgrade**.

### To perform a firmware upgrade from the Internet:

1. Click **Check for Upgrade** to see if there is new firmware available.
2. Click the **OK** on the popup dialogue box to start the firmware download and upgrade if a new version of firmware is available.

## Configuration Backup/Restore

Go to Maintenance > Maintenance > Configuration Backup/Restore to download the configuration file from the device. You can save it to external storage, e.g., your PC, or network storage. You can also upload a previously saved configuration file from external storage to the device. It is highly recommended you save one extra copy of the configuration file to external storage after you are done with access point setup.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance' (selected), and 'Support'. The left sidebar shows 'Maintenance' expanded with options: 'Firmware Upgrade', 'Configuration Backup/Restore' (selected), 'Factory Default', 'Reboot', and 'Diagnostics'. The main content area is titled 'Configuration Backup/Restore' and contains two sections: 'BACKUP/RESTORE TO/FROM LOCAL PC' and 'BACKUP/RESTORE TO/FROM TFTP SERVER'. The first section has 'Backup Configuration' with a 'Backup' button and 'Restore Configuration' with a 'Choose File' button (showing 'No file chosen') and a 'Restore' button. The second section has 'Backup Configuration to TFTP Server' with a 'Destination File' input, a 'TFTP Server' input (IP address format), and a 'Backup' button. It also has 'Restore Configuration from TFTP Server' with a 'Source File' input, a 'TFTP Server' input (IP address format), and a 'Restore' button.

Backup/Restore to/from Local PC	
<b>Backup Configuration</b>	<p>Once you have the access point working properly, you should back up the settings to a file on your computer. You can later restore the access point's settings from this file, if necessary.</p> <p>To create a backup file of the current settings:</p> <ul style="list-style-type: none"> <li>• Click <b>Backup</b>.</li> <li>• If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click <b>Save</b>.</li> </ul>
<b>Restore Configuration</b>	<p>To restore settings from a backup file:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose File</b>.</li> <li>2. Locate and select the previously saved backup file.</li> <li>3. Click <b>Restore</b>.</li> </ol>
Backup/Restore to/from TFTP server	
<b>Backup Configuration</b>	<p>To create a backup file of the current settings:</p> <ol style="list-style-type: none"> <li>1. Enter the destination file name you plan to save in TFTP server.</li> <li>2. Enter the IP address for the TFTP server. Only IPv4 addresses are supported.</li> <li>3. Click <b>Backup</b>.</li> </ol>
<b>Restore Configuration</b>	<p>To restore settings from a backup file:</p> <ol style="list-style-type: none"> <li>1. Enter the source file name stored in TFTP server.</li> <li>2. Enter the IP address for the TFTP server. Only IPv4 addresses are supported.</li> <li>3. Click <b>Restore</b>.</li> </ol>

## Factory Default

It's highly recommended you save your current configuration file before you restore to factory default settings. To save your current configuration file, click *Maintenance > Configuration Backup/Restore*.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance' (selected), and 'Support'. A left sidebar lists 'Maintenance' (expanded) with sub-items: 'Firmware Upgrade', 'Configuration Backup/Restore', 'Factory Default' (selected), 'Reboot', and 'Diagnostics'. The main content area is titled 'Factory Default' and contains a section 'Factory Default:' with two radio buttons: 'Reset All Parameters to Factory Default' (unselected) and 'No' (selected). At the bottom right of this section are 'Save' and 'Cancel' buttons.

### Factory Default

To restore your access point to its factory defaults, select an option and click **Save**.

- Reset All Parameters to Factory Default
  - No
- Don't restore to factory defaults.

## Reboot

Go to *Maintenance > Maintenance > Reboot* to power cycle the device. The current configuration file will remain after reboot.

The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance' (selected), and 'Support'. A left sidebar lists 'Maintenance' (expanded) with sub-items: 'Firmware Upgrade', 'Configuration Backup/Restore', 'Factory Default', 'Reboot' (selected), and 'Diagnostics'. The main content area is titled 'Reboot' and contains a section 'Device Reboot:' with two radio buttons: 'Yes' (selected) and 'No' (unselected). At the bottom right of this section are 'Save' and 'Cancel' buttons.

### Device Reboot

If you click **Save** when the Yes radio button is selected, the device will power cycle.

## Diagnostics

### Ping Test

Go to *Maintenance > Diagnostics > Ping Test* to determine the accessibility of a host on the network.

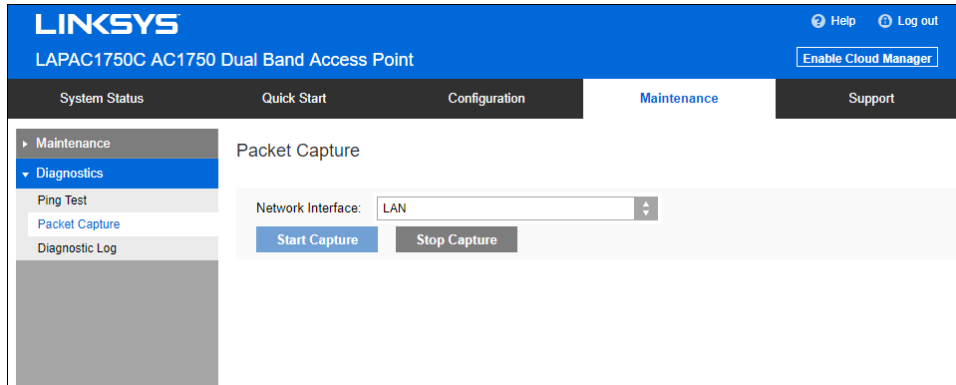
The screenshot shows the Linksys web interface for a LAPAC1750C AC1750 Dual Band Access Point. The top navigation bar includes 'System Status', 'Quick Start', 'Configuration', 'Maintenance' (selected), and 'Support'. The left sidebar shows 'Maintenance' > 'Diagnostics' > 'Ping Test' (selected). The main content area is titled 'Ping Test' and contains the following fields:

- IP Type:** A dropdown menu set to 'IPv4'.
- IP or Domain Name:** A text input field.
- Packet Size:** A text input field set to '32' bytes (32~65500).
- Times to Ping:** A dropdown menu set to '5' seconds.
- Ping Result:** A large empty text area for the results.
- Buttons:** 'Start to Ping' and 'Stop' buttons at the bottom right.

General	
IP Type	Enter the IP type of destination address.
IP or Domain Name	Enter the IP address or domain name that you want to ping.
Packet Size	Enter the size of the packet.
Times to Ping	Select the desired number from the drop-list. <ul style="list-style-type: none"><li>• 5</li><li>• 10</li><li>• 15</li><li>• Unlimited</li></ul>
Ping Result	Ping measures how fast you get a response after you've sent out a request. Measured in milliseconds (ms).

## Packet Capture

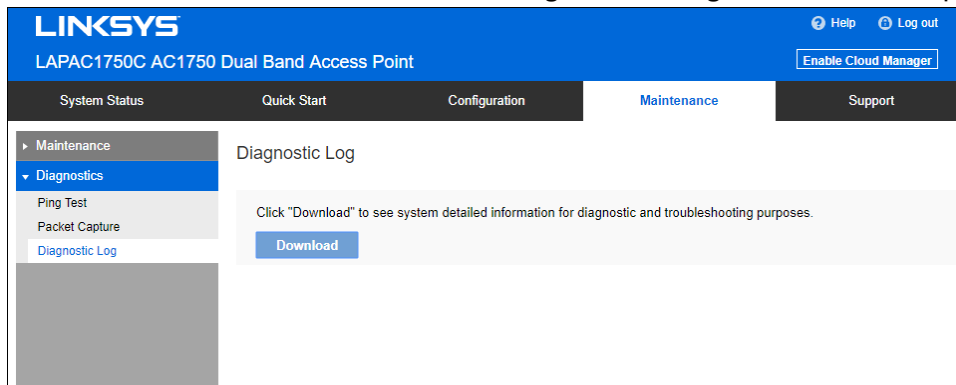
Go to *Maintenance > Diagnostics > Packet Capture* to capture and store 802.3 packets received and transmitted by the access point based on one specified network interface. The network interface can be radio, SSID or LAN.



<b>Network Interface</b>	Select the desired network interface from the drop-down list. The interface can be Radio, SSID or Ethernet.
<b>Start Capture</b>	Click to start the capture. You will be asked to specify a local file to store the packets.
<b>Stop Capture</b>	Click to stop the capture.

