AirTies

Wireless life

User Manual

7/24 people support
0845 557 5782 (from United Kingdom)
+90 212 444 0239 (International)

Contents

AirTies Documentation

This manual has been prepared by AirTies Wireless Networks Corporation. All rights reserved.

Manual Overview

This manual guides you through the steps necessary for setting up and configuring your AirTies device. Please read this manual carefully before beginning the installation process.

The Warranty does not cover failure or damage as a result of not following the instructions in the manual. AirTies will not be held responsible in such circumstances.

The User Manual is an important resource you can refer to for safe and proper use of your device. Please retain it for future reference.

Safety and Maintenance

- In order to prevent damage to your device, be sure to keep it in its original box during transportation.
- The device must be used solely with its original power adapter. Please note that the adapter is 220V only. Do not use with 110V AC.
- Do not insert a PSTN (phone) plug into the LAN port.
- If you encounter any problems, do not open or disassemble the device. Call AirTies Technical Support.
- In order to prevent electric shock, do not operate the device in wet or damp areas.
- In the event of a gas leak, do not use the device. Do not turn the device on or off. Do not plug or unplug the power cord.
- Avoid using the device in dusty environments. If dust buildup should occur, use a dry cloth to remove the dust.
- To clean the exterior of the device use a dry cloth. Do not attempt to clean the interior. There are no user serviceable components inside.
- For information regarding the installation and configuration of the device consult the remainder of this manual.

Installation for Apple Users

AirTies Access Points

Unpack your device and plug in the cables according to the Quick Start Installation Guide.

Use either a network (Cat5) cable connected directly to your Apple Mac computer.

Open up the 'Network' panel in the Apple Mac's System Preferences and enter the following:

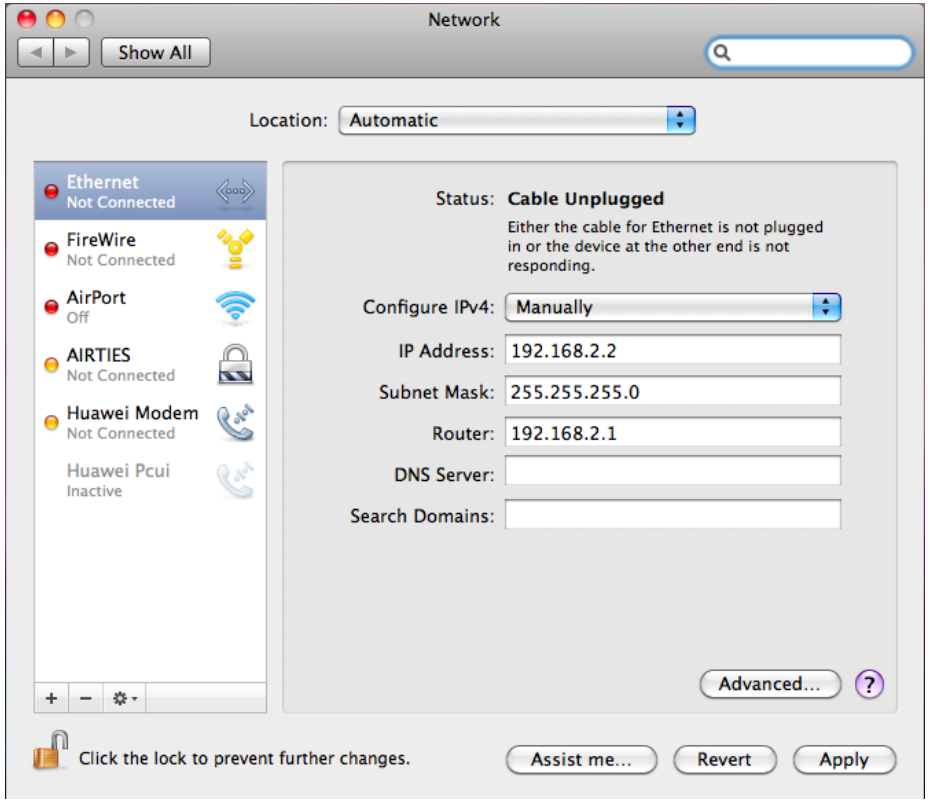
Configure IPv4: Manually

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Router: 192.168.2.1

Click Apply.



Location: Automatic

Status: **Cable Unplugged**

Either the cable for Ethernet is not plugged in or the device at the other end is not responding.

Configure IPv4: Manually

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Router: 192.168.2.1

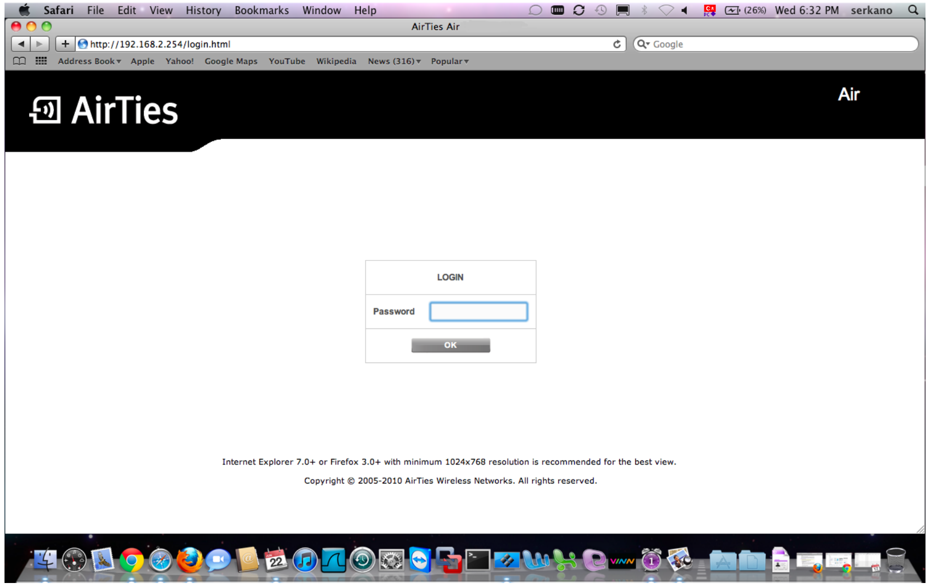
DNS Server:

Search Domains:

After applying the settings, open up the Apple Safari Web Browser and enter the following address in the address bar:

http://192.168.2.254

The AirTies Web User Interface (UI) will be displayed. You can log into the Web UI using a blank password. If you cannot connect to the device then reset the device by holding down the reset button on the back of the device for several seconds, until all the LEDs flash. Attempt to login again once the Access Point has restarted (due to the reset).

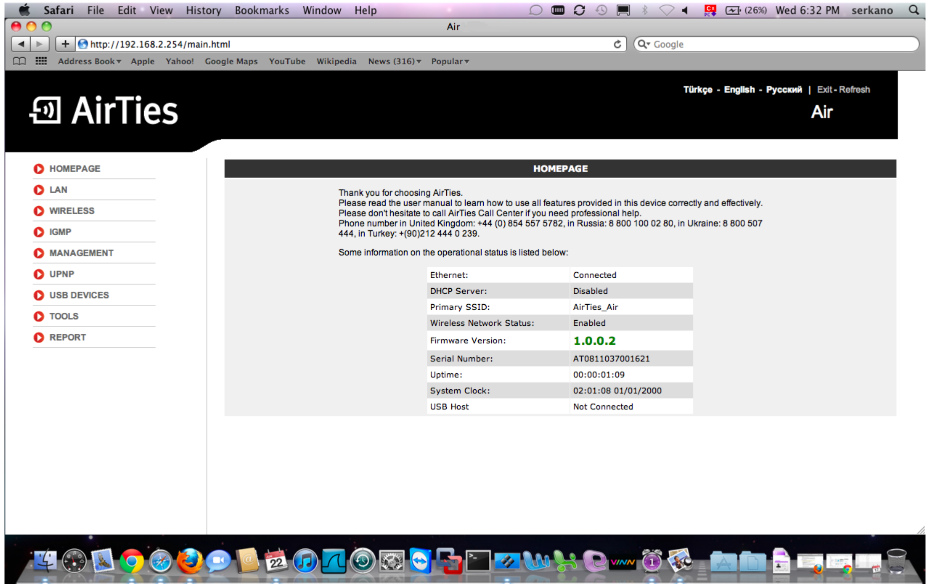

Safari File Edit View History Bookmarks Window Help
Wed 6:32 PM serkano
AirTies Air
Address Book Apple Yahoo! Google Maps YouTube Wikipedia News (316) Popular
AirTies
Air
LOGIN
Password
OK

http://192.168.2.254/login.html

Internet Explorer 7.0+ or Firefox 3.0+ with minimum 1024x768 resolution is recommended for the best view.

Copyright © 2005-2010 AirTies Wireless Networks. All rights reserved.

From the Web UI you can access all of the devices configuration options including wireless settings. For more detailed information about the Web UI please see the User Manual for the individual products.


Safari File Edit View History Bookmarks Window Help
(26%) Wed 6:32 PM serkano
Air
http://192.168.2.254/main.html
Google
Address Book Apple Yahoo! Google Maps YouTube Wikipedia News (316) Popular
AirTies
Türkçe - English - Русский | Exit - Refresh
Air
HOMEPAGE
LAN
WIRELESS
IGMP
MANAGEMENT
UPNP
USB DEVICES
TOOLS
REPORT

HOMEPAGE

Thank you for choosing AirTies.
Please read the user manual to learn how to use all features provided in this device correctly and effectively.
Please don't hesitate to call AirTies Call Center if you need professional help.
Phone number in United Kingdom: +44 (0) 854 557 5782, in Russia: 8 800 100 02 80, in Ukraine: 8 800 507 444, in Turkey: +(90)212 444 0 239.

Some information on the operational status is listed below:

Ethernet:	Connected
DHCP Server:	Disabled
Primary SSID:	AirTies_Air
Wireless Network Status:	Enabled
Firmware Version:	1.0.0.2
Serial Number:	AT0811037001621
Uptime:	00:00:01:09
System Clock:	02:01:08 01/01/2000
USB Host	Not Connected

Note: You are strongly recommended to add a password to the wireless network to stop intruders accessing your Local Area Network.

AirTies Network Assistant

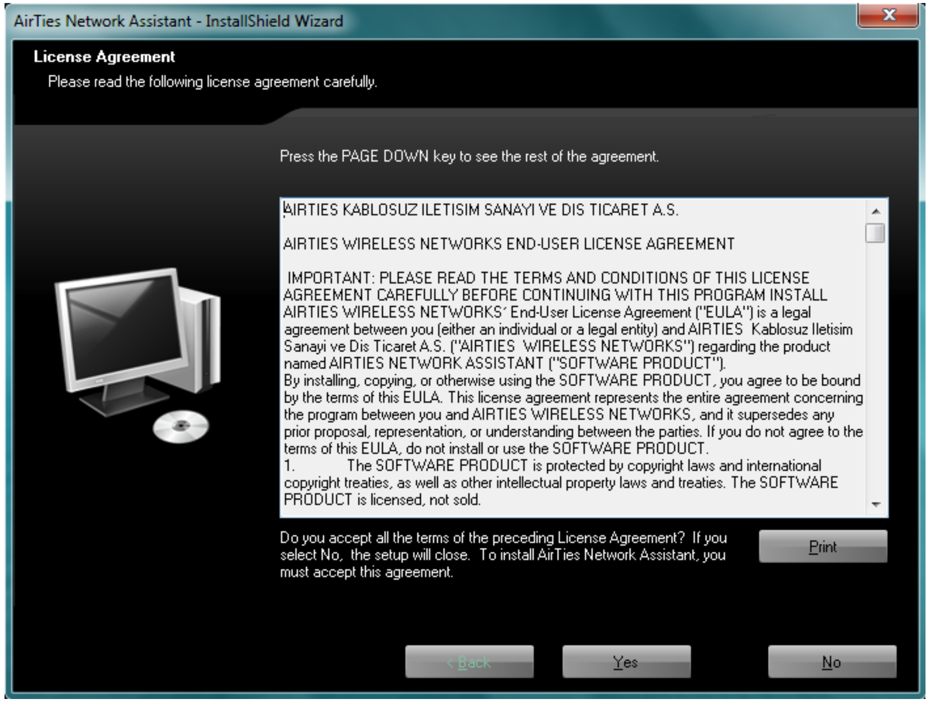
AirTies Network Assistant is an application that will setup and configure, monitor and manage home networks. It has been specifically designed to enable non technical users to perform tasks that are important to effectively managing the home network. Your AirTies product will be provided with a CD that contains the AirTies Network Assistant application. Alternatively you can download the latest version from www.airties.com. AirTies Network Assistant can be installed on as many PCs as you would like and can also be used to monitor networks that do not contain AirTies devices, although many key features will be missing because they require AirTies devices.

Minimum System Requirements

Any of Windows XP SP2 or greater, Windows Vista and Windows 7 operating systems installed on the PC. AirTies Network Assistant runs when Windows starts up and continues to monitor the network for any changes or problems. If problems are discovered then troubleshooting will fix the problems.

Installation

During AirTies Network Assistant installation your AirTies device will be setup and configured. Insert the CD that came with your AirTies device into the CD ROM drive of your PC, after a few seconds the animation will run. Select the product category and product that you want to configure from the menu. After selecting your product's name an animation shows your box contents. Ensure that the box contains everything shown in the animation and then click the "Next" button. Follow the animation showing how to configure the cabling of the product. Ensure that you follow the cabling for your product according to the animation. After the cabling animation has completed AirTies Network Assistant is installed. Setup application will display terms of End User Agreement. If you have a printer connected to your computer, you can print terms of use agreement clicking "Print" button. Click "Yes" button to pass next step or click "No" button to end your installation.



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

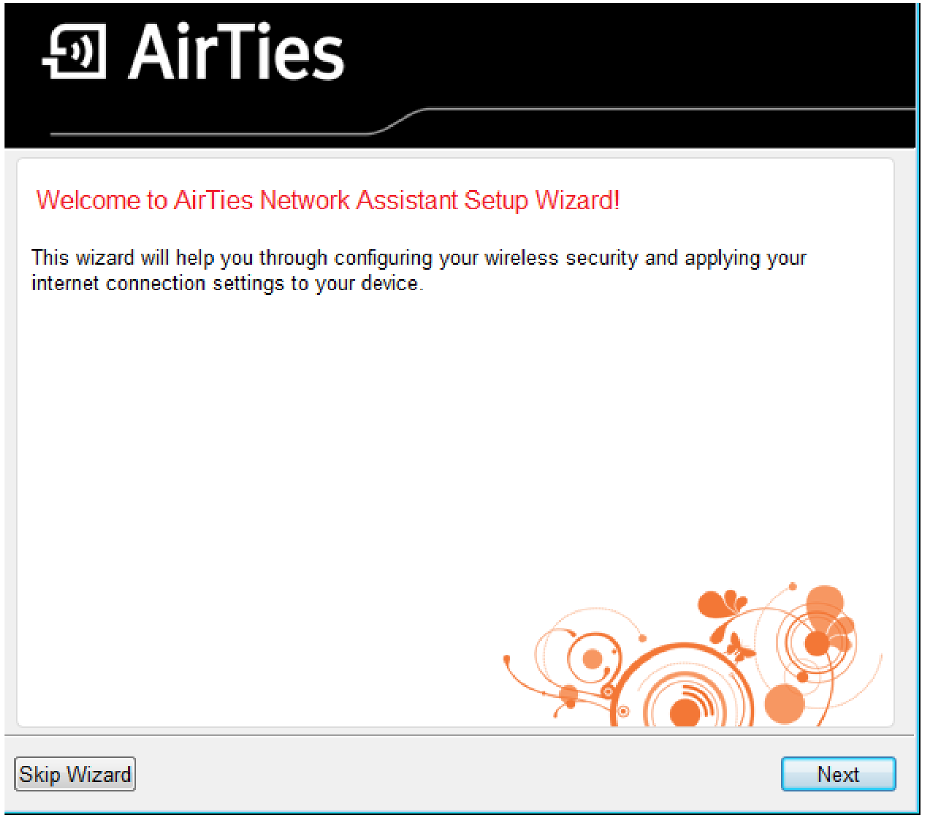
AIRTIES KABLOSUZ ILETISIM SANAYI VE DIS TICARET A.S.

AIRTIES WIRELESS NETWORKS END-USER LICENSE AGREEMENT

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL AIRTIES WIRELESS NETWORKS´ End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a legal entity) and AIRTIES Kablosuz Iletisim Sanayi ve Dis Ticaret A.S. ("AIRTIES WIRELESS NETWORKS") regarding the product named AIRTIES NETWORK ASSISTANT ("SOFTWARE PRODUCT").
By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the program between you and AIRTIES WIRELESS NETWORKS, and it supersedes any prior proposal, representation, or understanding between the parties. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.
1. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install AirTies Network Assistant, you must accept this agreement.

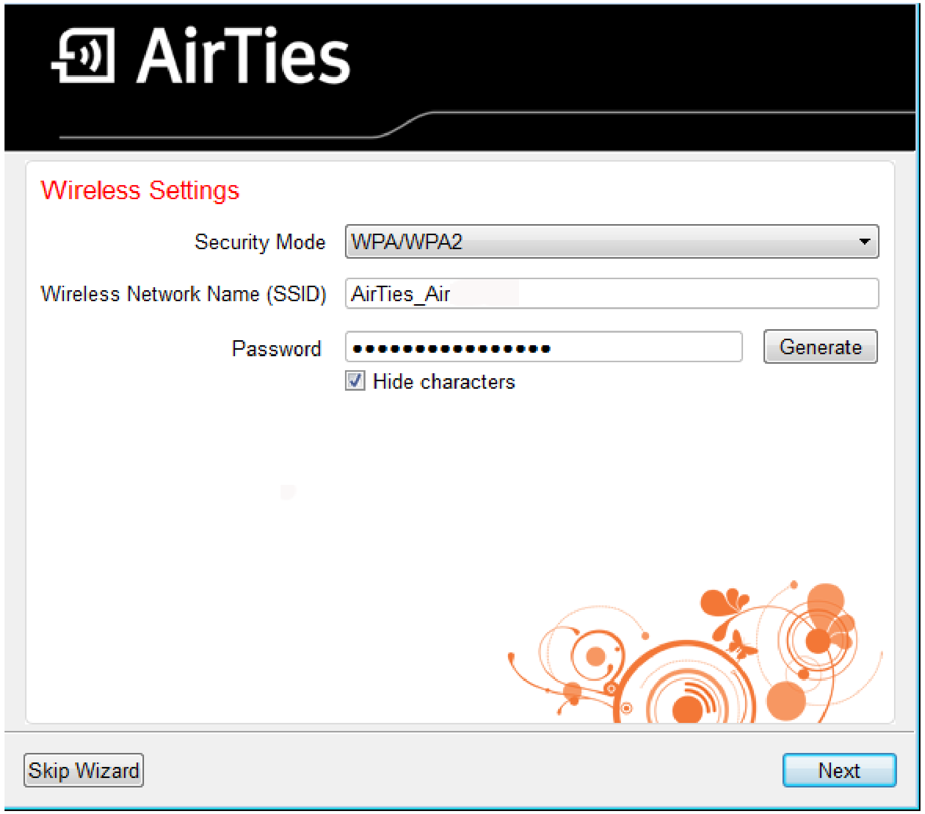
Once AirTies Network Assistant has completed installation, AirTies Network Assistant Setup Wizard will run.



Welcome to AirTies Network Assistant Setup Wizard!

This wizard will help you through configuring your wireless security and applying your internet connection settings to your device.

If your device and PC supports AirTouch/WPS then you will be prompted to press the button on your device to initialise AirTouch. Press the AirTouch button on your AirTies device and click the AirTouch button. A secure connection will be initialised between the AirTies device and PC running AirTies Network Assistant, which includes an automatically generated wireless key. Once the wireless connection has been created and device has been configured the wireless security key is displayed. Copy this if you want to share the connection with other non Windows 7 devices. If your AirTies device does not support AirTouch then you will be prompted to configure the wireless security manually for your device. Select WPA/WPA2 as the Security Mode. This is the highest level of security that you can configure. Enter a Wireless Network Name (SSID). This is the name that appears when you search for wireless networks from a PC. Enter a password for the wireless network. This should be at least eight characters long. You can see the characters by unchecking Hide characters. Click "Next" for saving your sets and passing next step.



Wireless Settings

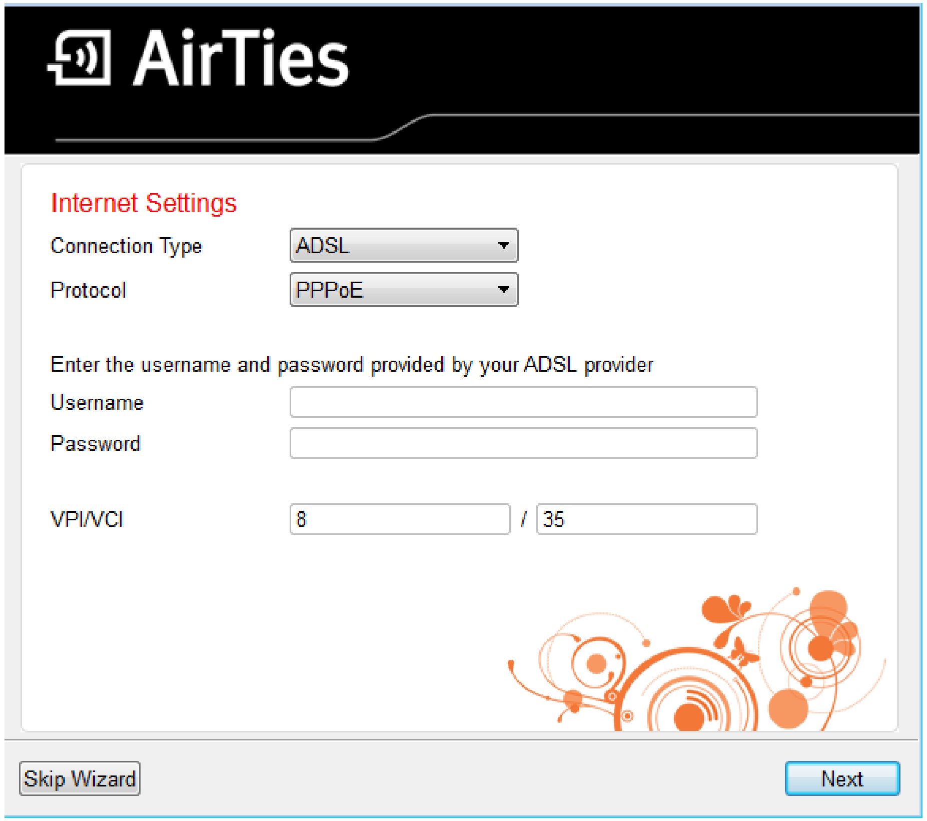
Security Mode: WPA/WPA2

Wireless Network Name (SSID): AirTies_Air

Password: ••••••••••••••••

☑ Hide characters

A screen will appear to say that the wireless network settings have been configured. Click "Next" button. Now you will be presented with configuration options for your Internet connection. These settings will be based on settings received from your Internet Service Provider (ISP). If you want to connect with ADSL connection, click "ADSL", if you want to connect using WAN Ethernet, click "Ethernet" option or if you want to 3G connection, click "3G" option as your Internet connection type that your device supports. If you experience any problems connecting to the Internet then it is recommended to contact you Internet Service Provider.



Internet Settings

Connection Type: ADSL

Protocol: PPPoE

Enter the username and password provided by your ADSL provider

Username:

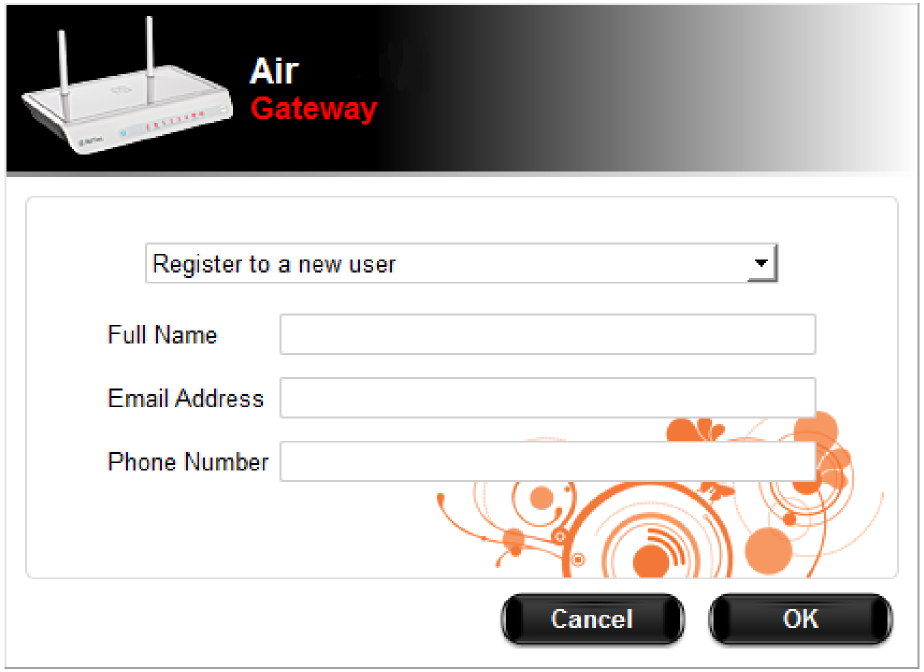
Password:

VPI/VCI: 8 / 35

The following settings should be configured if your device supports features.

- **For ADSL** you need to enter your username and password supplied from your ISP.
- **For Ethernet** you need to choose a protocol and enter username and password supplied by your ISP if needed.
- **For 3G** you need to enter the PIN from your 3G SIM card.

Click "Next" to save the Internet connection settings. The screen appears that indicates AirTies Network Assistant application has been installed successfully. If you want to save your device to AirTies database and take advantages of AirTies services, fill in the relevant sections.



Register to a new user

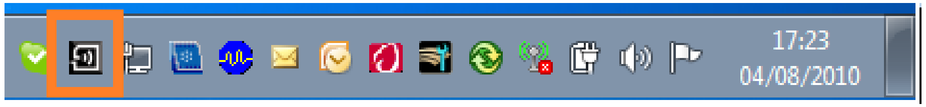
Full Name

Email Address

Phone Number

Running AirTies Network Assistant

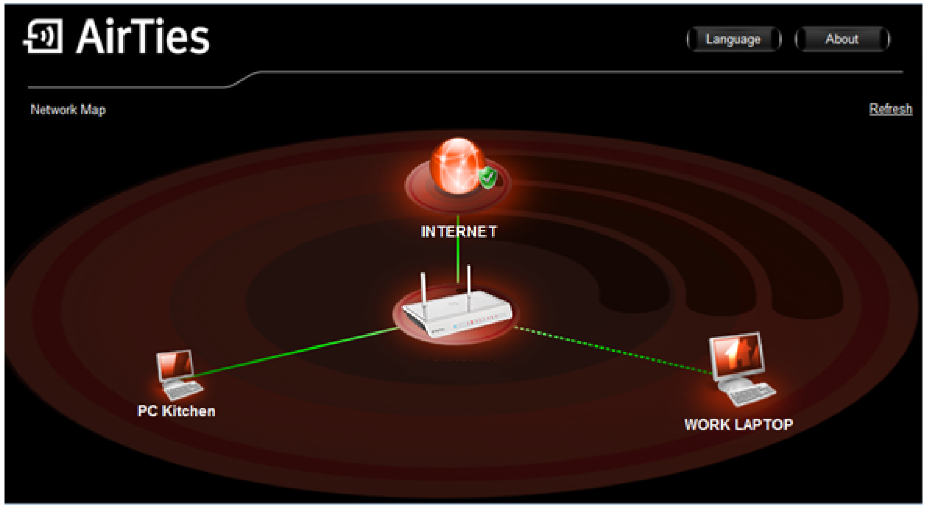
The AirTies Network Assistant application will always run in the background and can be accessed by clicking the AirTies logo in the notification area (bottom right corner, next to the clock). AirTies Network Assistant starts every time the PC starts, allowing for the network to be continually monitored.



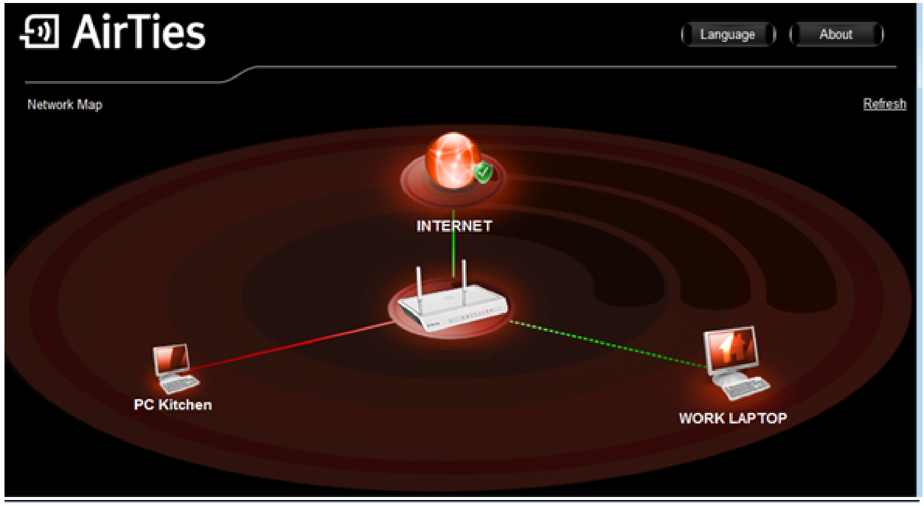
If you want to exit AirTies Network Assistant then you must right click the AirTies logo in the notification area and select "exit". If AirTies Network Assistant is not running and you want to run it then you must select the AirTies Network Assistant application from the start menu under All Programs > AirTies Wireless Networks > AirTies Network Assistant.

Network Display

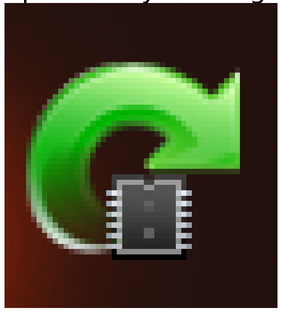
The network display is the central component of AirTies Network Assistant. Here all devices on the network are displayed with information about each device, status of network connection and problems with the network. Once AirTies Network Assistant has been installed and the connection between your PC and your AirTies device has been configured then the network display will be shown to the user. For normal usage when AirTies Network Assistant starts the network display will be shown.



You can change application language by clicking "Language" icon on the top right corner of AirTies Network Assistant application and you can be informed by clicking "About" icon. Your router is the device that has a connection to the Internet. It is the device that connects the home network to the Internet and is usually a gateway device such as an ADSL modem. There should only be one routing device on your network and this device is placed in the middle of the AirTies Network Assistant network display. From the router the Internet and local network device are connected. A green line indicates that a device is connected. A red line indicates that a device is not connected. As new devices are added to the network they will appear on AirTies Network Assistant. If a device is removed from the network then it will disappear from the network GUI after it has been disconnected for four hours. Dotted lines indicate a wireless connection and non dotted lines indicate a cable connection. A red cross on the line indicates that there is a problem. Clicking this will launch the trouble shooter application, which will identify the problem and attempt to solve it.



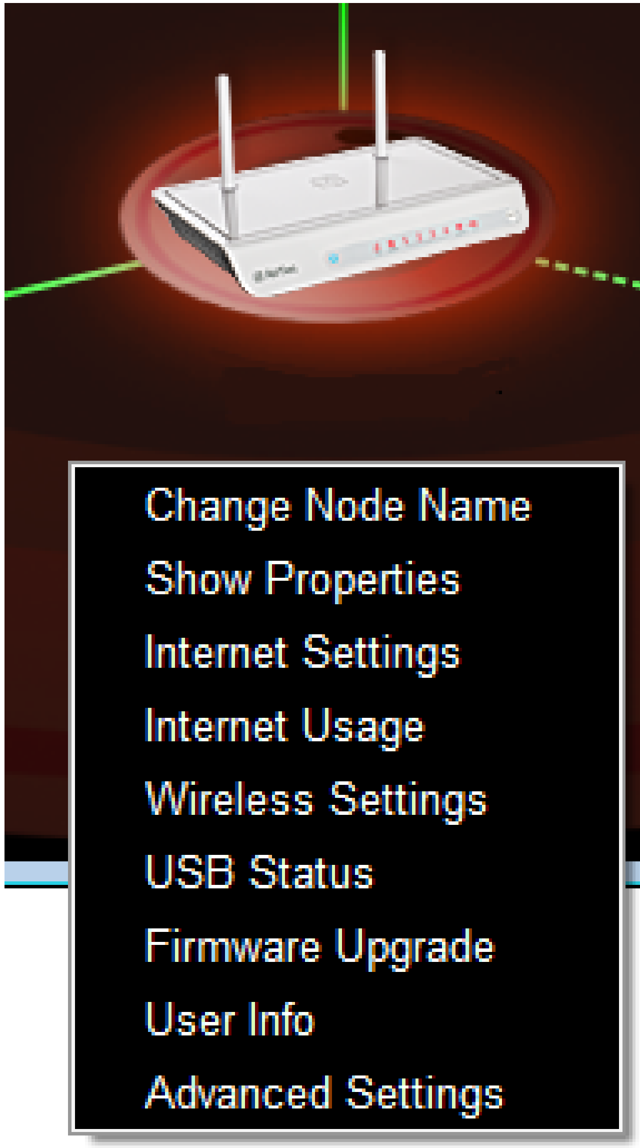
The network map should be updated automatically as new devices are added to the network. However, if the network map is not accurate then a manual refresh can run by clicking the refresh button on the top right of the screen. Each AirTies product will be displayed with their image on the network map. Non AirTies devices will be displayed with a generic image. It is not possible to manage non AirTies devices but the device can still be displayed on AirTies Network Assistant. If you see the following icon on the network map next to an AirTies product then the software on the device can be updated by clicking the icon.



Any devices that are present on your network map but you are not aware of should be investigated. Enabling wireless security or changing existing wireless security (see below) will ensure that intruders cannot continue to access your network.

Settings

Clicking an AirTies device allows for configuration to be updated.

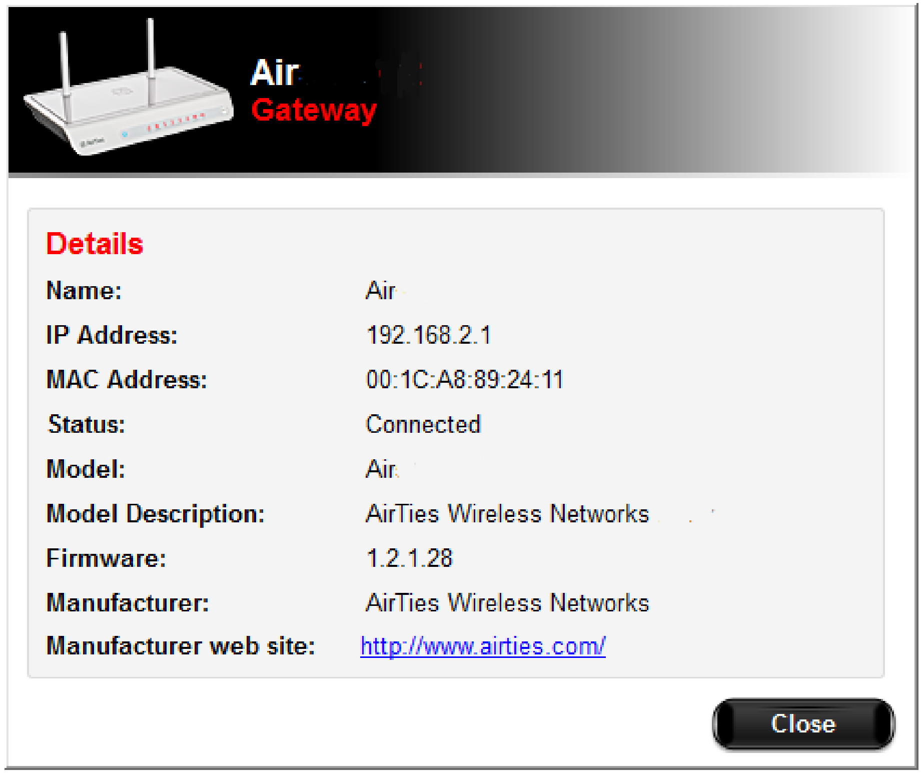


Change Node Name

Each device has a name, which is either the host name or the IP address. The node name can be updated to make it easier to keep track of devices on the network. For example, a games console may show on the network map as an IP address like 192.168.2.55 but can be renamed to be "games console 1".