## Diagnostic Log

Go to *Maintenance > Diagnostics > Diagnostic Log* to get system detail information, such as configuration file, system status and statistics data, hardware information, operational status. The information is useful in troubleshooting and working with technical support.



Click **Download** to download the device diagnostic log into a local file.

# Appendix A - Troubleshooting

## Overview

This chapter covers some common problems encountered while using the wireless access point, and some possible solutions to them. If you follow the suggested steps and the wireless access point still does not function properly, contact your dealer for further advice.

## General Problems

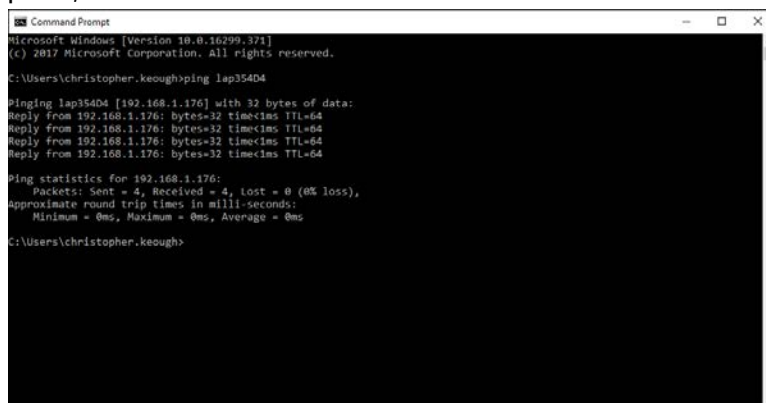
### I can't find new access point on my network.

Check the following:

- The wireless access point is properly installed, LAN connections are OK, and it is powered ON. Check the LEDs for system and port status.
- Ensure that your PC and the wireless access point are on the same network segment. (If you don't have a router, this must be the case.)
- You can use the following method to determine the IP address of the wireless access point, and then try to connect using the IP address, instead of the name.

To find the access point's IP address:

1. Open a MS-DOS Prompt or Command Prompt Window.
2. Use the Ping command to ping the wireless access point. Enter "ping" followed by the default name of the wireless access point. Default name is "lap" followed by the last five characters of device MAC address (e.g., ping lap964d6).
3. Check the output of the ping command to determine the IP address of the wireless access point, as shown below.



```
Microsoft Windows [Version 10.0.16299.371]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\christopher.keough>ping lap35404

Pinging lap35404 [192.168.1.176] with 32 bytes of data:
Reply from 192.168.1.176: bytes=32 time=1ms TTL=64
Reply from 192.168.1.176: bytes=32 time=1ms TTL=64
Reply from 192.168.1.176: bytes=32 time=1ms TTL=64
Reply from 192.168.1.176: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.176:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\christopher.keough>
```

If your PC uses a fixed (static) IP address, ensure that it is using an IP address that is in the network segment (subnet) with the wireless access point. On Windows PCs, you can use *Control Panel > Network* to check the properties for the TCP/IP protocol.



If there is no DHCP Server found, the wireless access point will roll back to an IP address and mask of 192.168.1.252 and 255.255.255.0.

### **My PC can't connect to the LAN via the wireless access point.**

Check the following:

- The SSID and security settings on the PC match the settings on the access point.
- On the PC, the wireless mode is set to Infrastructure.
- If using the Access Control feature, the PC's name and address is in the Trusted Stations list.
- If using 802.1x mode, ensure the PC's 802.1x software is configured correctly. See Appendix C ([p. 120](#)) for details of setup for the Windows XP 802.1x client. If using a different client, refer to the vendor's documentation.

# Appendix B - About Wireless LANs

## Overview

Wireless networks have their own terms and jargon. You must understand many of these terms in order to configure and operate a wireless LAN.

## Wireless LAN Terminology

### Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

#### Ad-hoc Mode

Ad-hoc Mode does not require an access point or a wired (Ethernet) LAN. Wireless stations, e.g., notebook PCs with wireless cards, communicate directly with each other.

#### Infrastructure Mode

In Infrastructure Mode, one or more access points are used to connect wireless stations, e.g., notebook PCs with wireless cards, to a wired (Ethernet) LAN. The wireless stations can then access all LAN resources.

**Note**—Access points can only function in Infrastructure Mode, and can communicate only with wireless stations that are set to Infrastructure Mode.

### SSID/ESSID

#### BSS/SSID

A group of wireless stations and a single access point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

## ESS/ESSID

A group of wireless stations, and multiple access points all using the same ID (ESSID), form an Extended Service Set (ESS).

Different access points within an ESS can use different channels. To reduce interference, it is recommended that adjacent access points use different channels.

As wireless stations are physically moved through the area covered by an ESS, they will automatically change to the access point that has the least interference or best performance.

## Channels

- The wireless channel sets the radio frequency used for communication.
- Access points use a fixed channel. You can select the channel used. This allows you to choose a channel that provides the least interference and best performance. For USA and Canada, the following channels are available:
  - 2.4GHz:
    - to 2.462 GHz; 11 channels
  - 5GHz:
    - 5.180 to 5.240 GHz; 4 channels
    - 5.745 to 5.825 GHz; 5 channels
- When using multiple access points it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is five channels, e.g., use Channels 1 and 6, or 6 and 11.
- In Infrastructure Mode wireless stations normally scan all channels looking for an access point. If more than one access point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using Ad-hoc Mode (no access point) all wireless stations should be set to use the same channel. However, most wireless stations will still scan all channels to see if there is an existing Ad-hoc group they can join.

## WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your wireless stations. If the data is encrypted, it is meaningless unless the receiver can decrypt it.

If WEP is used, the wireless stations and the wireless access point must have the same settings.

## WPA-PSK

In WPA-PSK, like WEP, data is encrypted before transmission. WPA is more secure than WEP. The PSK (pre-shared key) must be entered on each wireless station. The 256-bit encryption key is derived from the PSK, and changes frequently.

## WPA2-PSK

This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. It should be used if possible.

## WPA-Enterprise

This version of WPA requires a RADIUS server on your LAN to provide the client authentication according to the 802.1X standard. Data transmissions are encrypted using the WPA standard.

If this option is used:

- The access point must have a client login on the RADIUS server.
- Each user must have a user login on the RADIUS server.
- Each user's wireless client must support 802.1X and provide the login data when required.

All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

## WPA2-Enterprise

This version of WPA2 requires a RADIUS server on your LAN to provide the client authentication according to the 802.1X standard. Data transmissions are encrypted using the WPA2 standard.

If this option is used:

- The access point must have a client login on the RADIUS server.
- Each user must have a user login on the RADIUS server.
- Each user's wireless client must support 802.1X and provide the login data when required.

All data transmission is encrypted using the WPA2 standard. Keys are automatically generated, so no key input is required.

## 802.1x

This uses the 802.1X standard for client authentication, and WEP for data encryption. If possible, you should use WPA-Enterprise instead, because WPA encryption is much stronger than WEP encryption.

If this option is used:

- The access point must have a client login on the RADIUS server.
- Each user must have a user login on the RADIUS server.
- Each user's wireless client must support 802.1X and provide the login data when required.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

# Appendix C - PC and Server Configuration

## Overview

All wireless stations need to have settings that match the wireless access point. These settings depend on the mode in which the access point is being used.

- If using WEP or WPA2-PSK, it is only necessary to ensure that each wireless station's settings match those of the wireless access point, as described below.
- For 802.1x modes, configuration is much more complex. The RADIUS server must be configured correctly, and setup of each wireless station is also more complex.

## Using WEP

For each of the following items, each wireless station must have the same settings as the wireless access point.

<b>Mode</b>	On each PC, the mode must be set to Infrastructure.
<b>SSID (ESSID)</b>	<p>This must match the value used on the wireless access point.</p> <p>The default value is LinksysSMB24G for radio 1 and LinksysSMB5G for radio 2.</p> <p><b>Note</b>—<i>The SSID is case sensitive.</i></p>
<b>Wireless Security</b>	<ul style="list-style-type: none"><li>• Each wireless station must be set to use WEP data encryption.</li><li>• The key size (64 bit, 128 bit) must be set to match the access point.</li><li>• The key values on the PC must match the key values on the access point.</li></ul> <p><b>Note</b>—<i>One set of WEP keys is supported per radio.</i></p>

## Using WPA2-PSK

For each of the following items, each wireless station must have the same settings as the wireless access point.