Show Properties

The properties can be displayed for each device. Properties for AirTies devices are displayed: Properties for local computer running AirTies Network Assistant are displayed:

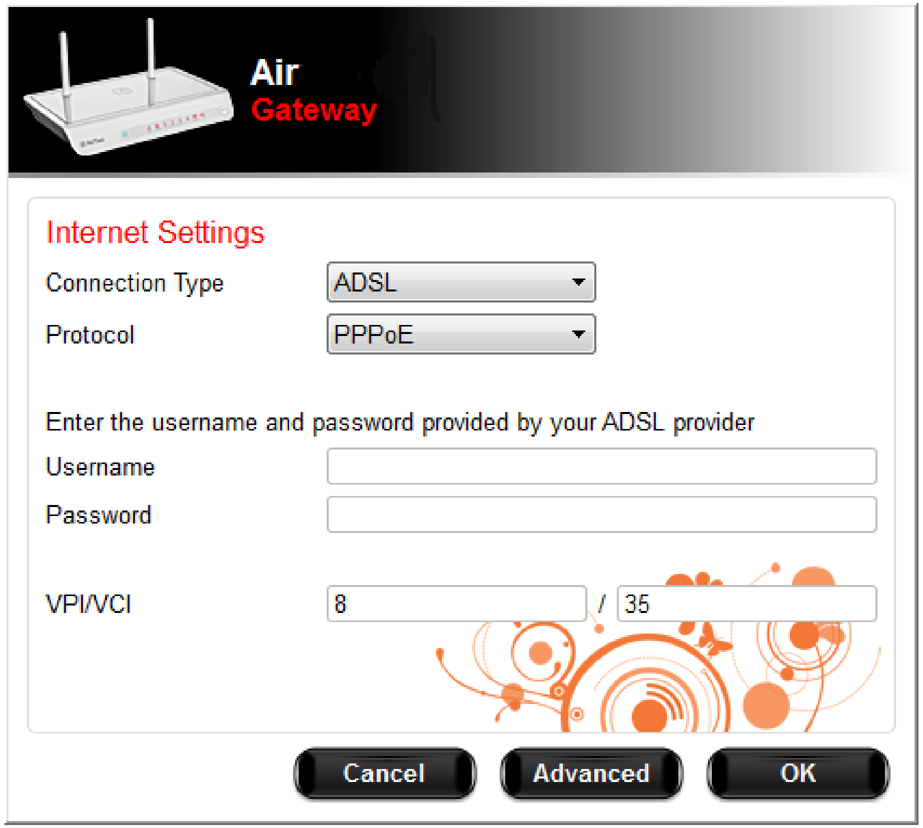


Details

Name:	Air
IP Address:	192.168.2.1
MAC Address:	00:1C:A8:89:24:11
Status:	Connected
Model:	Air
Model Description:	AirTies Wireless Networks
Firmware:	1.2.1.28
Manufacturer:	AirTies Wireless Networks
Manufacturer web site:	http://www.airties.com/

Internet Settings

The Internet settings for the AirTies device can be configured. The connection type can be selected from either ADSL or Ethernet. For ADSL connections the username and password that is supplied from your Internet Service Provider (ISP) is entered with VPI/VCI settings if they are not the default for your country. For Ethernet connections the protocol is defined and username and password are configured if PPPoE is defined.



Internet Settings

Connection Type: ADSL

Protocol: PPPoE

Enter the username and password provided by your ADSL provider

Username:

Password:

VPI/VCI: 8 / 35

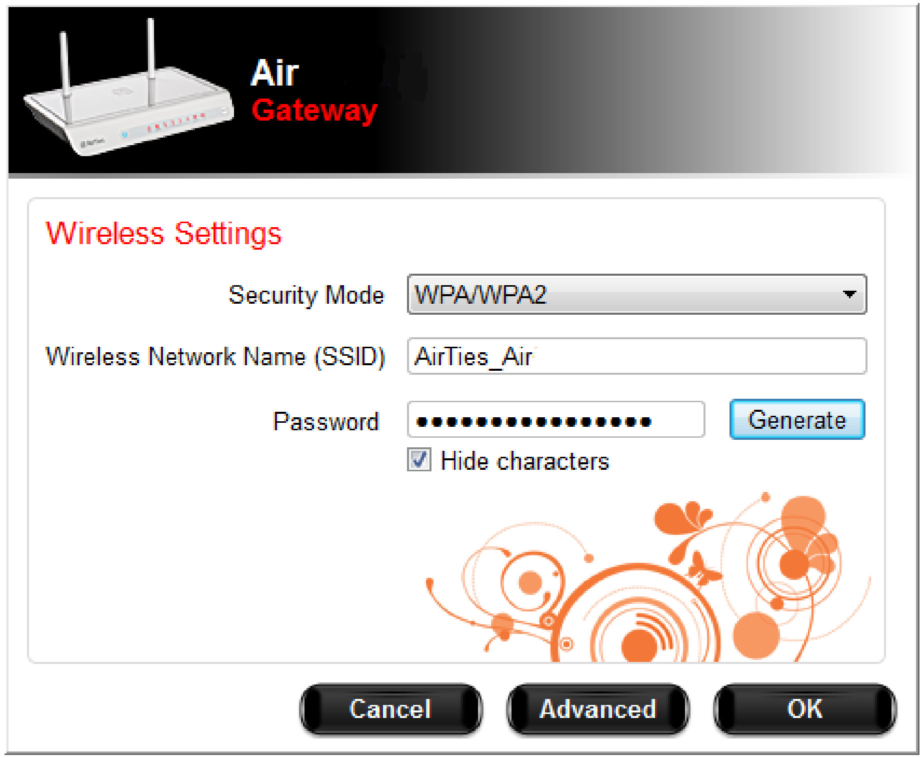
Click OK to save your settings. Click Advanced to show all Internet settings. Click Cancel to cancel any changes made and return to the network map.

Internet Usage

The amount of data that is sent and received from and to the Internet is counted and stored on the gateway device. This allows for users to monitor how much data they are using, which is useful when they have an account with their ISP which limits the amount of data that they can download and upload. To see the download and upload data in real time click Real-Time.

Wireless Settings

The wireless settings of the device can be changed: The security mode can be changed to either "None" or "WPA/WPA2". The Wireless Network Name (SSID) can be changed. This is the name that appears when you search for wireless networks from a PC. The password used to connect to the wireless network can be changed. This should be at least eight characters long. You can see the characters by unchecking Hide characters.



Wireless Settings

Security Mode: WPA/WPA2

Wireless Network Name (SSID): AirTies_Air

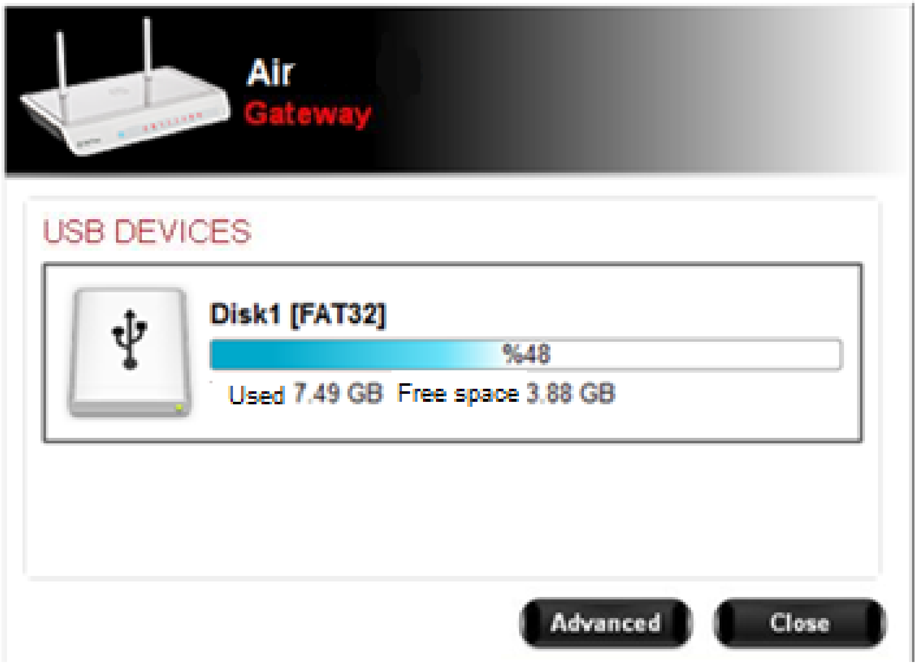
Password: ●●●●●●●●●●●●●●●●

☑ Hide characters

Click "OK" to save your settings. Click "Advanced" to show all Internet settings. Click "Cancel" to cancel any changes made and return to the network map. Note that for devices that are connected via MESH changes made to the gateway will be propagated to all devices connected via MESH.

USB Status (If your device has USB Host)

USB status shows whether a printer or USB disk is inserted into the device. For disks the amount of free disk space is displayed:



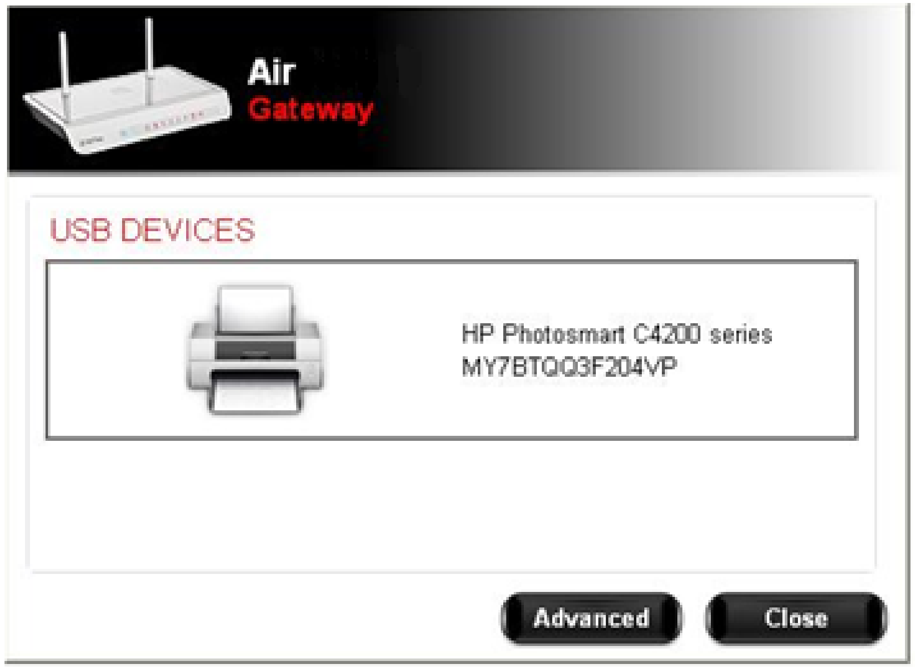
USB DEVICES

Disk1 [FAT32]

%48

Used 7.49 GB Free space 3.88 GB

For printers the printer model is displayed:



USB DEVICES

HP Photosmart C4200 series
MY7BTQQ3F204VP

Firmware Upgrade

AirTies Network Assistant will automatically check for new firmware updates for devices. If new firmware is available then an icon will be displayed on the device to let the user know that there is new firmware available. Clicking on the icon will perform a firmware upgrade on the device.

A manual update can also be made by selecting "Firmware Upgrade". A check will be made for new firmware: If no firmware was found then the user will be informed: If new firmware is discovered then the firmware on the device will be updated.

Software Upgrade

For the local PC there is a software upgrade option instead of firmware upgrade. This will check for any newer versions of AirTies Network Assistant and update if the user requests.

User Info

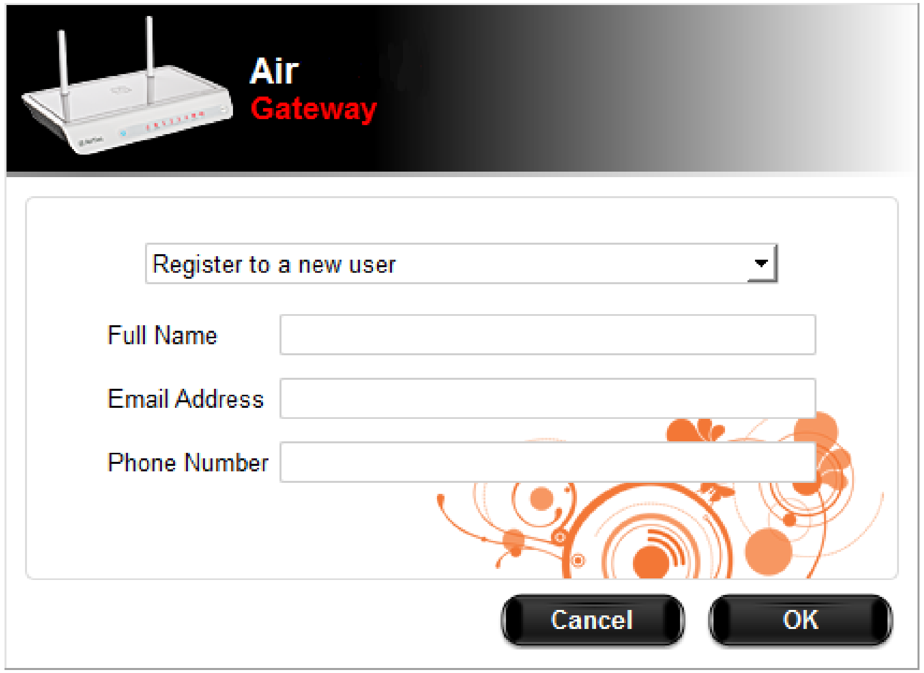
Registering a device provides AirTies with useful information that we use to help the customer with if they have a problem and also use to help us improve our products and customer experience. Each AirTies device on the home network can be registered with AirTies. If a user does not want to register then they can select 'Do not register' from the drop down box. Click "OK" to save your settings. Click "Cancel" to cancel any changes made and return to the network map.

Advanced Settings

Advanced settings open the devices' Web configuration page and allow for all other settings to be updated by the user (see settings below).

Adding AirTies Devices

When another device is added to the network then it will be displayed in the network map. If the new device is an AirTies device then the user s prompted to register the device.



Register to a new user

Full Name

Email Address

Phone Number

The user can choose not to register the device, register as a new user or use an existing user's details that already have devices registered to them on the network. Clicking "OK" registers the new device. Clicking "Cancel" closes the prompt.

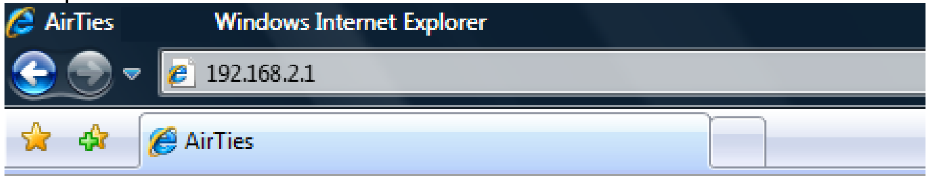
Advanced Settings

You can set the basic settings of the device, which are ADSL and wireless settings, with the Easy Installation CD. The easy installation CD allows for quick and easy installation when you first setup your device. There is also a web interface to the device that allows for basic and advanced settings to be configured. You do not need to be connected to the Internet to access the device's Web UI. To connect to the device follow these steps:

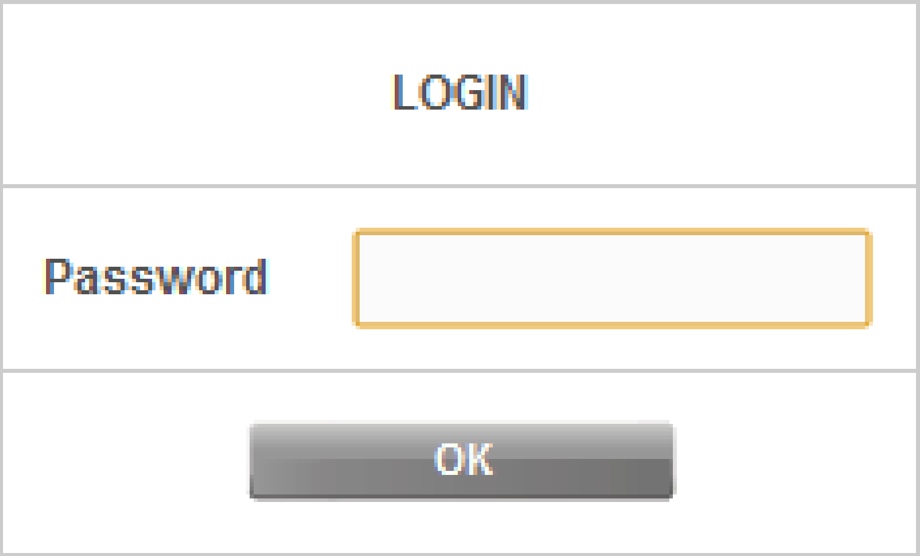
For Gateway Devices the IP address will be 192.168.2.1

1- Run a Web browser program on your computer (Internet Explorer, Mozilla Firefox etc.).

2- In the Web Browser's "Address" field, write the address 192.168.2.1 which is the default web interface address of device and press "Enter"



3- The "Welcome" screen of the Web Interface will appear. On the screen you will see a dialog box asking for the password to be entered. By default there is no login password for your device. Leave the password fiend empty and click OK.



For Access Points the default IP address is 192.168.2.254 if no DHCP server is discovered on the network.

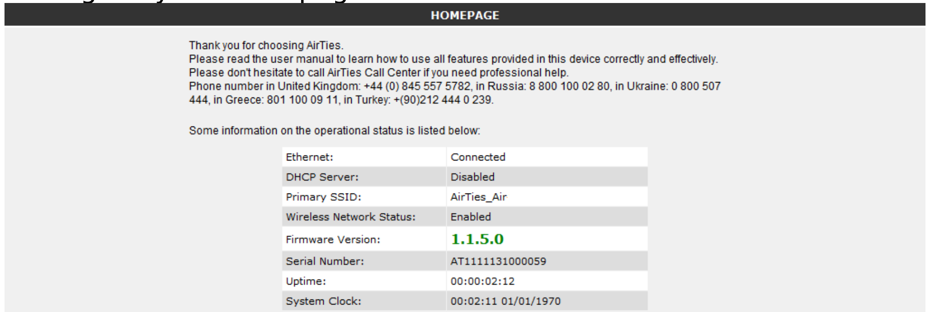
If a DHCP Server is discovered on the network then you need to discover the address of the device. This can be done as follows -

- Windows users should use AirTies Network Assistant
- Windows users can locate the device under Network and select properties
- Non windows users should log into their existing gateway and view the LAN / DHCP settings to see what IP address has been giving to the AirTies device. The device name will appear in the list of clients.

Note: To set a password on the login screen, read "MANAGEMENT" under the "Password Settings" section

Homepage

After the splash screen is the "Homepage" screen. You can see the information about the current working status and the general settings at your homepage screen.



HOMEPAGE

Thank you for choosing AirTies.
Please read the user manual to learn how to use all features provided in this device correctly and effectively.
Please don't hesitate to call AirTies Call Center if you need professional help.
Phone number in United Kingdom: +44 (0) 845 557 5782, in Russia: 8 800 100 02 80, in Ukraine: 0 800 507 444, in Greece: 801 100 09 11, in Turkey: +(90)212 444 0 239.

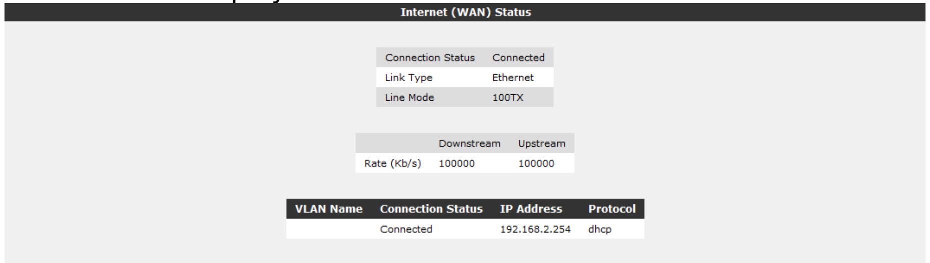
Some information on the operational status is listed below:

Ethernet:	Connected
DHCP Server:	Disabled
Primary SSID:	AirTies_Air
Wireless Network Status:	Enabled
Firmware Version:	1.1.5.0
Serial Number:	AT1111131000059
Uptime:	00:00:02:12
System Clock:	00:02:11 01/01/1970

INTERNET SETTINGS

Internet (WAN) Status

When you click the "INTERNET" menu item the Internet WAN page Status will be displayed.



Internet (WAN) Status

Connection Status	Connected
Link Type	Ethernet
Line Mode	100TX

	Downstream	Upstream
Rate (Kb/s)	100000	100000

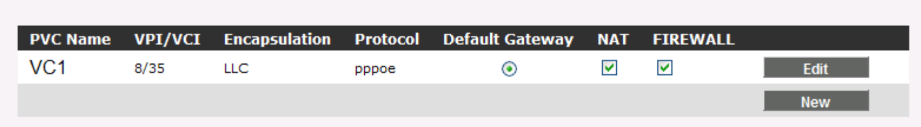
VLAN Name	Connection Status	IP Address	Protocol
	Connected	192.168.2.254	dhcp

Here you can see detailed information about the Internet connection and upstream / downstream data transfer rates.

Internet Settings

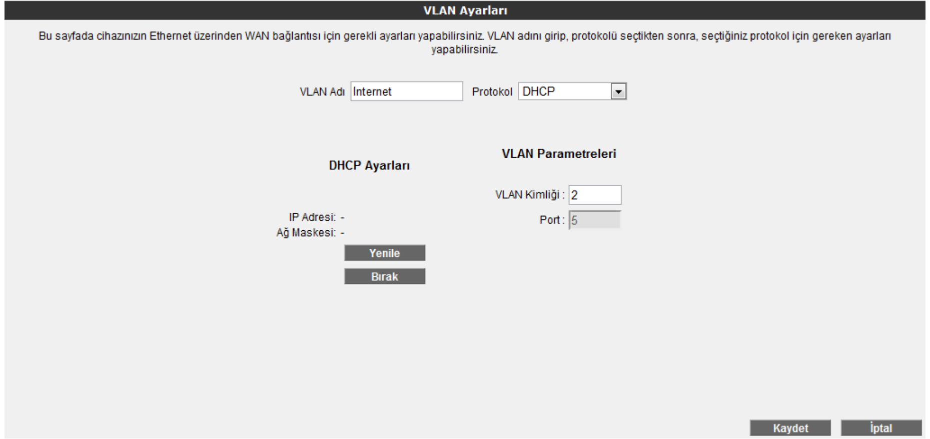
When you click "Internet Settings" from the "INTERNET" a menu showing your default WAN settings will be displayed. Please, follow these steps for making your device's internet settings:

1. When you click "Internet Settings", you will see a table which shows your device's default PVC connection.



PVC Name	VPI/VCI	Encapsulation	Protocol	Default Gateway	NAT	FIREWALL	
VC1	8/35	LLC	pppoe	●	☑	☑	Edit
							New

2. NAT and Firewall can be enabled or disabled from the "Internet Settings" page, by default these are enabled and should be enabled under normal operation. To configure your internet connection settings click the "Edit" button.



VLAN Ayarları

Bu sayfada cihazınızın Ethernet üzerinden WAN bağlantısı için gerekli ayarları yapabilirsiniz. VLAN adını girip, protokolü seçtikten sonra, seçtiğiniz protokol için gereken ayarları yapabilirsiniz.

VLAN Adı: Internet
Protokol: DHCP

DHCP Ayarları

IP Adresi: -
Ağ Maskesi: -

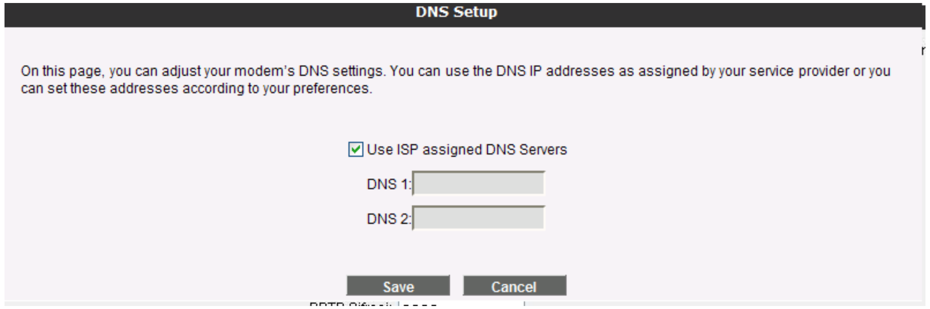
VLAN Parametreleri

VLAN Kimliği : 2
Port : 5

3. First of all, you should know to support which from PPPoE, DHCP, Bridge or Static protocols. According to the protocol, Internet Service Provider should give you to the information that you need. After you fill the informations in the interested area, click "Save".

DNS Setting

For advanced users there is the option to adjust your DNS settings. When you click "DNS Setup" from the "INTERNET" a page giving you the option to specify two DNS servers is displayed.



DNS Setup

On this page, you can adjust your modem's DNS settings. You can use the DNS IP addresses as assigned by your service provider or you can set these addresses according to your preferences.

☑ Use ISP assigned DNS Servers

DNS 1:

DNS 2:

By default the checkbox "Use ISP assigned DNS Servers" should always be selected. If you want to specify your own DNS servers then you can uncheck this checkbox and specify your own primary and secondary DNS servers by entering the IP address of each server.

Click "Save" to complete the DNS setup.

MAC Cloning

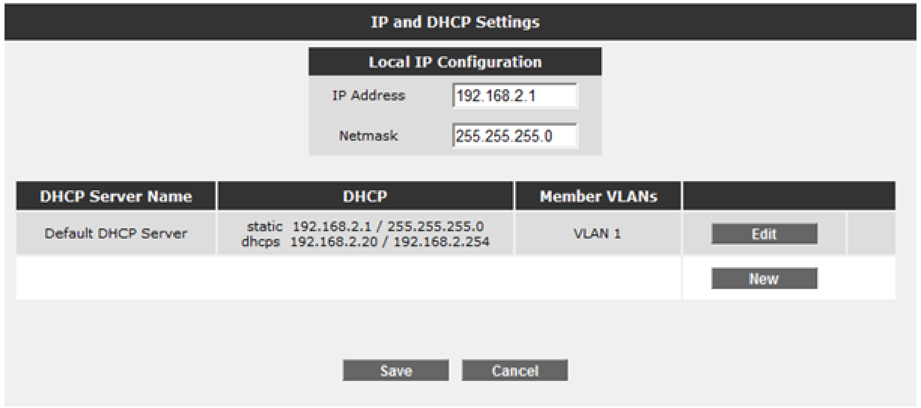
You will see that "Mac Cloning" submenu, under the "INTERNET" menu on your device's web interface.

In this page, MAC address and Hostname can be set manually and MAC address can be also cloned automatically.

LAN SETTINGS

Any device that you connect to your router, such as PCs, network printers, IP cameras, etc., are clients. Any operation related to clients that will have a local network connection to your router can be done through the "LAN" menu of the Web interface and its submenus.

When you click on the "LAN" menu, the "LAN Client List" screen will come up. All clients that are connected to your router and their connection details are shown on this screen.



IP and DHCP Settings

Local IP Configuration

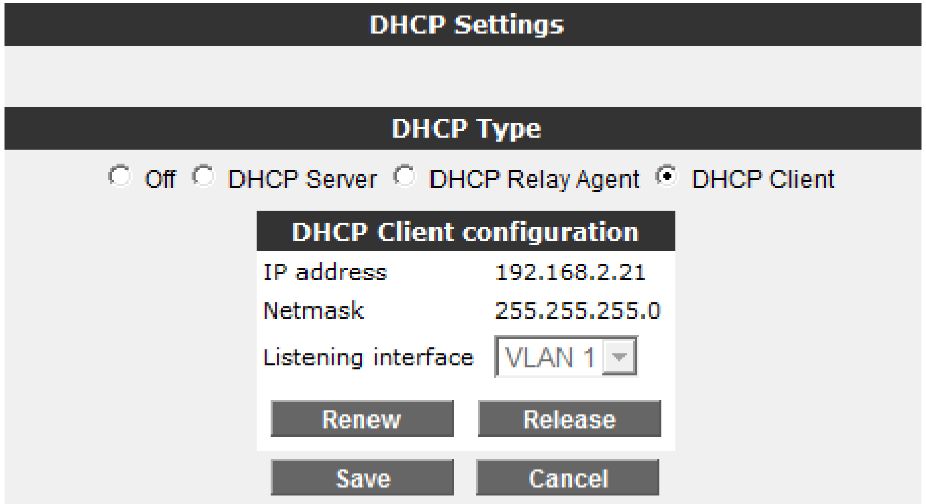
IP Address: 192.168.2.1

Netmask: 255.255.255.0

DHCP Server Name	DHCP	Member VLANs	
Default DHCP Server	static 192.168.2.1 / 255.255.255.0 dhcps 192.168.2.20 / 192.168.2.254	VLAN 1	Edit
			New

IP and DHCP Settings

Each client that is connected to your device takes a local IP address (Internet Protocol Address). The device's module which distributes IP address informations is called DHCP (Dynamic Host Configuration Protocol). You can configure the IP and DHCP Settings of your device, from the IP and DHCP Settings submenu under the LAN menu.


DHCP Settings

DHCP Type

○ Off ○ DHCP Server ○ DHCP Relay Agent ● DHCP Client

DHCP Client configuration

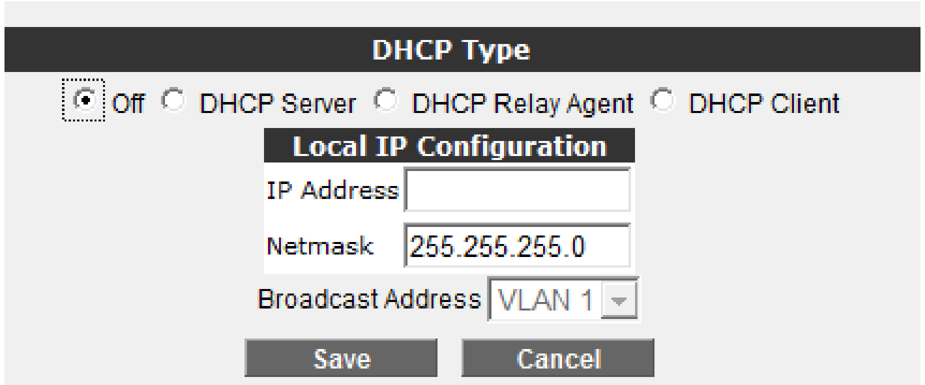
IP address	192.168.2.21
Netmask	255.255.255.0
Listening interface	VLAN 1

You can change the IP address and Netmask of your device in the "Local IP Configuration" table. The default IP Address of your device is 192.168.2.1, and the default Netmask is 255.255.255.0. You can change these values depending on the requirements of your existing network.

To configure IP and network mask settings of your device and devices are connected to your network, click the "Edit" button in the "IP and DHCP Settings" menu. You see the "DHCP Settings" menu. There are 4 different options for DHCP configuration in this section.

Disable DHCP (Off)

Stops all DHCP activity on the device. When in this mode, the clients must have their IP addresses assigned manually or by a different DHCP server in order to communicate with the network. To disable DHCP select "Off" and enter an IP address and Net mask. Click "Save" to save your settings.


DHCP Type

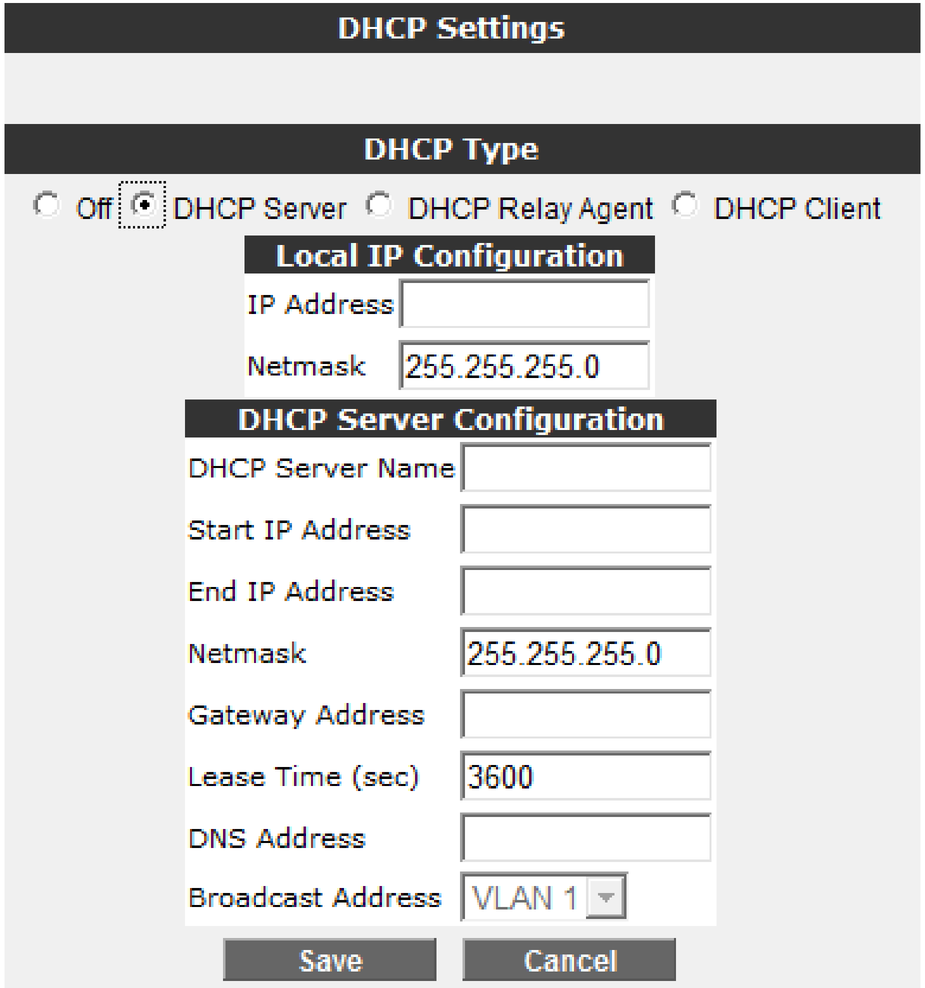
● Off ○ DHCP Server ○ DHCP Relay Agent ○ DHCP Client

Local IP Configuration

IP Address	
Netmask	255.255.255.0
Broadcast Address	VLAN 1

DHCP Server

DHCP Server mode configures the device to assign IP addresses to connecting devices. There must only be one DHCP Server on the network, which in most cases will be the router. DHCP is enabled by default. In this section you can assign an address range from which your device can assign local IP addresses to clients and the lease time. The default IP address range is 192.168.2.2 through 192.168.2.254. Maximum lease time for an assigned IP address is set as 3600 seconds, which means the assigned IP address will be renewed every 3600 seconds. To configure the device as a DHCP server select "DHCP Server" and enter an IP address, Net mask, DHCP Server Name, Start and End addresses that will be assigned devices, Net mask, Gateway Address, Lease Time, DNS Address. Click "Save" to save your settings.