<b>Mode</b>	On each PC, the mode must be set to Infrastructure.
<b>SSID (ESSID)</b>	<p>This must match the value used on the wireless access point.</p> <p>The default value is LinksysSMB24G for radio 1 and LinksysSMB5G for radio 2.</p> <p><b>Note</b>—<i>The SSID is case sensitive.</i></p>
<b>Wireless Security</b>	<p>On each client, wireless security must be set to WPA2-PSK.</p> <ul style="list-style-type: none"><li>• The pre-shared key entered on the access point must also be entered on each wireless client.</li><li>• The encryption method (e.g. TKIP, AES) must be set to match the access point.</li></ul>

## Using WPA2-Enterprise

This is the most secure and most complex system.

WPA-Enterprise mode provides greater security and centralized management, but it is more complex to configure.

### Wireless Station Configuration

For each of the following, wireless stations must have the same settings as the wireless access point.

<b>Mode</b>	On each PC, the mode must be set to Infrastructure.
<b>SSID (ESSID)</b>	<p>This must match the value used on the wireless access point.</p> <p>The default value is LinksysSMB24G for radio 1 and LinksysSMB5G for radio 2.</p> <p><b>Note</b>—<i>The SSID is case sensitive.</i></p>
<b>802.1x Authentication</b>	Each client must obtain a certificate for authentication for the RADIUS server.
<b>802.1x Encryption</b>	<p>Typically, EAP-TLS is used. This is a dynamic key system, so keys do NOT have to be entered on each wireless station.</p> <p>You can also use a static WEP key (EAP-MD5). The wireless access point supports both methods simultaneously.</p>

## RADIUS Server Configuration

If using WPA2-Enterprise mode, the RADIUS server on your network must be configured as follows:

- It must provide and accept certificates for user authentication.
- There must be a client login for the wireless access point itself.
- The wireless access point will use its default name as its client login name. (However, your RADIUS server may ignore this and use the IP address instead.)
- The Shared Key, set on the Security screen of the access point, must match the Shared Secret value on the RADIUS server.
- Encryption settings must be correct.

## 802.1x Server Setup (Windows 2000 Server)

This section describes using Microsoft Internet Authentication Server as the RADIUS server, since it is the most common RADIUS server available that supports the EAP-TLS authentication method.

The following services on the Windows 2000 Domain Controller (PDC) are also required.

- dhcpcd
- dns
- rras
- webserver (IIS)
- RADIUS Server (Internet Authentication Service)
- Certificate Authority

## Windows 2000 Domain Controller Setup

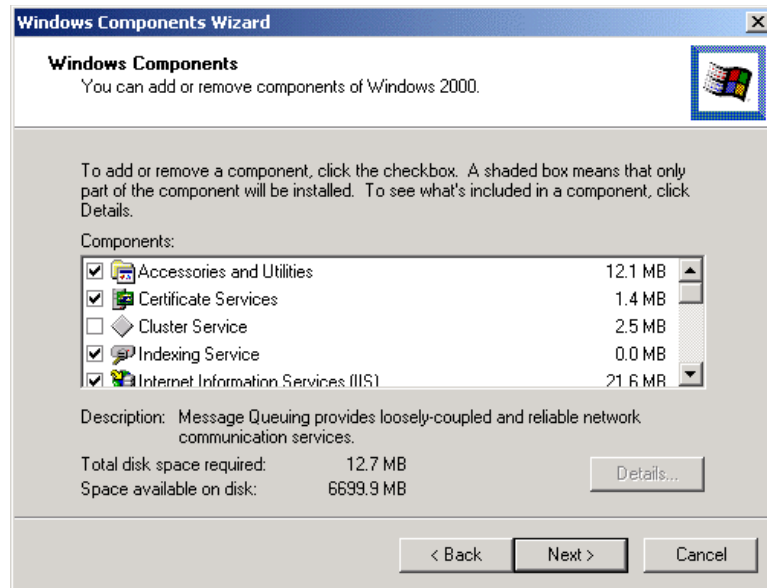
1. Run dcpromo.exe from the command prompt.
2. Follow all of the default prompts, ensure that DNS is installed and enabled during installation.

## Services Installation

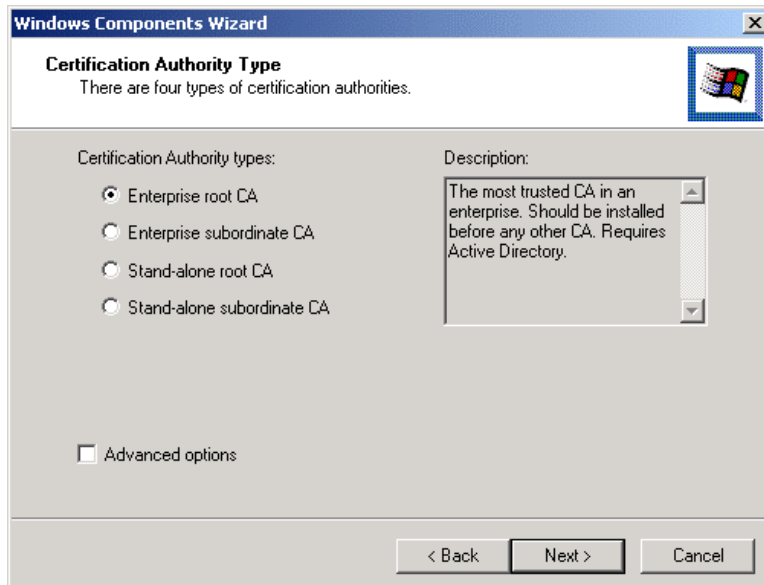
1. Select the *Control Panel > Add/Remove Programs*.
2. Click *Add/Remove Windows Components* from the left side.
3. Ensure that the following components are selected.
  - Certificate Services—After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select Yes to select certificate services and continue



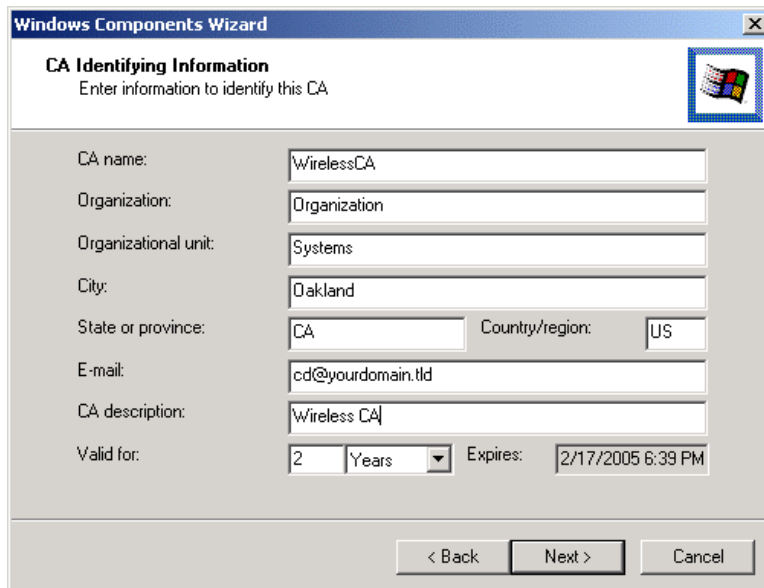
- World Wide Web Server—Select World Wide Web Server on the Internet Information Services (IIS) component.
- From the Networking Services category, select Dynamic Host Configuration Protocol (DHCP), and Internet Authentication Service (DNS should already be selected and installed).