DHCP Settings

DHCP Type

○ Off ● DHCP Server ○ DHCP Relay Agent ○ DHCP Client

Local IP Configuration

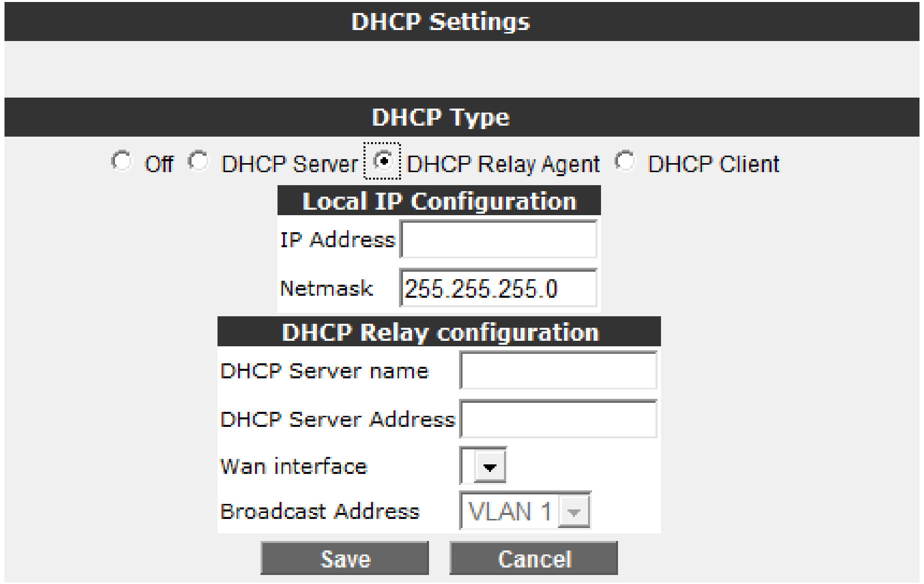
IP Address	
Netmask	255.255.255.0

DHCP Server Configuration

DHCP Server Name	
Start IP Address	
End IP Address	
Netmask	255.255.255.0
Gateway Address	
Lease Time (sec)	3600
DNS Address	
Broadcast Address	VLAN 1

DHCP Relay Agent

DHCP relay makes it possible for a DHCP server on a different network to assign local IP addresses to clients connected to your device. To enable this, the address of the device (modem, server etc) that runs the DHCP service needs to be known. If DHCP Relay is enabled the DHCP server on your device is disabled and cannot assign IP addresses to clients. To configure DHCP Relay Agent select "DHCP Relay Agent" and enter an IP address for the device, DHCP Server name and address of the DHCP Server. Click "Save" to save your settings.



DHCP Settings

DHCP Type

○ Off ○ DHCP Server ● DHCP Relay Agent ○ DHCP Client

Local IP Configuration

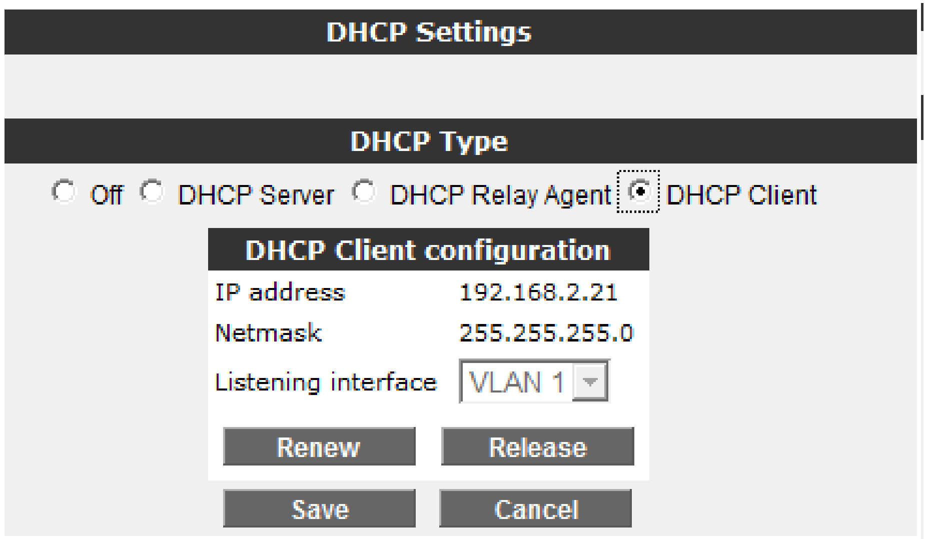
IP Address	
Netmask	255.255.255.0

DHCP Relay configuration

DHCP Server name	
DHCP Server Address	
Wan interface	
Broadcast Address	VLAN 1

DHCP Client

If your device is supported this feature, DHCP client mode configures the device to obtain an IP address from a DHCP server on the network . You can use this option if you would like your device to get an IP address from a DHCP server on the local network. You also have to specify which VLAN is to be the listening interface. Click "Save" for your settings to take effect.



DHCP Settings

DHCP Type

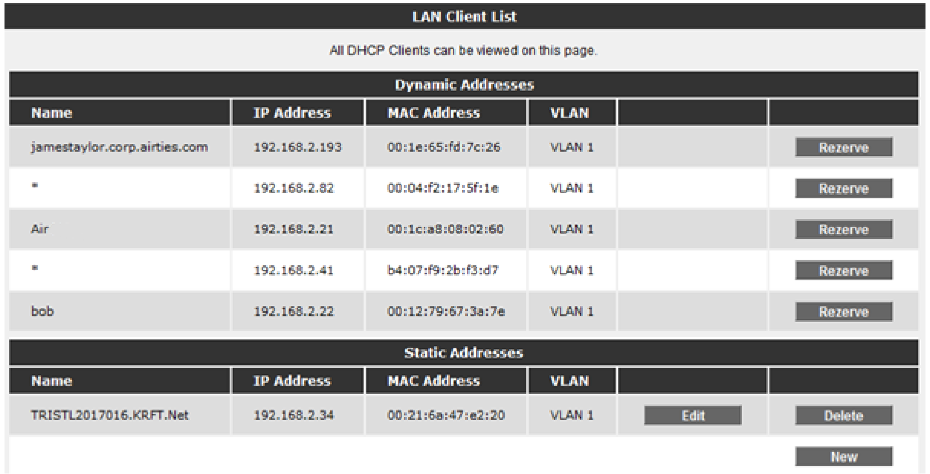
○ Off ○ DHCP Server ○ DHCP Relay Agent ● DHCP Client

DHCP Client configuration

IP address	192.168.2.21
Netmask	255.255.255.0
Listening interface	VLAN 1

LAN Clients

If the device is configured as a DHCP server then you can see a list of all the clients connected to the device. Select LAN Client under the LAN menu of the Web Interface. Through this menu, you can also reserve an IP address for a client. When an IP address is reserved for a client, it cannot be assigned to any other client. Whenever the client connects to the router, it gets the IP address reserved for it. Click the reserve button next to a dynamic address to reserve this as a static address.



LAN Client List

All DHCP Clients can be viewed on this page.

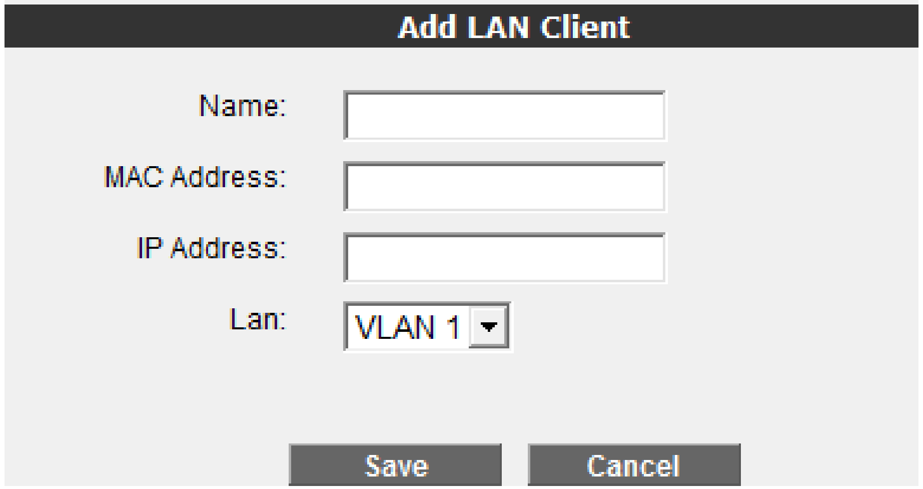
Dynamic Addresses

Name	IP Address	MAC Address	VLAN		
jamestaylor.corp.airties.com	192.168.2.193	00:1e:65:fd:7c:26	VLAN 1		Rezerve
*	192.168.2.82	00:04:f2:17:5f:1e	VLAN 1		Rezerve
Air	192.168.2.21	00:1c:a8:08:02:60	VLAN 1		Rezerve
*	192.168.2.41	b4:07:f9:2b:f3:d7	VLAN 1		Rezerve
bob	192.168.2.22	00:12:79:67:3a:7e	VLAN 1		Rezerve

Static Addresses

Name	IP Address	MAC Address	VLAN		
TRISTL2017016.KRFT.Net	192.168.2.34	00:21:6a:47:e2:20	VLAN 1	Edit	Delete
					New

You can see the IP addresses that are reserved in the "Static Addresses" table. "Dynamic Addresses" table shows the IP addresses assigned but not reserved. To new static address click "New". Enter the Name, MAC Address, IP Address and select the LAN. Click "Save" to create the new static address.



Add LAN Client

Name:	
MAC Address:	
IP Address:	
Lan:	VLAN 1

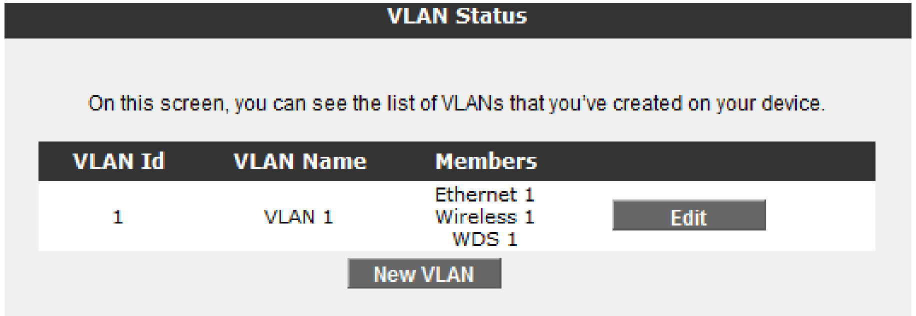
VLAN Configuration

If your device is supported this feature, you will see the VLAN Status and you can configure VLANs.

Virtual Local Area Networks (VLANs) separate a single physical network into multiple logical networks. A reason why you may create a VLAN is if you want to separate your network for security reasons, your guests can use one VLAN and you can use another.

By default the device is configured to operate over a single VLAN.

To configure VLANs select VLAN Configuration under the LAN menu.



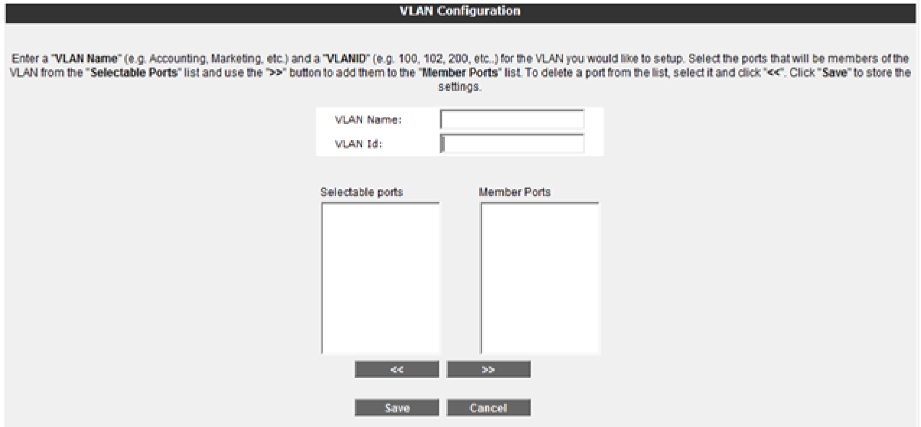
VLAN Status

On this screen, you can see the list of VLANs that you've created on your device.

VLAN Id	VLAN Name	Members	
1	VLAN 1	Ethernet 1 Wireless 1 WDS 1	Edit

A list of VLANs will be shown. By default there will be a single VLAN named VLAN 1. This is the entire network.

To create a new VLAN click New VLAN.



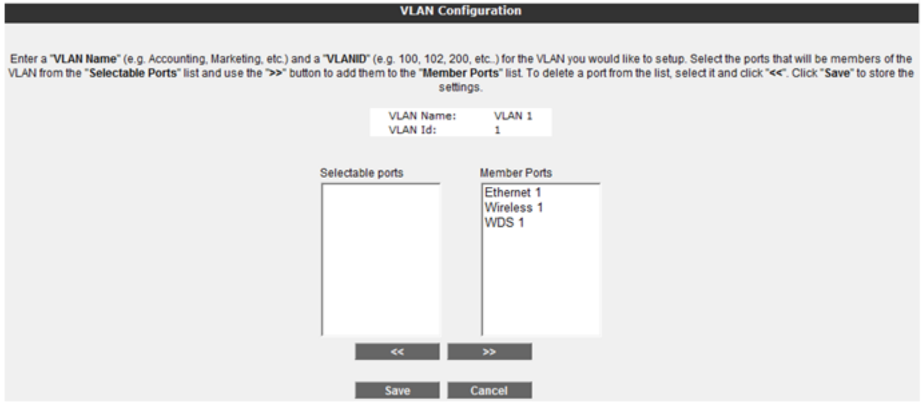
VLAN Configuration

Enter a "**VLAN Name**" (e.g. Accounting, Marketing, etc.) and a "**VLANID**" (e.g. 100, 102, 200, etc..) for the VLAN you would like to setup. Select the ports that will be members of the VLAN from the "**Selectable Ports**" list and use the "**>>**" button to add them to the "**Member Ports**" list. To delete a port from the list, select it and click "**<<**". Click "**Save**" to store the settings.

VLAN Name:	
VLAN Id:	

Enter a VLAN Name and VLAN Id for the new VLAN. Select the ports that you want to add to the VLAN (Ethernet ports, wireless ports). Click "Save" to save your changes.

To add or remove ports from the VLANs select Edit from the main VLAN menu for the VLAN that you want to update.



VLAN Configuration

Enter a "**VLAN Name**" (e.g. Accounting, Marketing, etc.) and a "**VLANID**" (e.g. 100, 102, 200, etc..) for the VLAN you would like to setup. Select the ports that will be members of the VLAN from the "**Selectable Ports**" list and use the "**>>**" button to add them to the "**Member Ports**" list. To delete a port from the list, select it and click "**<<**". Click "**Save**" to store the settings.

VLAN Name: VLAN 1
VLAN Id: 1

Selectable ports

Member Ports
Ethernet 1
Wireless 1
WDS 1

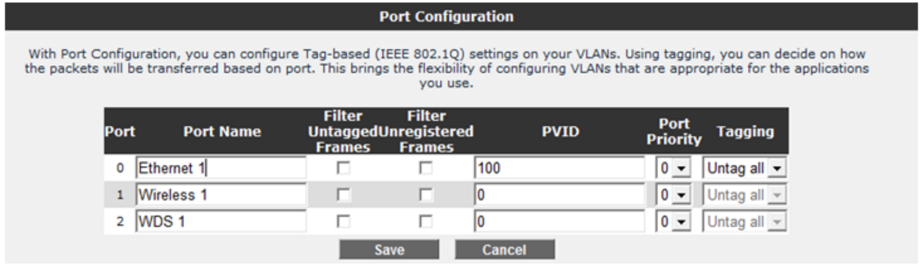
From the list of selectable ports select the port that you want to add and click ">>". Select "Save" to save your changes.

Note that a port can only be a member of one VLAN at any time so if you want to add a port to a VLAN you must first remove it from any VLAN that it is currently configured to use.

Port Configuration

If your device is supported this feature, you can configure to tags on each port to allow data to be separated to different VLANs.

Select Port Configuration from the LAN menu.



Port Configuration

With Port Configuration, you can configure Tag-based (IEEE 802.1Q) settings on your VLANs. Using tagging, you can decide on how the packets will be transferred based on port. This brings the flexibility of configuring VLANs that are appropriate for the applications you use.

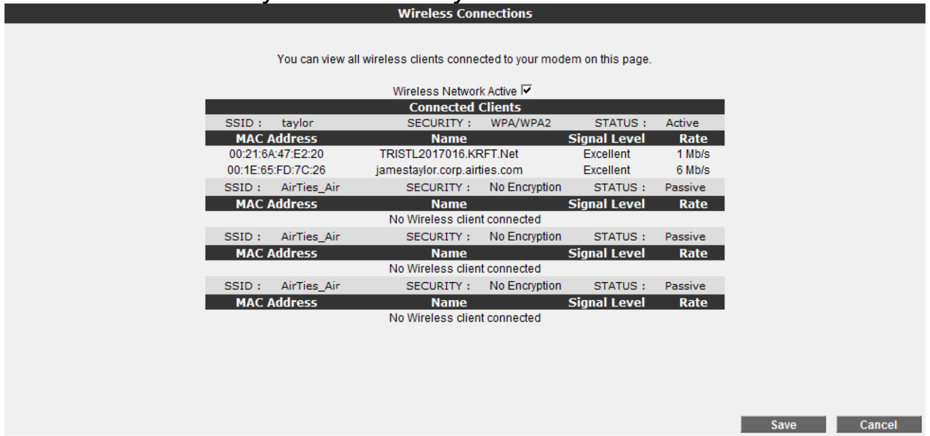
Port	Port Name	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
0	Ethernet 1	☐	☐	100	0	Untag all
1	Wireless 1	☐	☐	0	0	Untag all
2	WDS 1	☐	☐	0	0	Untag all

For each port the tagging can be configured to add or remove a VLAN tag. Data can also be filtered based on untagged and unregistered frames. Click "Save" to save your changes.

Wireless Network Settings

From Advanced Settings in AirTies Network Assistant, when you click the WIRELESS menu, you will be in the Wireless Connections screen that lists all the wireless clients connected to the AirTies device, grouped by wireless SSID.

The Wireless Network Active box lets you enable or disable the wireless feature of your device. By default this is enabled.



Wireless Connections

You can view all wireless clients connected to your modem on this page.

Wireless Network Active ☑

Connected Clients

SSID : taylor SECURITY : WPA/WPA2 STATUS : Active

MAC Address	Name	Signal Level	Rate
00:21:6A:47:E2:20	TRISTL2017016.KRFT.Net	Excellent	1 Mb/s
00:1E:65:FD:7C:26	jamestaylor.corp.airties.com	Excellent	6 Mb/s

SSID : AirTies_Air SECURITY : No Encryption STATUS : Passive

MAC Address	Name	Signal Level	Rate

No Wireless client connected

SSID : AirTies_Air SECURITY : No Encryption STATUS : Passive

MAC Address	Name	Signal Level	Rate

No Wireless client connected

SSID : AirTies_Air SECURITY : No Encryption STATUS : Passive

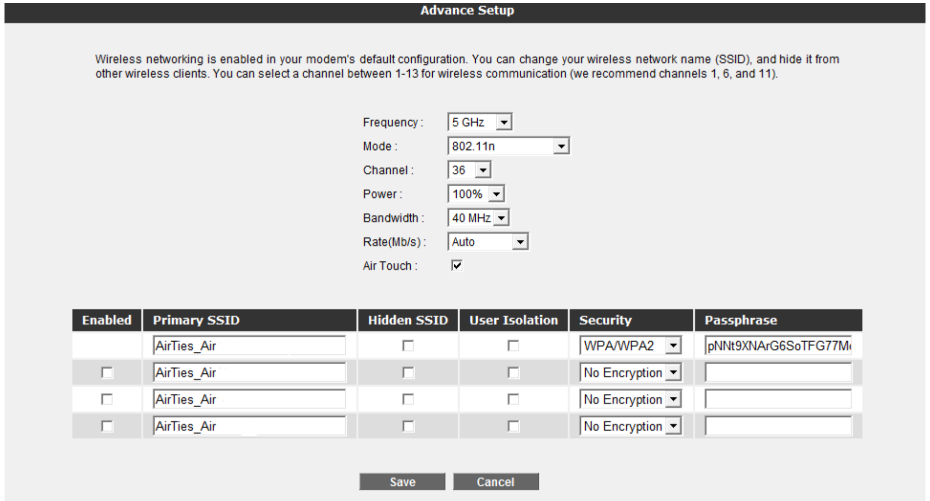
MAC Address	Name	Signal Level	Rate

No Wireless client connected

Go to Wireless Settings under the WIRELESS menu to configure your wireless network.

Access Point

To enable the Access Point feature you must select Access Point from the Operating Mode drop down box.



Advance Setup

Wireless networking is enabled in your modem's default configuration. You can change your wireless network name (SSID), and hide it from other wireless clients. You can select a channel between 1-13 for wireless communication (we recommend channels 1, 6, and 11).

Frequency :	5 GHz
Mode :	802.11n
Channel :	36
Power :	100%
Bandwidth :	40 MHz
Rate(Mb/s) :	Auto
Air Touch :	☑

Enabled	Primary SSID	Hidden SSID	User Isolation	Security	Passphrase
	AirTies_Air	□	□	WPA/WPA2	pNNt9XNArG6SoTFG77M
□	AirTies_Air	□	□	No Encryption	
□	AirTies_Air	□	□	No Encryption	
□	AirTies_Air	□	□	No Encryption	

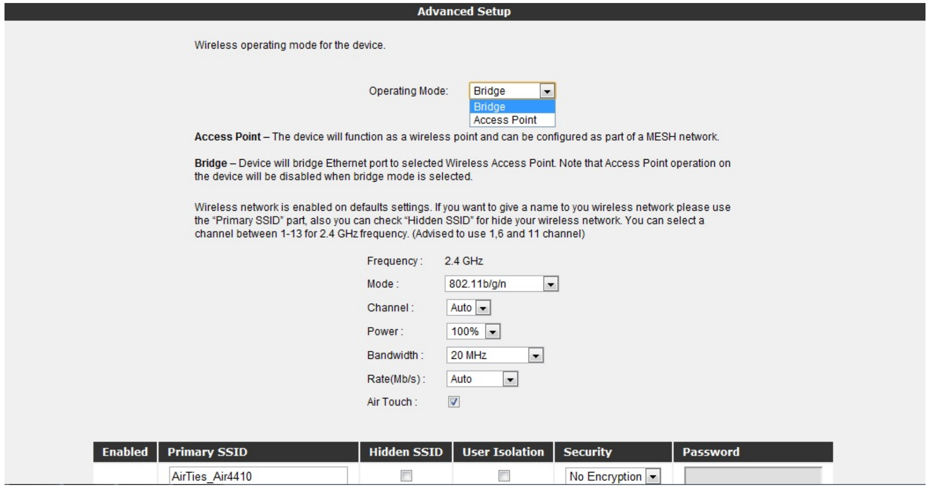
- In the Frequency field you can choose whether to use 2.4Ghz or 5Ghz (if your device is supported).
- In the Mode field, you can choose the wireless mode the device will operate in.
- In the Channel field, you can specify the frequency the device will broadcast in. If you are using 2.4Ghz then it is recommended that you choose one of 1, 6, or 11 as the channel number.
- Power displays the total transmitted power from your device.
- Bandwidth field allows you to specify whether to use 20MHz or 40MHz. When in 802.11n mode. 40MHz should be selected to achieve 300Mbps wireless data rates
- You can assign a name to your wireless network by entering the name in the Primary SSID field. This name is broadcast by your device.
- Rate shows the highest wireless data transfer rate supported by your device. It is set to Auto by default. This allows for automatic adjustment of data transfer rate based on distance and signal quality.

Universal Bridge

The Universal Bridge feature allows for any device with an Ethernet port to be wirelessly connected to an existing Access Point. This allows for devices such as Set Top Boxes, Connected TVs and printers to be connected to an existing Wi-Fi Access Point.

To enable the Universal Bridge feature you must select Universal Bridge from the Operating Mode drop down box.

Note that the device can be in either Access Point mode or Bridge mode. When Bridge mode is enabled the Access Point feature on the device is disabled.



Advanced Setup

Wireless operating mode for the device.

Operating Mode: Bridge

Access Point – The device will function as a wireless point and can be configured as part of a MESH network.

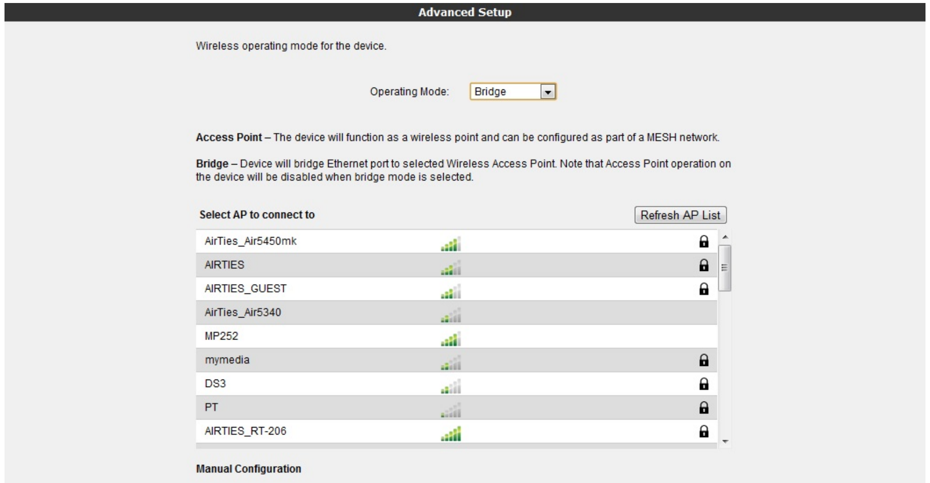
Bridge – Device will bridge Ethernet port to selected Wireless Access Point. Note that Access Point operation on the device will be disabled when bridge mode is selected.

Wireless network is enabled on defaults settings. If you want to give a name to you wireless network please use the "Primary SSID" part, also you can check "Hidden SSID" for hide your wireless network. You can select a channel between 1-13 for 2.4 GHz frequency. (Advised to use 1,6 and 11 channel)

Frequency :	2.4 GHz
Mode :	802.11b/g/n
Channel :	Auto
Power :	100%
Bandwidth :	20 MHz
Rate(Mb/s) :	Auto
Air Touch :	☑

Enabled	Primary SSID	Hidden SSID	User Isolation	Security	Password
	AirTies_Air4410	□	□	No Encryption	

A search will be made for existing Access Points. After approximately 30 seconds a list of Access Points that have been found are displayed with the signal strength and security of each one.



Advanced Setup

Wireless operating mode for the device.

Operating Mode: Bridge

Access Point – The device will function as a wireless point and can be configured as part of a MESH network.

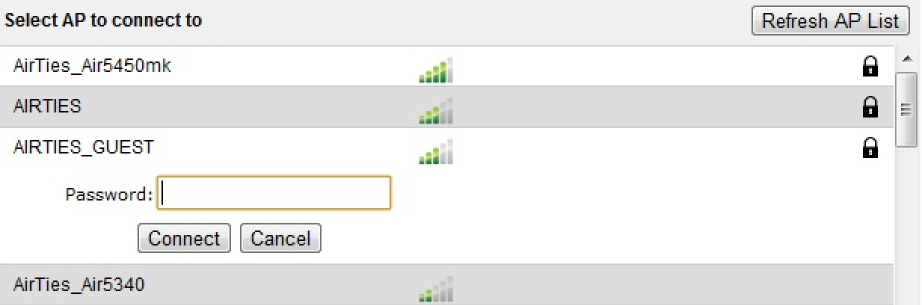
Bridge – Device will bridge Ethernet port to selected Wireless Access Point. Note that Access Point operation on the device will be disabled when bridge mode is selected.

Select AP to connect to

AirTies_Air5450mk	🔒
AIRTIES	🔒
AIRTIES_GUEST	🔒
AirTies_Air5340	
MP252	
mymedia	🔒
DS3	🔒
PT	🔒
AIRTIES_RT-206	🔒

Manual Configuration

From the list select your Access Point that you want to bridge with. When you select the Access Point you will be prompted for your password if a secure connection has been configured on the Access Point. Enter the password and click Connect.



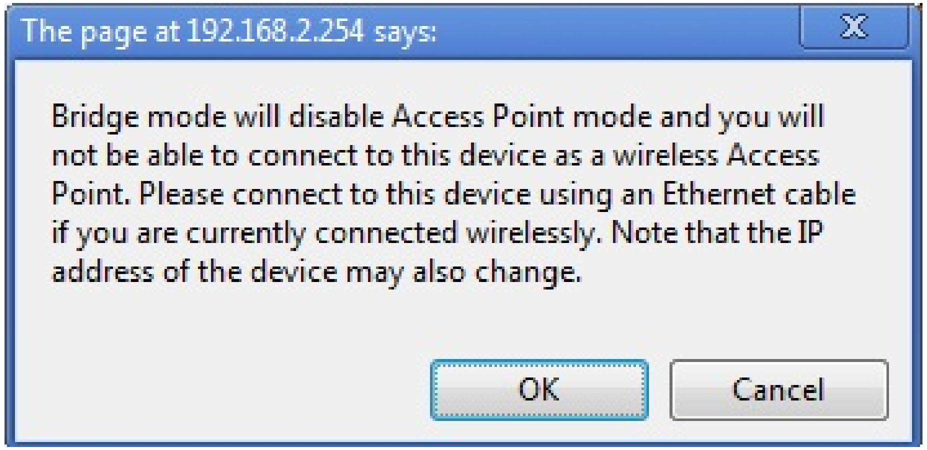
Select AP to connect to

AirTies_Air5450mk	🔒
AIRTIES	🔒
AIRTIES_GUEST	🔒

Password:

AirTies_Air5340

A warning will be displayed, informing the user that wireless Access Point will be disabled and that they will only be able to connect to the device with an Ethernet cable. Click OK to save the changes and enable Universal Bridge mode.



The page at 192.168.2.254 says:

Bridge mode will disable Access Point mode and you will not be able to connect to this device as a wireless Access Point. Please connect to this device using an Ethernet cable if you are currently connected wirelessly. Note that the IP address of the device may also change.

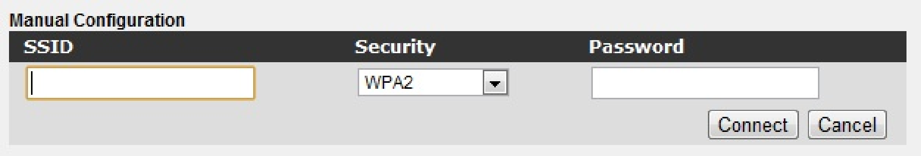
The device is now configured as a bridge device. Connecting a device using a network cable will bridge the device to the wireless Access Point that you configured. The device should not be connected by cable to the Access Point that it has been bridged with otherwise your network will not function correctly.

Note that the IP address of the device may change. AirTies Network Assistant can be used to find your device and reconfigure if necessary. Alternatively you can connect a computer directly to the device to connect and configure the device.

If you want to turn your device back into Access Point mode then you need to do this from the Wireless Settings menu.

Manual Mode

If your SSID is hidden then you need to configure the Access Point using manual mode. Underneath the list of SSIDs you can manually enter the SSID, security mode and password of your existing Access Point.



Manual Configuration

SSID	Security	Password
	WPA2	

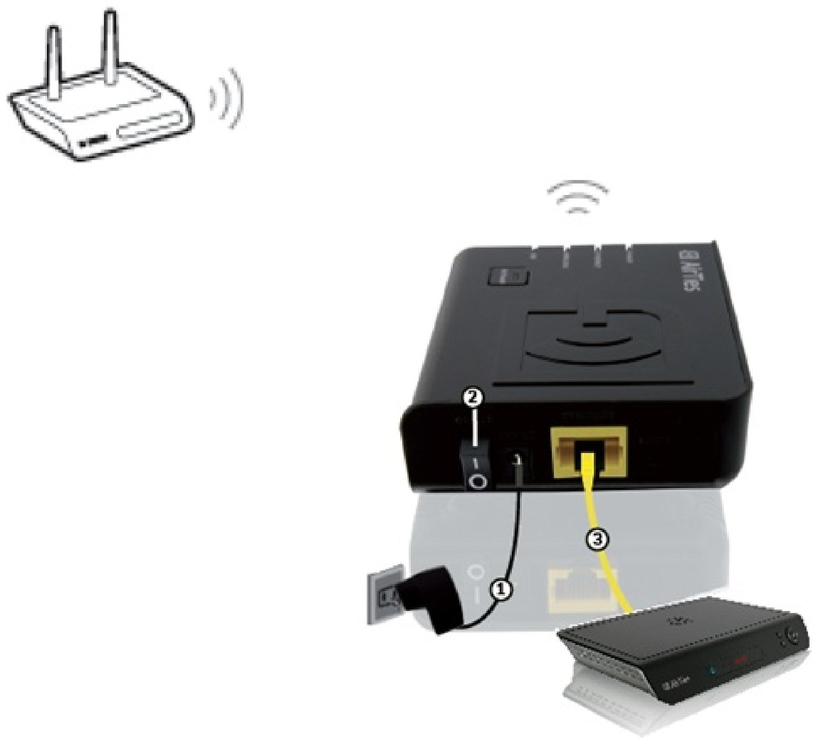
Click Connect to enable bridge mode. Click OK at the warning. The device is now in Universal Bridge mode.

To use Universal Bride you must change your device cabling:

Universal Bridge Cabling

First complete the cabling process as shown in the diagrams.

1. Connect the power adapter inside your box to the power inlet socket of your device and plug into the electric socket.
2. Turn on the Air 4410 by switching the On/Off button to position "1".
3. Connect the Ethernet cable inside your box to the Air 4410's Ethernet port and connect the other end to the Ethernet enables device that you want to connect to your wireless network.



If your device is supported multiSSID, up to four separate SSIDs can be configured. By default one is configured. To add additional SSIDs you need to check the Enabled check box.

- Primary SSID is the name that the wireless device broadcasts. This is the name that can be seen on computers when you select what wireless device to connect to.
- Checking the Hidden SSID box will hide your SSID during broadcast. This is not recommended since hiding the SSID will prevent laptops from seeing your network within their range.

- Checking User Isolation will prevent clients connecting to your network from connecting to each other.
- The security level can be set in the Security drop down box. This should be set to the highest security level WPA/WPA2.
- The passphrase for the wireless connection is set in the "Passphrase" section. This should contain at least 8 characters.
- It is possible to set up 4 wireless SSIDs to have multiple networks.

Click "Save" to store your settings.

Wireless Security Settings

It is not necessary to configure wireless security to enable wireless communication. However, due to growing importance of data security, it is strongly recommended that you choose one of the security protocols described below that best fits your needs.

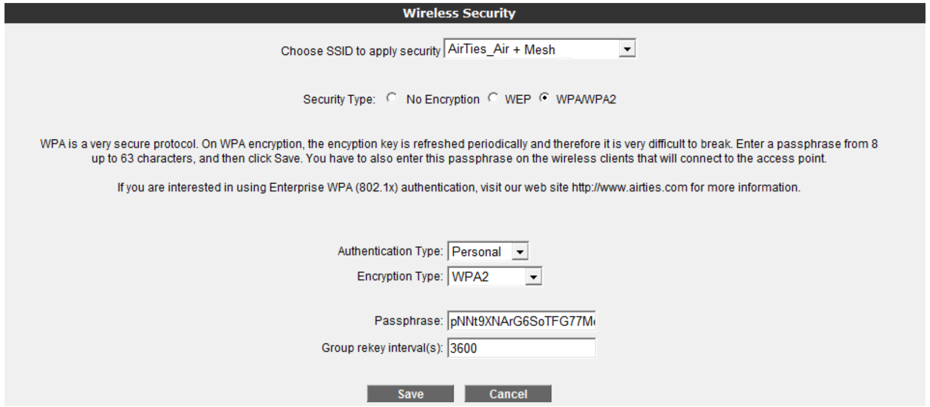
Wi-Fi Protected Access (WPA), WPA2, and Wired Equivalent Privacy (WEP) are wireless encryption protocols used to encrypt the data traffic within the wireless network. It is recommended that you use the most secure standard, which is WPA2.

MAC Address Filtering allows you to control which network cards can connect to the AirTies device and share your Internet access. For your wireless network security, it is recommended that both MAC Address filtering and WPA2 wireless encryption protocols be activated.

WPA2 Security Settings

WPA2, defined by the IEEE 802.11i standard, is one of the latest wireless encryption methods. If you would like to use WPA2 in your wireless network, all the wireless adapters in your network should support WPA2. For Centrino platform computers, it is necessary to download the WPA2 updates for the Windows XP operating system to be able to use WPA2 (www.microsoft.com).

To enable WPA2 encryption: 1. Go to Wireless Security Settings under the WIRELESS menu of the Web interface of your device. 2. From the Security drop down box of the first SSID select WPA2. 3. Select WPA/WPA2 from Security Type. 4. Enter a Passphrase that is 8 to 63 characters long (use a combination of letters and digits) in the Passphrase field. Make sure you choose a key that is not easy to guess. Click Save. 5. You must activate WPA2 and set the same network key in all the devices that will communicate with your AirTies device.



Wireless Security

Choose SSID to apply security: AirTies_Air + Mesh

Security Type: ○ No Encryption ○ WEP ● WPA/WPA2

WPA is a very secure protocol. On WPA encryption, the encyption key is refreshed periodically and therefore it is very difficult to break. Enter a passphrase from 8 up to 63 characters, and then click Save. You have to also enter this passphrase on the wireless clients that will connect to the access point.