4. Click **Next**.
5. Select Enterprise root CA and click **Next**.



6. Enter the information for the Certificate Authority and click **Next**.



The screenshot shows the 'Windows Components Wizard' window with the 'CA Identifying Information' tab selected. The window title is 'Windows Components Wizard' and the subtitle is 'CA Identifying Information'. Below the subtitle is the instruction 'Enter information to identify this CA'. The form contains the following fields and values:

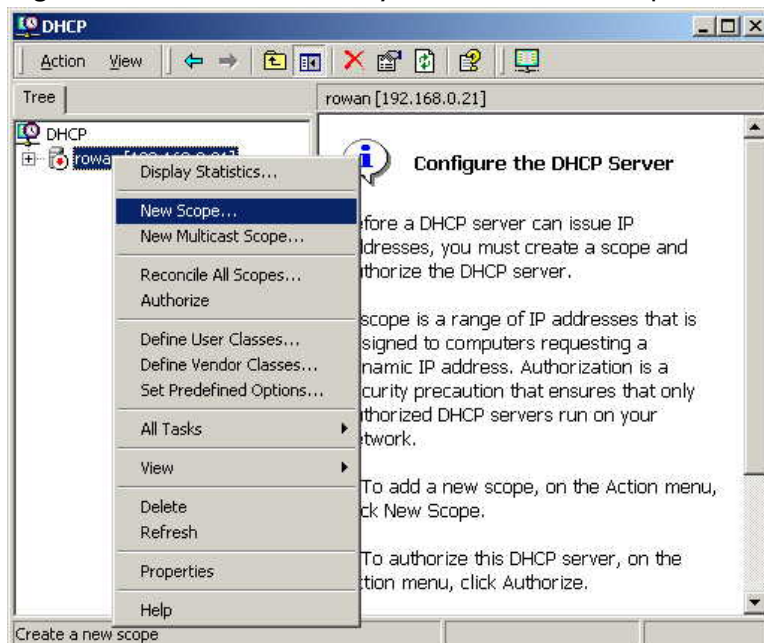
Field	Value
CA name:	WirelessCA
Organization:	Organization
Organizational unit:	Systems
City:	Oakland
State or province:	CA
Country/region:	US
E-mail:	cd@yourdomain.tld
CA description:	Wireless CA
Valid for:	2 Years
Expires:	2/17/2005 6:39 PM

At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Click **Next** if you don't want to change the CA's configuration data.
8. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click **OK**, then **Finish**.

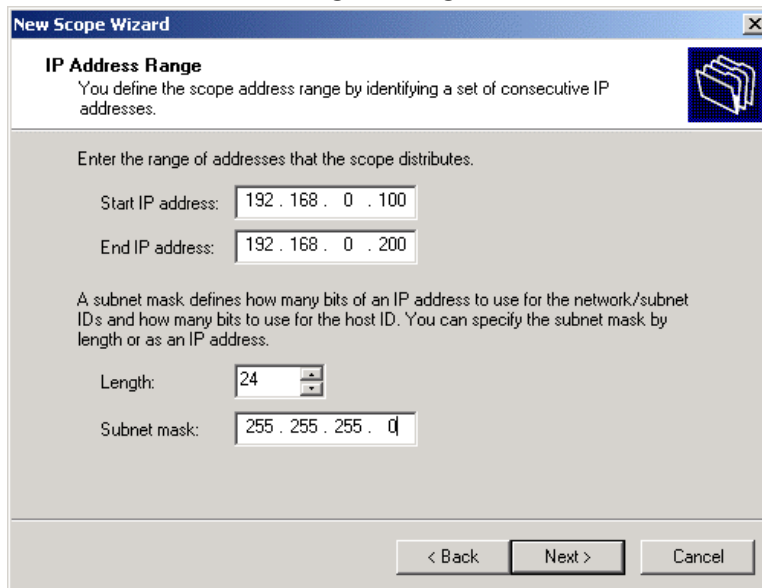
## DHCP server configuration

1. Click on *Start > Programs > Administrative Tools > DHCP*.
2. Right-click on the server entry and select **New Scope**.



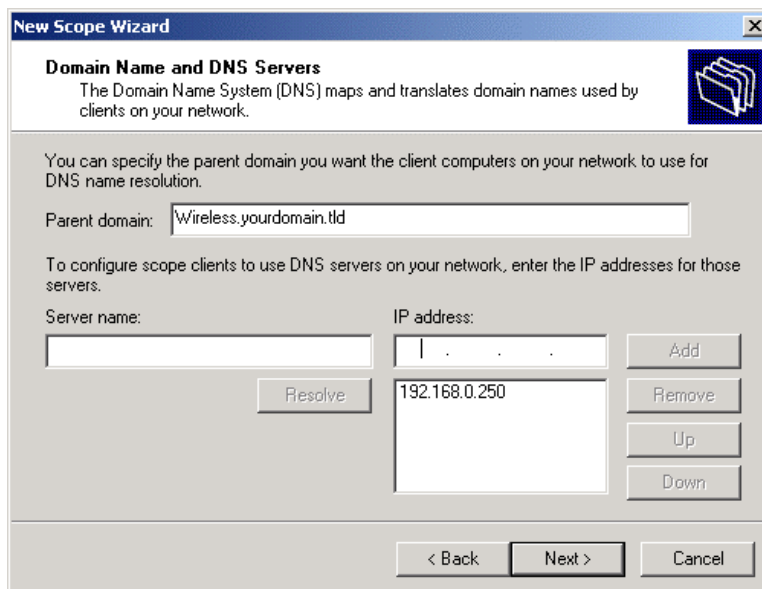
3. Click **Next** when the New Scope Wizard Begins.

4. Enter the name and description for the scope, click **Next**.
5. Define the IP address range. Change the subnet mask if necessary. Click **Next**.



The screenshot shows the 'New Scope Wizard' window, specifically the 'IP Address Range' step. The window title is 'New Scope Wizard'. The main heading is 'IP Address Range' with a subtext: 'You define the scope address range by identifying a set of consecutive IP addresses.' Below this, it says 'Enter the range of addresses that the scope distributes.' There are two text boxes: 'Start IP address:' with the value '192 . 168 . 0 . 100' and 'End IP address:' with the value '192 . 168 . 0 . 200'. Below these, it explains: 'A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.' There are two more text boxes: 'Length:' with a value of '24' and a small up/down arrow, and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click **Next**.
7. Change the Lease Duration time if preferred. Click **Next**.
8. Select Yes, I want to configure these options now, and click **Next**.
9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click **Next**.
10. For the parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address. Click **Next**.



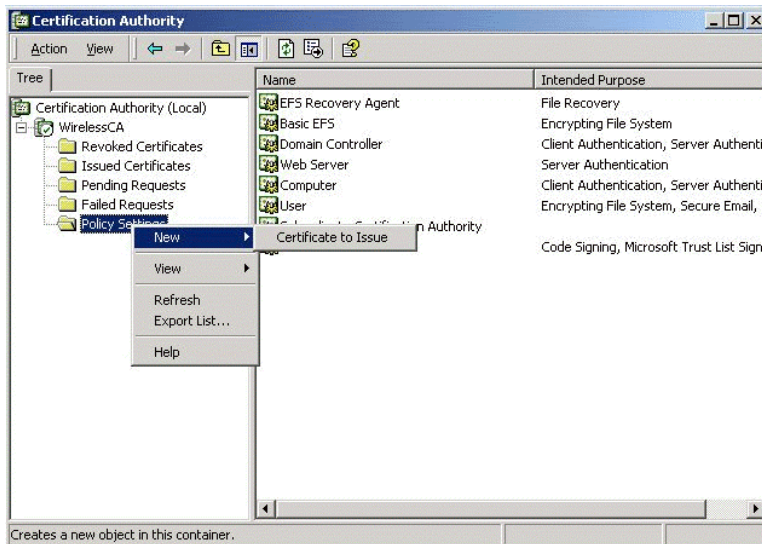
The screenshot shows the 'New Scope Wizard' window, specifically the 'Domain Name and DNS Servers' step. The window title is 'New Scope Wizard'. The main heading is 'Domain Name and DNS Servers' with a subtext: 'The Domain Name System (DNS) maps and translates domain names used by clients on your network.' Below this, it says 'You can specify the parent domain you want the client computers on your network to use for DNS name resolution.' There is a text box for 'Parent domain:' with the value 'Wireless.yourdomain.tld'. Below this, it says 'To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.' There are two columns: 'Server name:' and 'IP address:'. The 'Server name' column has an empty text box. The 'IP address' column has a text box with the value '192.168.0.250'. To the right of the 'IP address' column, there are four buttons: 'Add', 'Remove', 'Up', and 'Down'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

11. If you don't want a WINS server, just click **Next**.

12. Select Yes, I want to activate this scope now. Click **Next**, then **Finish**.
13. Right-click on the server and select Authorize. It may take a few minutes to complete.

## Certificate Authority Setup

1. Select *Start > Programs > Administrative Tools > Certification Authority*.
2. Right-click *Policy Settings* and select *New > Certificate to Issue*.

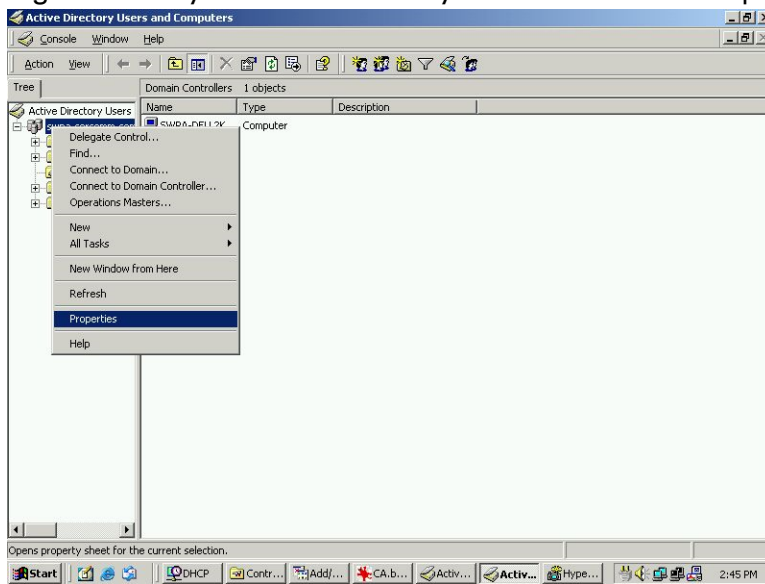


3. Select *Authenticated Session* and *Smartcard Logon* (select more than one by holding down the Ctrl key). Click **OK**.

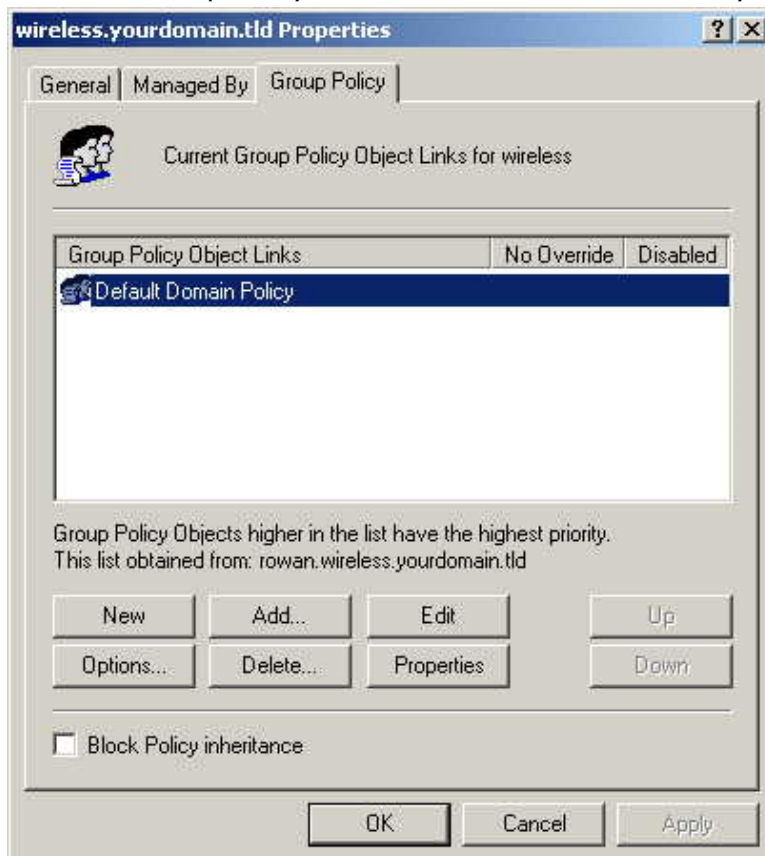


4. Select *Start > Programs > Administrative Tools > Active Directory Users and Computers*.

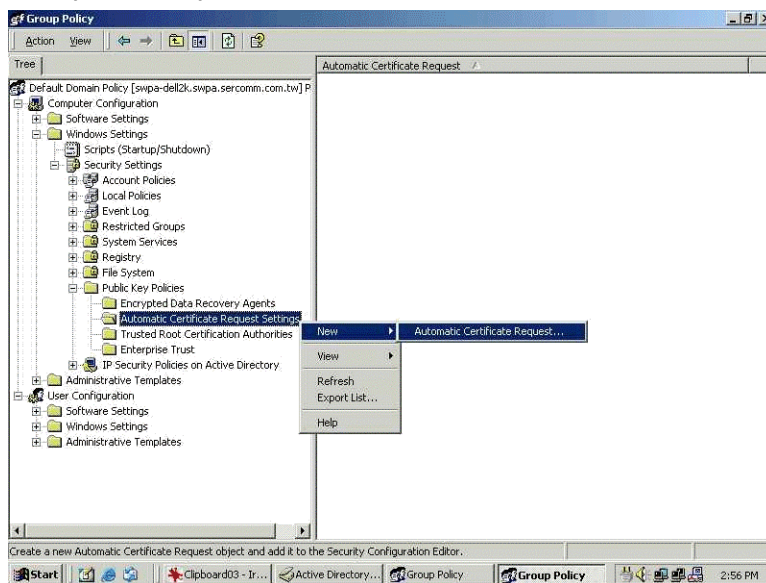
5. Right-click on your active directory domain and select Properties.



6. Select the Group Policy tab, choose Default Domain Policy then click **Edit**.



7. Select *Computer Configuration > Windows Settings > Security Settings > Public Key Policies*, right-click *Automatic Certificate Request Settings > New > Automatic Certificate Request*.



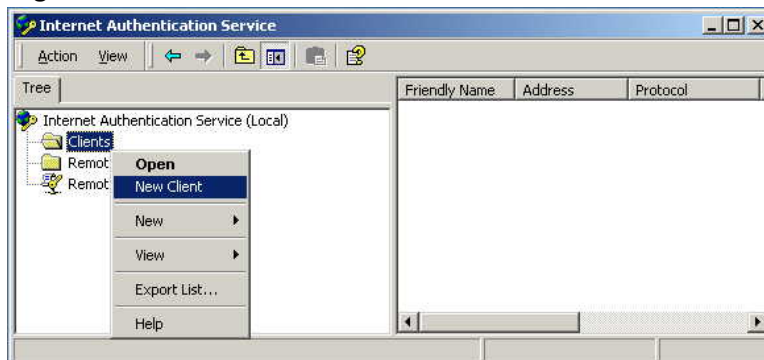
8. When the Certificate Request Wizard appears, click **Next**.
9. Select **Computer**, click **Next**.



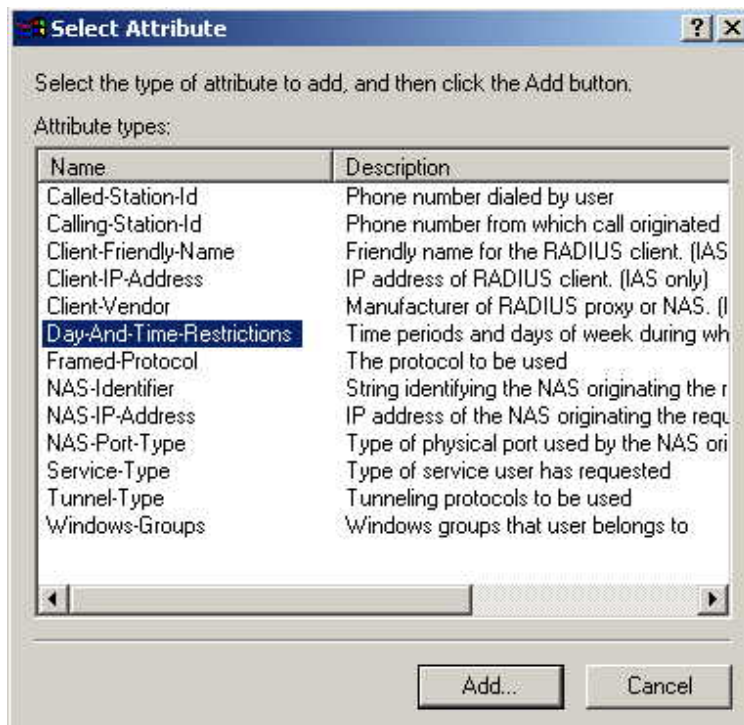
10. Ensure that your Certificate Authority is checked, click **Next**.
11. Review the policy change information and click **Finish**.
12. Click *Start > Run*, type "cmd" and press **Enter**. Enter "secdit /refreshpolicy machine\_policy". This command may take a few minutes to take effect.

## Internet Authentication Service (RADIUS) Setup

1. Select *Start > Programs > Administrative Tools > Internet Authentication Service*.
2. Right-click on *Clients* and select *New Client*.