If you are interested in using Enterprise WPA (802.1x) authentication, visit our web site http://www.airties.com for more information.

Authentication Type: Personal

Encryption Type: WPA2

Passphrase: pNNt9XNArG6SoTFG77M

Group rekey interval(s): 3600

WEP Security Settings

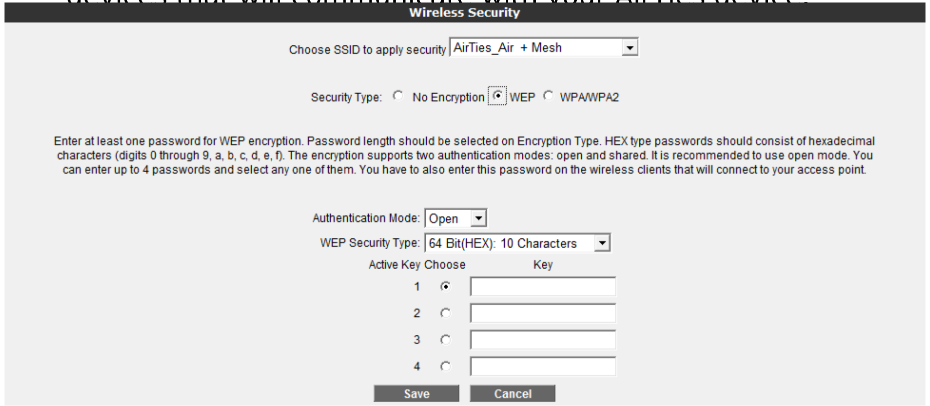
WEP is less secure then WPA and should only be used if your PC's wireless card does not support WPA. To configure WEP secutiry:

1. Go to Wireless Security Settings under the WIRELESS menu of the Web interface of your device.
2. From the Security drop down box of the first SSID select WEP.
3. Select Open for Authentication Mode.
4. For WEP Security Type you can select: a. 10 Hexadecimal characters (A-F and 0-9) for 64-bit encryption. b. 5 ASCII

characters for 64-bit encryption. c. 26 Hexadecimal characters for 128-bit encryption. d. 13 ASCII characters for 123-bit encryption.

5. You can enter up to 4 network keys and choose the one you want to use. Click Save.

6. You must activate WEP and set the same network key in all the devices that will communicate with your AirTies device.



Wireless Security

Choose SSID to apply security: AirTies_Air + Mesh

Security Type: ○ No Encryption ● WEP ○ WPA/WPA2

Enter at least one password for WEP encryption. Password length should be selected on Encryption Type. HEX type passwords should consist of hexadecimal characters (digits 0 through 9, a, b, c, d, e, f). The encryption supports two authentication modes: open and shared. It is recommended to use open mode. You can enter up to 4 passwords and select any one of them. You have to also enter this password on the wireless clients that will connect to your access point.

Authentication Mode: Open

WEP Security Type: 64 Bit(HEX): 10 Characters

Active Key	Choose	Key
1	●	
2	○	
3	○	
4	○	

MAC Filtering

1. Click on MAC Filtering under the WIRELESS menu of the Web interface of your device.

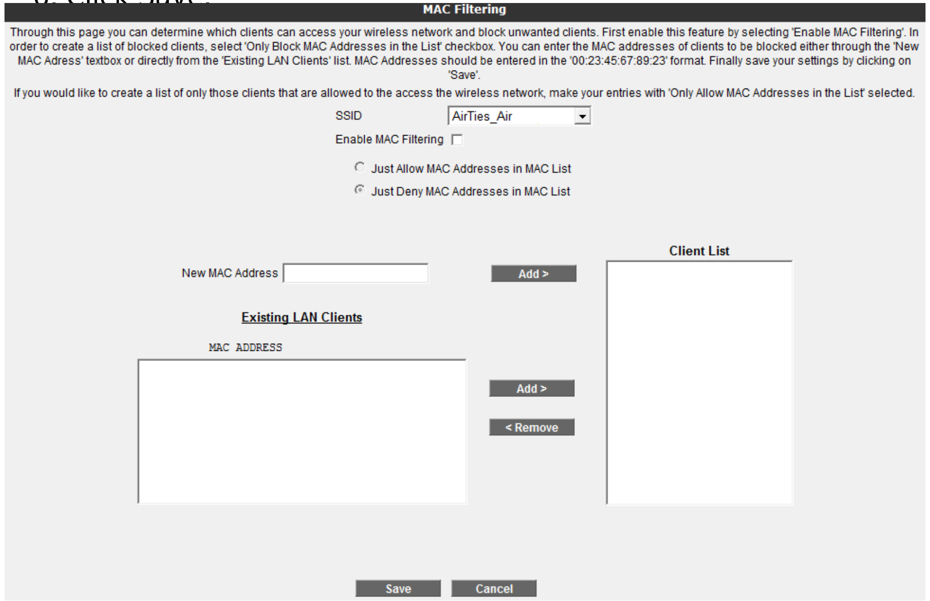
2. Select the SSID that you want to configure MAC Filtering for.

3. Check the Enable MAC Filtering box.

4. To add the devices that will be permitted to access the wireless network: * Select Just Allow MAC Addresses in MAC List. * For each device to be allowed access, enter the wireless MAC address of the device (e.g."00-14-38-15-60-DD") in the New MAC Address field and then click the ADD button.

5. To add devices that will be blocked from accessing the wireless network: * Select Just Deny MAC Addresses in MAC List. * For each device to be blocked, enter the wireless MAC address of the device in the New MAC Address field and then click the ADD button.

6. Click Save.



MAC Filtering

Through this page you can determine which clients can access your wireless network and block unwanted clients. First enable this feature by selecting 'Enable MAC Filtering'. In order to create a list of blocked clients, select 'Only Block MAC Addresses in the List' checkbox. You can enter the MAC addresses of clients to be blocked either through the 'New MAC Adress' textbox or directly from the 'Existing LAN Clients' list. MAC Addresses should be entered in the '00:23:45:67:89:23' format. Finally save your settings by clicking on 'Save'.

If you would like to create a list of only those clients that are allowed to the access the wireless network, make your entries with 'Only Allow MAC Addresses in the List' selected.

SSID: AirTies_Air

Enable MAC Filtering □

○ Just Allow MAC Addresses in MAC List

● Just Deny MAC Addresses in MAC List

New MAC Address:

Your AirTies device supports 802.1x Authentication protocol as well. For detailed information about how to setup 802.1x security, please check the AirTies Website at www.airties.com .

MESH

AirTouch technology automatically configures two devices to create a MESH. Simply push the AirTouch button on the two devices that you want to configure a MESH between. MESH can also be configured manually.

AirTies Mesh Technology resolves weak wireless signal and coverage area problems often encountered in multi-story concrete buildings. To extend wireless coverage area, it is necessary to use AirTies access point devices functioning in repeater mode. The access points function as repeaters and communicate with each other via a special protocol that maintains the signal strength over long distances and through barriers such as concrete walls. Computers connect to all devices through the Mesh Network. This way, the wireless coverage area can be extended to the maximum while any signal strength problems through barriers are resolved.

The following steps will help you set up a Mesh Network with your modem:

Important:

a. Your modem and repeaters must all operate on the same channel. Therefore, it is recommended you to use channels 1, 6 or 11.

b. Your modem and repeaters must also all operate at the same security level.

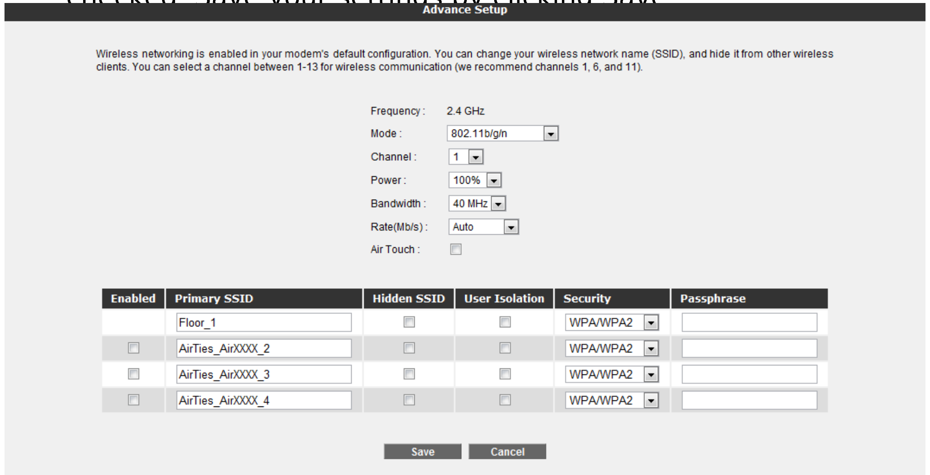
c. The signal level received at the location of the repeaters must not be below medium.

d. Repeaters must be in DHCP client mode and your modem must be in DHCP server mode. You can check this in the LAN menu of the web interface.

e. In the following example, the SSIDs are called Floor_1, Floor_2 and Floor_3. This type of naming system has been used to help your understand the procedure. But in practice we recommend you use the same name for all SSIDs. For example, if they are all called AirTies, users can automatically connect to the device with the best signal strength.

Step One (Configuring the Modem):

1. Enter the Wireless Settings section of the WIRELESS main menu in the device's web interface. Change the SSID name to Floor_1. Enter the channel that the mesh network will use in the Channel field. We recommended you use 1, 6 or 11. While the Mesh Network is set up manually, the AirTouch box must not be checked. Save your settings by clicking Save.



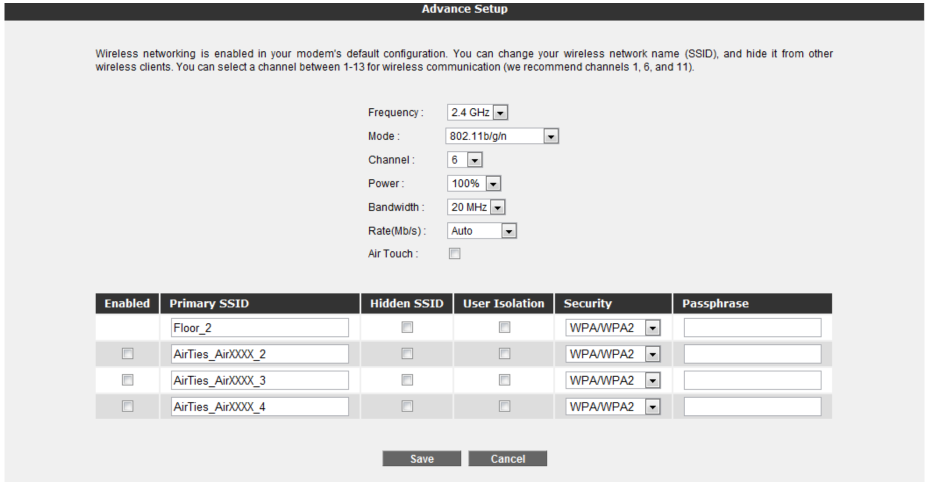
Wireless networking is enabled in your modem's default configuration. You can change your wireless network name (SSID), and hide it from other wireless clients. You can select a channel between 1-13 for wireless communication (we recommend channels 1, 6, and 11).

Frequency : 2.4 GHz
Mode : 802.11b/g/n
Channel : 1
Power : 100%
Bandwidth : 40 MHz
Rate(Mb/s) : Auto
Air Touch : □

Enabled	Primary SSID	Hidden SSID	User Isolation	Security	Passphrase
	Floor_1	□	□	WPA/WPA2	
□	AirTies_AirXXXX_2	□	□	WPA/WPA2	
□	AirTies_AirXXXX_3	□	□	WPA/WPA2	
□	AirTies_AirXXXX_4	□	□	WPA/WPA2	

Step Two (Configuring the Repeater on Floor_2):

1. Enter the Wireless Settings section of the WIRELESS main menu in the device's web interface. Change the SSID name to Floor_2. Enter the channel that the mesh network will use in the Channel field. The AirTouch box must not be checked. Save your settings by clicking Save.



Advance Setup

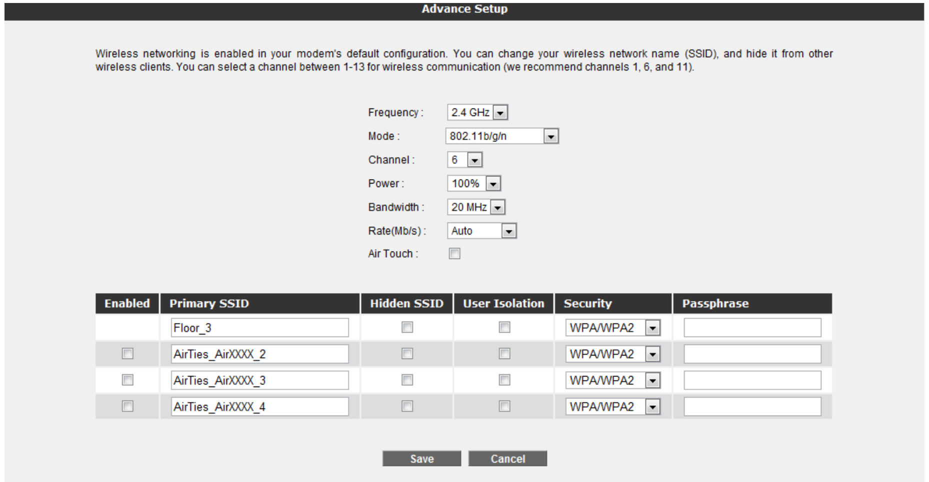
Wireless networking is enabled in your modem's default configuration. You can change your wireless network name (SSID), and hide it from other wireless clients. You can select a channel between 1-13 for wireless communication (we recommend channels 1, 6, and 11).

Frequency : 2.4 GHz
Mode : 802.11b/g/n
Channel : 6
Power : 100%
Bandwidth : 20 MHz
Rate(Mb/s) : Auto
Air Touch : □

Enabled	Primary SSID	Hidden SSID	User Isolation	Security	Passphrase
	Floor_2	□	□	WPA/WPA2	
□	AirTies_AirXXXX_2	□	□	WPA/WPA2	
□	AirTies_AirXXXX_3	□	□	WPA/WPA2	
□	AirTies_AirXXXX_4	□	□	WPA/WPA2	

Step Three (Configuring the Repeater in Floor_3):

1. Enter the Wireless Settings section of the WIRELESS main menu in the device's web interface. Change the SSID name to Floor 3. Enter the channel that the "mesh network" will use in the Channel field. The AirTouch box must not be checked. Save your settings by clicking Save.



Advance Setup

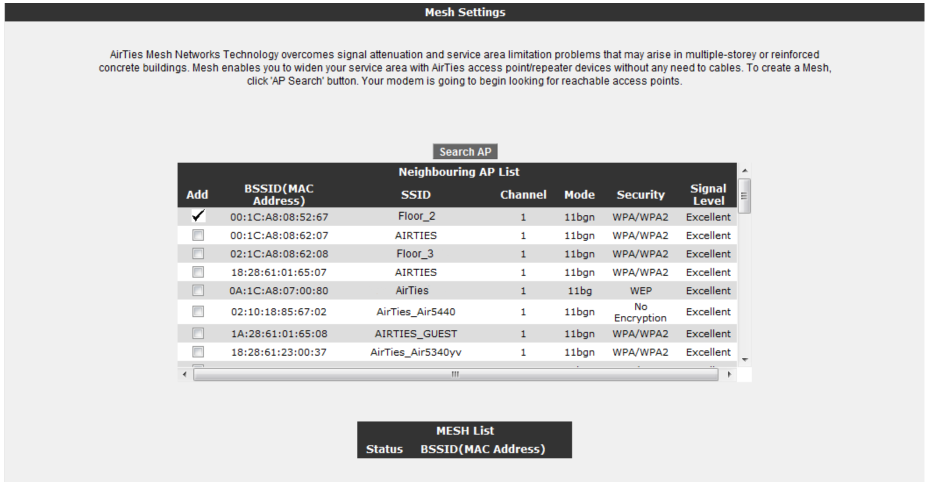
Wireless networking is enabled in your modem's default configuration. You can change your wireless network name (SSID), and hide it from other wireless clients. You can select a channel between 1-13 for wireless communication (we recommend channels 1, 6, and 11).

Frequency : 2.4 GHz
Mode : 802.11b/g/n
Channel : 6
Power : 100%
Bandwidth : 20 MHz
Rate(Mb/s) : Auto
Air Touch : □

Enabled	Primary SSID	Hidden SSID	User Isolation	Security	Passphrase
	Floor_3	□	□	WPA/WPA2	
□	AirTies_AirXXXX_2	□	□	WPA/WPA2	
□	AirTies_AirXXXX_3	□	□	WPA/WPA2	
□	AirTies_AirXXXX_4	□	□	WPA/WPA2	

Step Four:

1. Select the Mesh menu in the WIRELESS main menu in your modem's web interface. Click on the Find AP button in the screen that has opened called MESH Settings.
2. When you click the Find AP button, the device will begin searching for wireless access point devices it can connect to and will list the ones it finds.
3. Select the access point or points that you want a Mesh connection with your modem by checking the boxes. In the access points you selected, the signal level must be at least medium or higher. Complete the Mesh settings of your modem by clicking the Save button.



Mesh Settings

AirTies Mesh Networks Technology overcomes signal attenuation and service area limitation problems that may arise in multiple-storey or reinforced concrete buildings. Mesh enables you to widen your service area with AirTies access point/repeater devices without any need to cables. To create a Mesh, click 'AP Search' button. Your modem is going to begin looking for reachable access points.