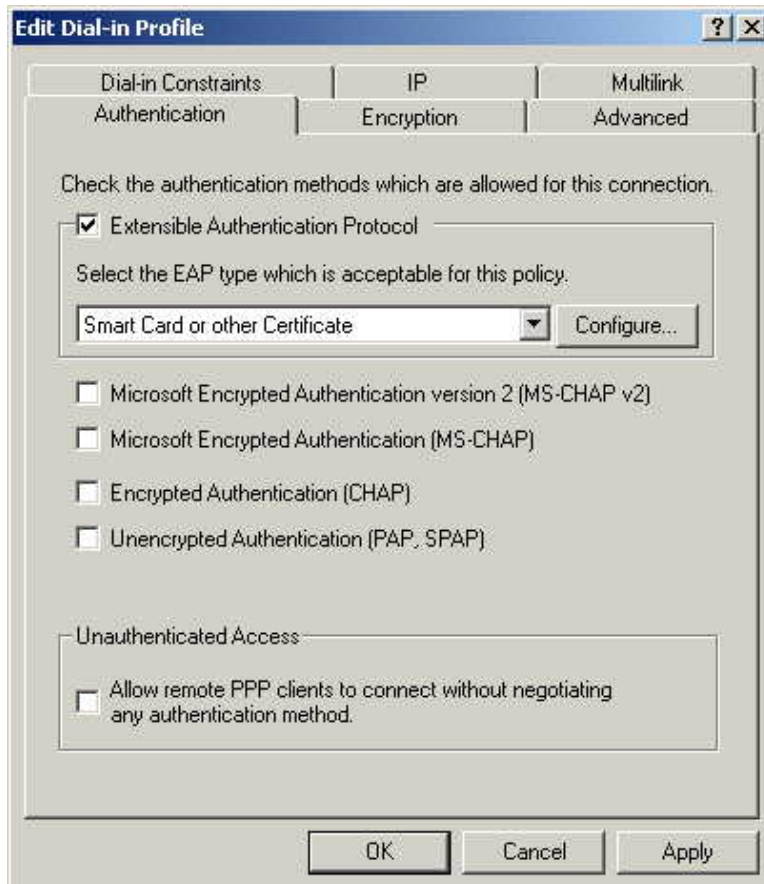


3. Enter a name for the access point, click **Next**.
4. Enter the address or name of the wireless access point, and set the shared secret, as entered on the Security Settings of the wireless access point.
5. Click **Finish**.
6. Right-click on *Remote Access Policies*, select *New Remote Access Policy*.
7. Assuming you are using EAP-TLS, name the policy "eap-tls", and click **Next**.
8. Click **Add...**  
If you don't want to set any restrictions and a condition is required, select *Day-And-Time-Restrictions*, and click **Add...**





9. Click **Permitted**, then **OK**. Select **Next**.
10. Select *Grant remote access permission*. Click **Next**.
11. Click **Edit Profile...** and select the Authentication tab. Enable Extensible Authentication Protocol and select Smart Card *or* other Certificate. Deselect other authentication methods listed. Click **OK**.

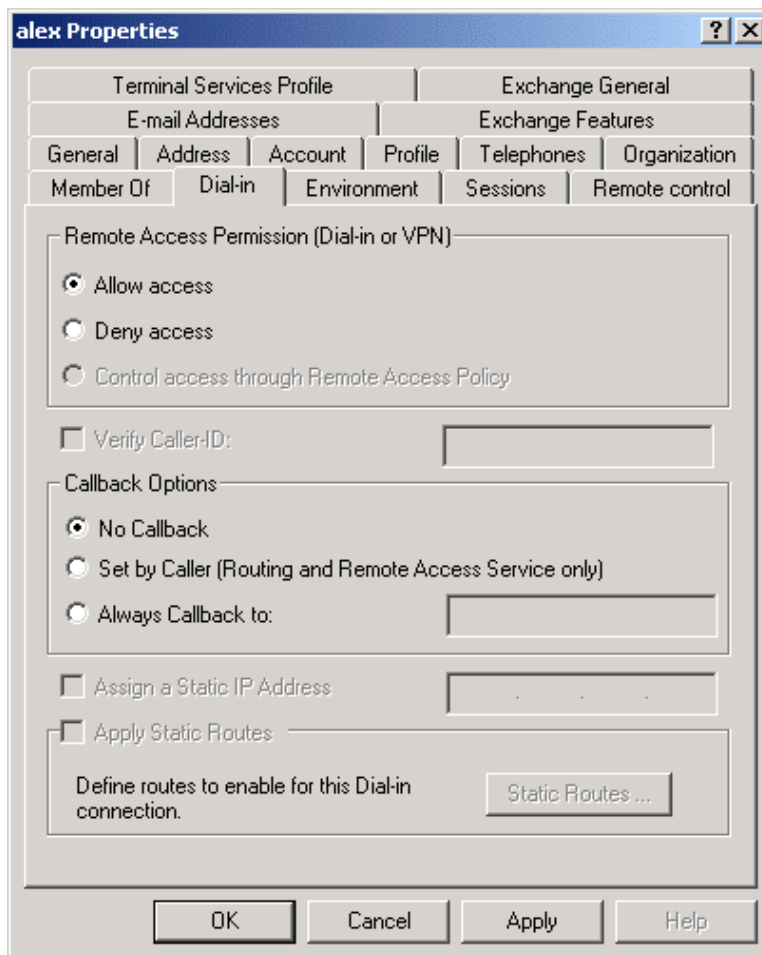


12. Select No if you don't want to view the help for EAP. Click Finish.



## Remote Access Login for Users

1. Select *Start > Programs > Administrative Tools > Active Directory Users and Computers*.
2. Double-click on the user who you want to enable.
3. Select the Dial-in tab and enable Allow access. Click **OK**.



## 802.1x Client Setup on Windows XP

Windows XP ships with a complete 802.1x client implementation. If using Windows 2000, you can install SP3 (Service Pack 3) to gain the same functionality.

If you don't have either of these systems, you must use the 802.1x client software provided with your wireless adapter. Refer to your vendor's documentation for setup instructions.

The following instructions assume:

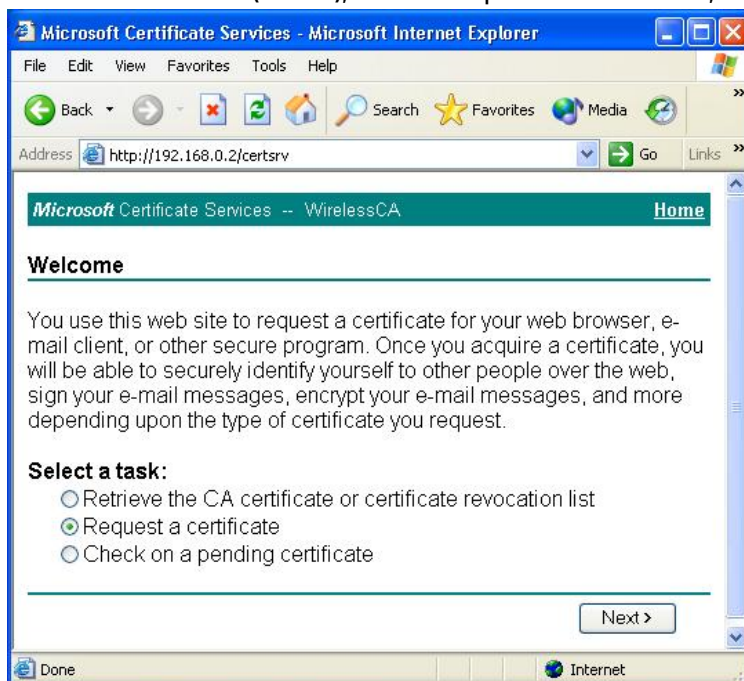
- You are using Windows XP.
- You are connecting to a Windows 2000 server for authentication.
- You already have a login (User name and password) on the Windows 2000 server.

## Client Certificate Setup

1. Connect to a network that doesn't require port authentication.
2. Start your Web browser. In the address box, enter the IP address of the Windows 2000 Server, followed by "/certsrv", e.g., "<http://192.168.0.2/certsrv>".
3. You will be prompted for a user name and password. Enter the User name and Password assigned to you by your network administrator and click **OK**.



4. On the first screen (below), select Request a certificate, click **Next**.



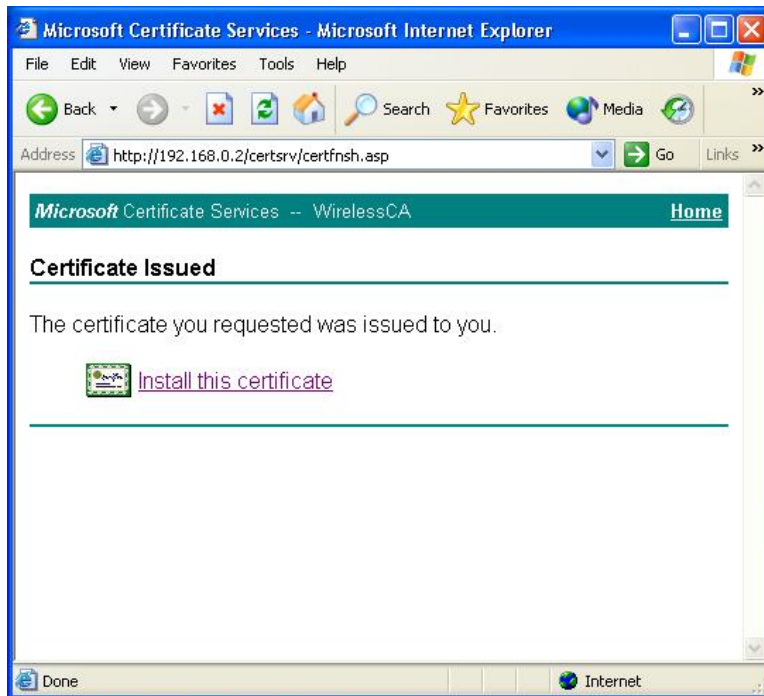
5. Select User certificate request and select User Certificate, click **Next**.

The screenshot shows a Microsoft Internet Explorer window titled "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar displays "http://192.168.0.2/certsrv/certrqus.asp". The page content includes a breadcrumb "Microsoft Certificate Services -- WirelessCA" and a "Home" link. The main heading is "Choose Request Type". Below it, the text says "Please select the type of request you would like to make:". There are two radio button options: "User certificate request:" (which is selected) and "Advanced request:". Under the selected option, there is a dropdown menu with "User Certificate" selected. At the bottom right of the form area is a "Next >" button. The status bar at the bottom shows "Done" and "Internet".

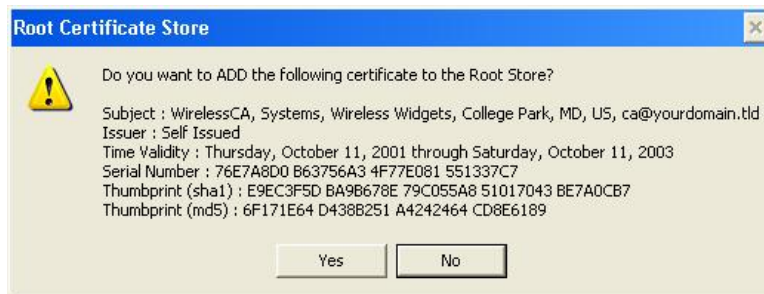
6. Click **Submit**.

The screenshot shows the same Microsoft Internet Explorer window, but the address bar now displays "http://192.168.0.2/certsrv/certrqbi.asp?type=0". The page content includes the same breadcrumb and "Home" link. The main heading is "User Certificate - Identifying Information". Below it, the text says "All the necessary identifying information has already been collected. You may now submit your request." There are two buttons: "More Options >>" and "Submit >". The status bar at the bottom shows "Done" and "Internet".

7. A message will be displayed, and the certificate will be returned to you.  
Click **Install this certificate**.



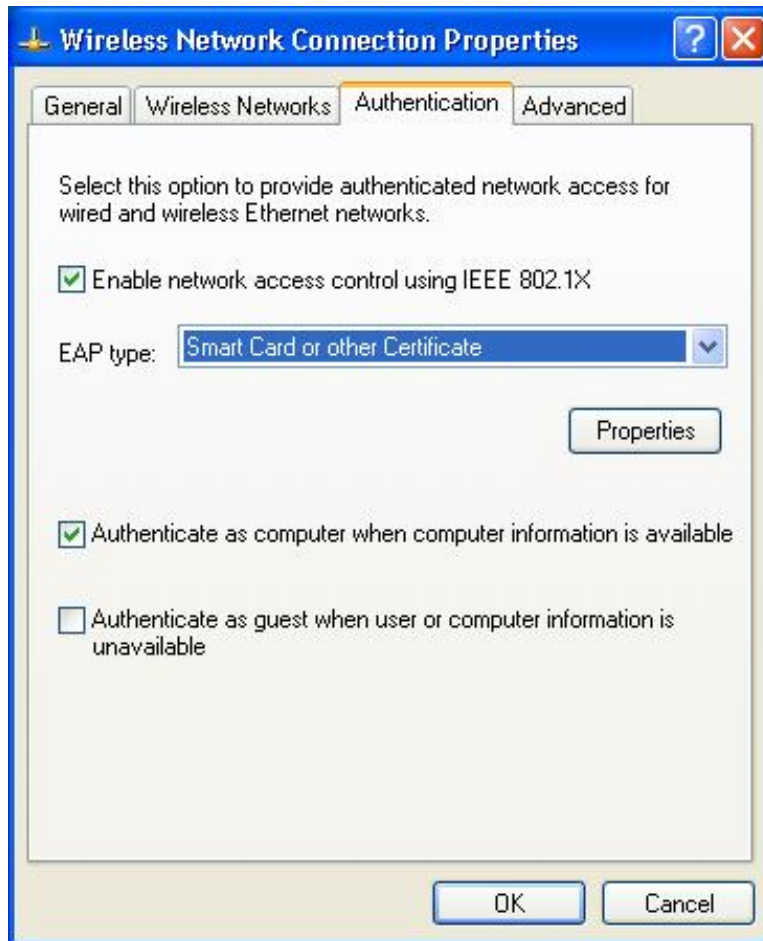
8. You will receive a confirmation message. Click **Yes**.



9. Certificate setup is now complete.

## 802.1x Authentication Setup

1. Select *Start > Control Panel > Network Connections*.
2. Right-click on the Wireless Network Connection and select Properties.
3. Select the Authentication tab and ensure that Enable network access control using IEEE 802.1X is selected, and Smart Card or other Certificate is selected from the EAP type.



## Encryption Settings

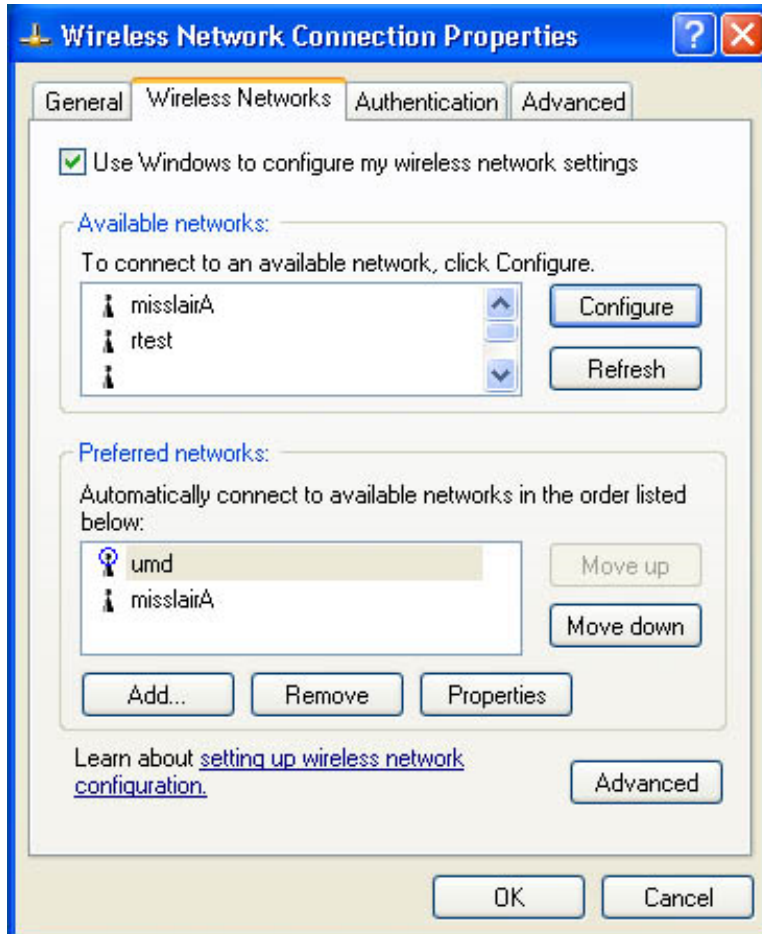
The encryption settings must match the access point on the wireless network you wish to join.

- Windows XP will detect any available wireless networks, and allow you to configure each network independently.
- Your network administrator can advise you of the correct settings for each network. 802.1x networks typically use EAP-TLS. This is a dynamic key system, so there is no need to enter key values.

## Enabling Encryption

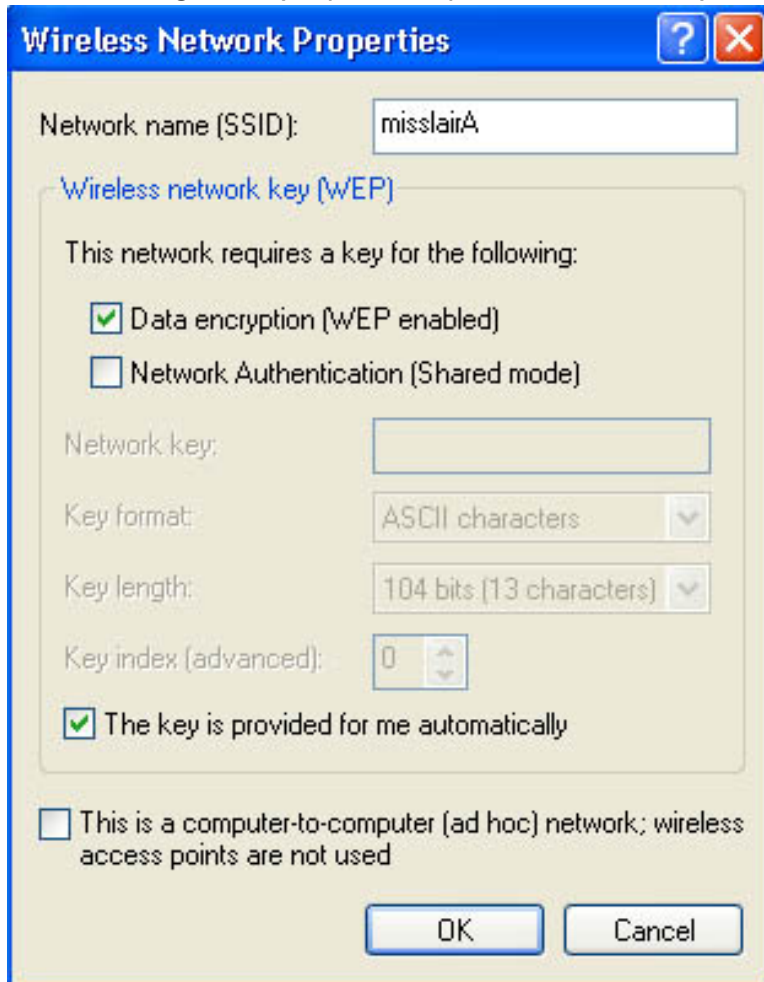
To enable encryption for a wireless network:

1. Click on the *Wireless Networks* tab.



2. Select the wireless network from the Available networks list and click **Configure**.

3. Select and enter the correct values, as advised by your Network Administrator.  
For example, to use EAP-TLS, you would enable Data encryption, and click the checkbox for the setting *The key is provided for me automatically*, as shown below.



The image shows a Windows XP 'Wireless Network Properties' dialog box. The title bar is blue with a question mark and a close button. The main area has a light beige background. At the top, 'Network name (SSID):' is followed by a text box containing 'misslairA'. Below this is a section titled 'Wireless network key (WEP)' in blue. Inside this section, it says 'This network requires a key for the following:'. There are two checkboxes: 'Data encryption (WEP enabled)' which is checked, and 'Network Authentication (Shared mode)' which is unchecked. Below these are four fields: 'Network key:' with an empty text box, 'Key format:' with a dropdown menu showing 'ASCII characters', 'Key length:' with a dropdown menu showing '104 bits (13 characters)', and 'Key index (advanced):' with a spinner box showing '0'. At the bottom of the WEP section is a checked checkbox 'The key is provided for me automatically'. Below the WEP section is an unchecked checkbox 'This is a computer-to-computer (ad hoc) network; wireless access points are not used'. At the very bottom are 'OK' and 'Cancel' buttons.

4. Setup for Windows XP and 802.1x client is now complete.

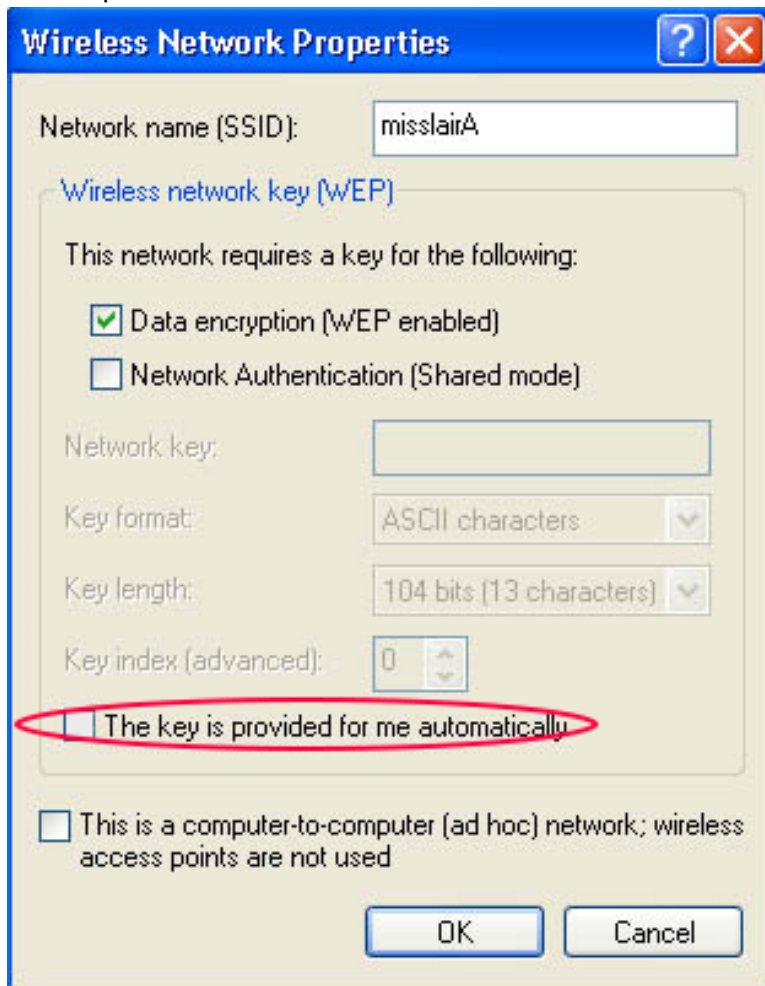
## Using 802.1x Mode (without WPA)

This is very similar to using WPA-Enterprise.

The only difference is that on your client, you must NOT enable the setting *The key is provided for me automatically*.



Instead, you must enter the WEP key manually, ensuring it matches the WEP key used on the access point.



The image shows a Windows XP-style dialog box titled "Wireless Network Properties". It has a blue title bar with a question mark icon and a red close button. The dialog is divided into sections. The first section is "Network name (SSID):" with a text box containing "misslairA". The second section is "Wireless network key (WEP)". It contains the text "This network requires a key for the following:" followed by two checkboxes: "Data encryption (WEP enabled)" which is checked, and "Network Authentication (Shared mode)" which is unchecked. Below these are four fields: "Network key:" (empty text box), "Key format:" (dropdown menu showing "ASCII characters"), "Key length:" (dropdown menu showing "104 bits (13 characters)"), and "Key index (advanced):" (spin box showing "0"). At the bottom of this section is a checkbox labeled "The key is provided for me automatically", which is unchecked and circled in red. Below this is another checkbox labeled "This is a computer-to-computer (ad hoc) network; wireless access points are not used", which is also unchecked. At the very bottom are "OK" and "Cancel" buttons.

**Note**—On some systems, the 64-bit WEP key is shown as 40-bit and the 128-bit WEP key is shown as 104-bit. This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

## Regulatory Approvals

### Federal Communication Commission Interference Statement

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.



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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

## **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.

***Note**—The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi products marketed in US must fixed to US operation channels only.*

## **Industry Canada statement**

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

## **Caution**

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

## **Avertissement**

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

## **Radiation Exposure Statement**

This equipment complies with IC 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.

## **Déclaration d'exposition aux radiations**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.