Neighbouring AP List

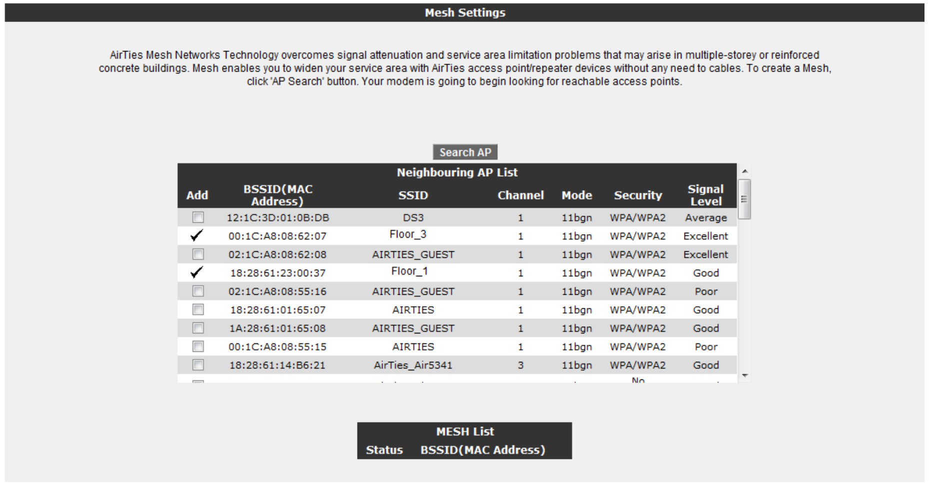
Add	BSSID(MAC Address)	SSID	Channel	Mode	Security	Signal Level
✓	00:1C:A8:08:52:67	Floor_2	1	11bgn	WPA/WPA2	Excellent
□	00:1C:A8:08:62:07	AIRTIES	1	11bgn	WPA/WPA2	Excellent
□	02:1C:A8:08:62:08	Floor_3	1	11bgn	WPA/WPA2	Excellent
□	18:28:61:01:65:07	AIRTIES	1	11bgn	WPA/WPA2	Excellent
□	0A:1C:A8:07:00:80	AirTies	1	11bg	WEP	Excellent
□	02:10:18:85:67:02	AirTies_Air5440	1	11bgn	No Encryption	Excellent
□	1A:28:61:01:65:08	AIRTIES_GUEST	1	11bgn	WPA/WPA2	Excellent
□	18:28:61:23:00:37	AirTies_Air5340yv	1	11bgn	WPA/WPA2	Excellent

MESH List

Status	BSSID(MAC Address)

Step Five:

1. Select the Mesh menu in the WIRELESS main menu in your repeater's web interface. Click the Find AP button in the screen that has opened called MESH Settings.
2. When you click the Find AP button, the device will start to search for wireless access point devices it can connect to and will list the ones it finds.
3. Select the devices that you want a Mesh connection with your repeater by checking the boxes. Complete your repeater's Mesh settings by clicking the Save button.



Mesh Settings

AirTies Mesh Networks Technology overcomes signal attenuation and service area limitation problems that may arise in multiple-storey or reinforced concrete buildings. Mesh enables you to widen your service area with AirTies access point/repeater devices without any need to cables. To create a Mesh, click 'AP Search' button. Your modem is going to begin looking for reachable access points.

Neighbouring AP List

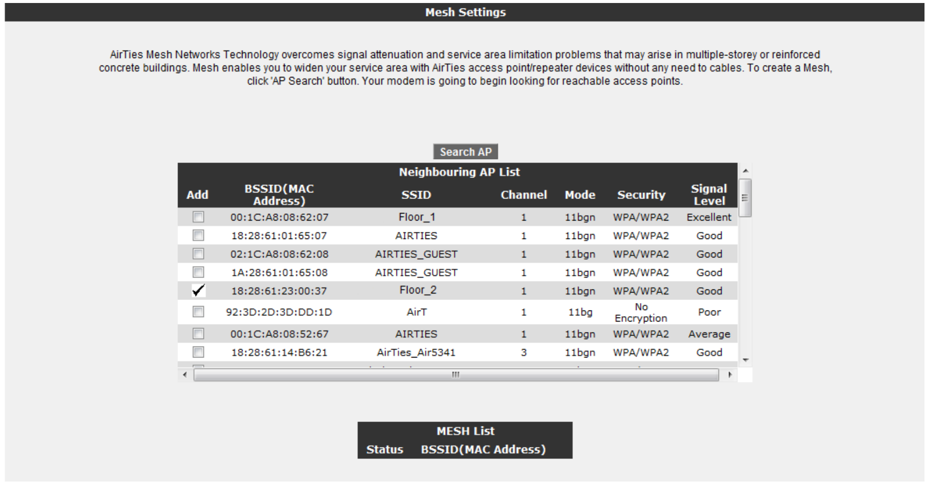
Add	BSSID(MAC Address)	SSID	Channel	Mode	Security	Signal Level
□	12:1C:3D:01:0B:DB	DS3	1	11bgn	WPA/WPA2	Average
✓	00:1C:A8:08:62:07	Floor_3	1	11bgn	WPA/WPA2	Excellent
□	02:1C:A8:08:62:08	AIRTIES_GUEST	1	11bgn	WPA/WPA2	Excellent
✓	18:28:61:23:00:37	Floor_1	1	11bgn	WPA/WPA2	Good
□	02:1C:A8:08:55:16	AIRTIES_GUEST	1	11bgn	WPA/WPA2	Poor
□	18:28:61:01:65:07	AIRTIES	1	11bgn	WPA/WPA2	Good
□	1A:28:61:01:65:08	AIRTIES_GUEST	1	11bgn	WPA/WPA2	Good
□	00:1C:A8:08:55:15	AIRTIES	1	11bgn	WPA/WPA2	Poor
□	18:28:61:14:B6:21	AirTies_Air5341	3	11bgn	WPA/WPA2	Good

MESH List

Status	BSSID(MAC Address)

Step Six:

1. Select the Mesh menu under the WIRELESS main menu in your repeater's web interface. Click the Find AP button in the screen that has opened called MESH Settings.
2. When you click the Find AP button, the device will start to search for wireless access point devices it can connect to and will list the ones it finds.
3. Select the devices that you want a Mesh connection with your repeater by checking the boxes. Complete your repeater's Mesh settings by clicking the Save button.



Mesh Settings

AirTies Mesh Networks Technology overcomes signal attenuation and service area limitation problems that may arise in multiple-storey or reinforced concrete buildings. Mesh enables you to widen your service area with AirTies access point/repeater devices without any need to cables. To create a Mesh, click 'AP Search' button. Your modem is going to begin looking for reachable access points.

Neighbouring AP List

Add	BSSID(MAC Address)	SSID	Channel	Mode	Security	Signal Level
□	00:1C:A8:08:62:07	Floor_1	1	11bgn	WPA/WPA2	Excellent
□	18:28:61:01:65:07	AIRTIES	1	11bgn	WPA/WPA2	Good
□	02:1C:A8:08:62:08	AIRTIES_GUEST	1	11bgn	WPA/WPA2	Good
□	1A:28:61:01:65:08	AIRTIES_GUEST	1	11bgn	WPA/WPA2	Good
✓	18:28:61:23:00:37	Floor_2	1	11bgn	WPA/WPA2	Good
□	92:3D:2D:3D:DD:1D	AirT	1	11bg	No Encryption	Poor
□	00:1C:A8:08:52:67	AIRTIES	1	11bgn	WPA/WPA2	Average
□	18:28:61:14:B6:21	AirTies_Air5341	3	11bgn	WPA/WPA2	Good

MESH List

Status	BSSID(MAC Address)

FIREWALL Settings

A firewall prevents unauthorised Internet users from accessing your local network and your computer.

AirTies Firewall has a SPI, Stateful Packet Inspection, feature. SPI monitors the protocol and packet addresses being received to determine if the information should be passed through the firewall to the connected computers on your network. The Internet addresses that are a source of malicious attacks are permanently blocked from accessing your network.

You can also limit or block the Internet access of any local user by defining advanced rules for Internet access.

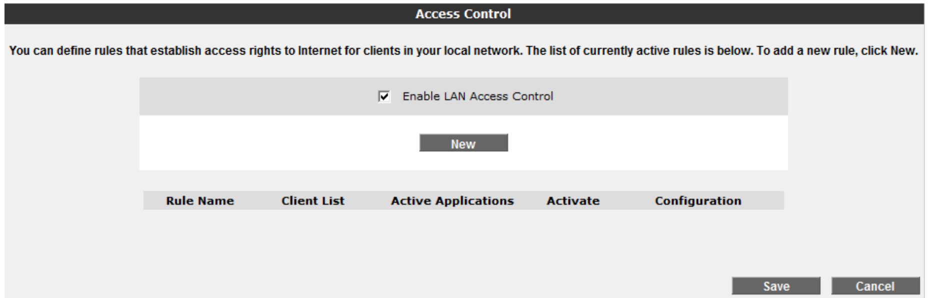
Firewall is activated by default.

The following sections describe the submenus under the FIREWALL menu of the web interface.

Access Control

You can allow or block Internet access for any computer on your local network using the Access Control feature. These access restrictions can be based on IP address as well as MAC address. Access Control is enabled by default.

To define a new access rule, click "New".



Access Control

You can define rules that establish access rights to Internet for clients in your local network. The list of currently active rules is below. To add a new rule, click New.

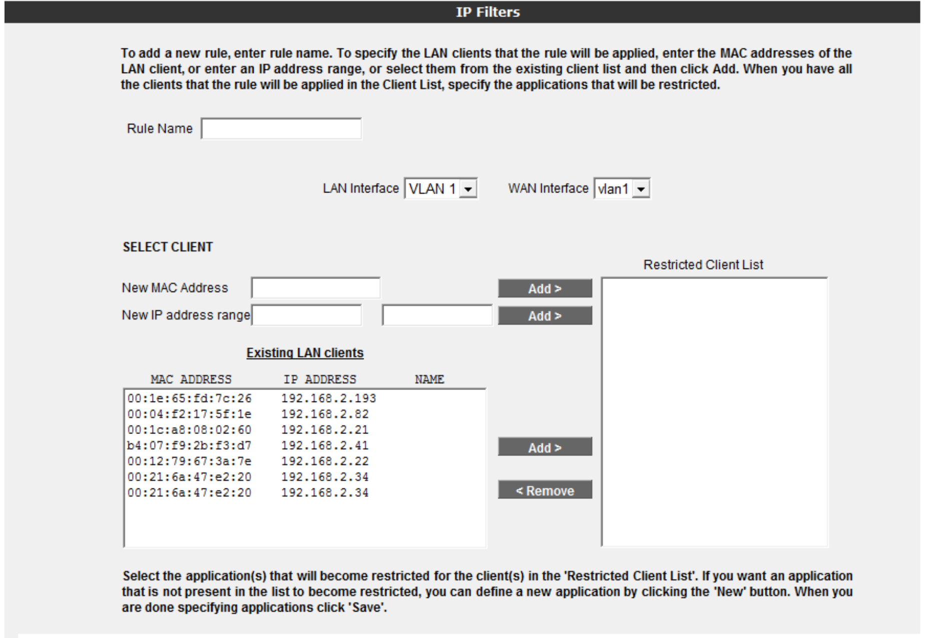
☑ Enable LAN Access Control

Rule Name	Client List	Active Applications	Activate	Configuration

On the page that appears:

1. Enter a name for the access rule you would like to define in the "Rule Name" field. Choose a name that is easy to remember.
2. If VLAN is implemented then select the LAN or WAN interface, otherwise take the defaults.
3. In the "SELECT CLIENT" section you can enter the IP or MAC addresses of the clients whose access you would like to restrict with this rule.
4. Access control can be defined based on local IP or MAC address (uniquely identifies the network adapter of the device). If an access rule is defined by MAC address, the rule defined for the device will be valid even if the local IP address changes.
5. It is possible to enter the MAC or IP addresses individually or choose them from the list of client devices in the local network.
6. Enter the MAC address of the device you would like to restrict traffic from in "New MAC Address" or IP address of the device in the "New IP address range" field. For a single IP address, enter the same value in the two boxes that define the range.

(e.g. 192.168.2.2 and 192.168.2.2). To restrict access for all devices in an IP address range, enter the beginning and ending IP addresses (e.g. 192.168.2.2 and 192.168.2.50). Click the "Add >" button to add the device to the restricted list



IP Filters

To add a new rule, enter rule name. To specify the LAN clients that the rule will be applied, enter the MAC addresses of the LAN client, or enter an IP address range, or select them from the existing client list and then click Add. When you have all the clients that the rule will be applied in the Client List, specify the applications that will be restricted.

Rule Name

LAN Interface VLAN 1 WAN Interface vlan1

SELECT CLIENT

New MAC Address

New IP address range

Existing LAN clients

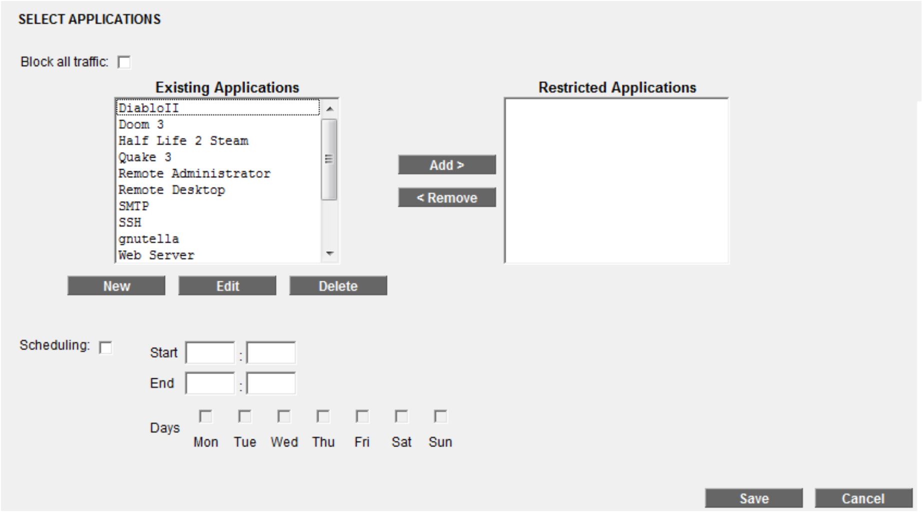
MAC ADDRESS	IP ADDRESS	NAME
00:1e:65:fd:7c:26	192.168.2.193	
00:04:f2:17:5f:1e	192.168.2.82	
00:1c:a8:08:02:60	192.168.2.21	
b4:07:f9:2b:f3:d7	192.168.2.41	
00:12:79:67:3a:7e	192.168.2.22	
00:21:6a:47:e2:20	192.168.2.34	
00:21:6a:47:e2:20	192.168.2.34	

Restricted Client List

Select the application(s) that will become restricted for the client(s) in the 'Restricted Client List'. If you want an application that is not present in the list to become restricted, you can define a new application by clicking the 'New' button. When you are done specifying applications click 'Save'.

7. Select "Block all traffic" to block all traffic to and from the Internet interface.

8. To block an application select an application from the list and click "Add>" to add the application to the restricted application list.



SELECT APPLICATIONS

Block all traffic: □

Existing Applications

DiabloII
Doom 3
Half Life 2 Steam
Quake 3
Remote Administrator
Remote Desktop
SMTP
SSH
gnutella
Web Server

Restricted Applications

Scheduling: □

Start :
End :

Days

□	□	□	□	□	□	□
Mon	Tue	Wed	Thu	Fri	Sat	Sun

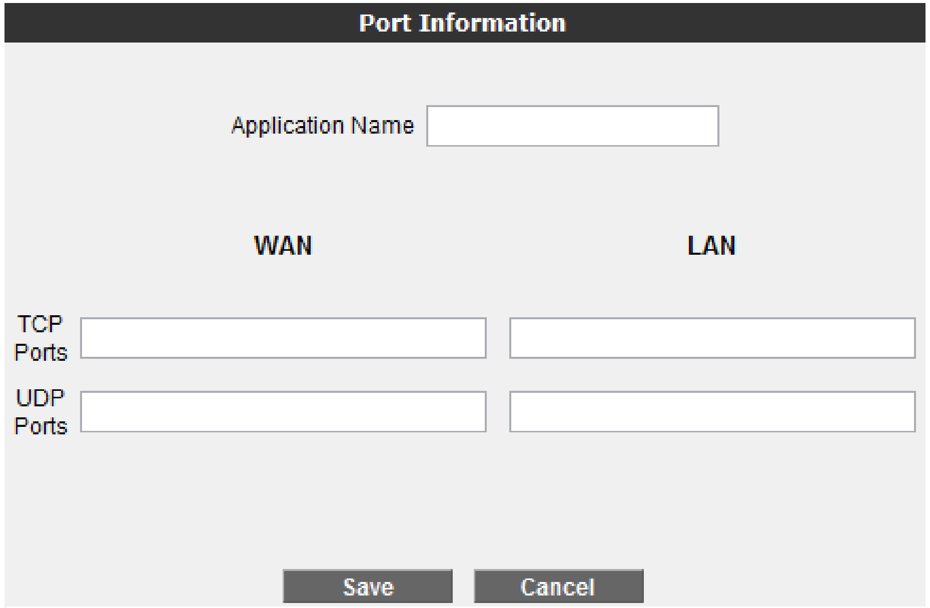
9. To define a new application, click the "New" button.

10. Enter a name for the application you are defining in the "Application Name" field.

11. Enter the WAN port for the application in the WAN TCP and UDP fields.

12. Enter the internal port number that the application will use in the local network in the LAN TCP and UDP fields.

13. Click "Save".

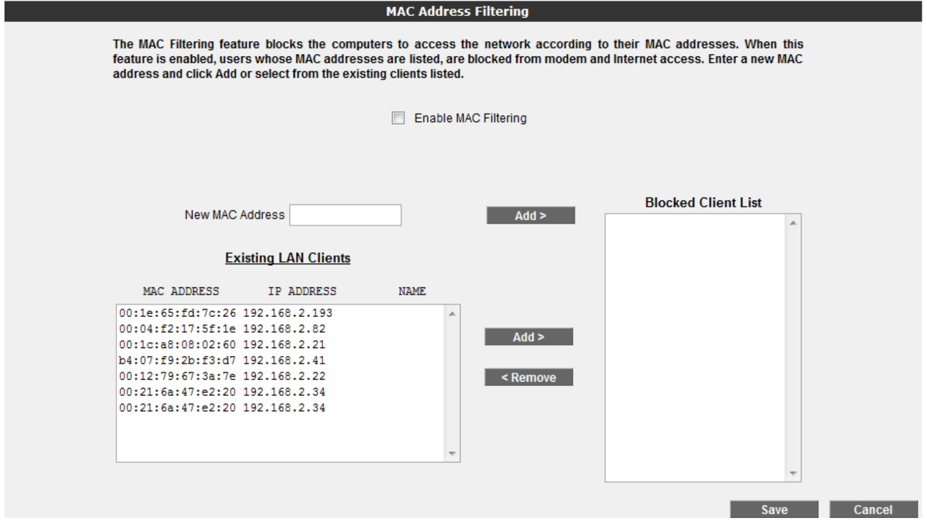


14. The new application definition will be added to the existing applications list.
15. A schedule for your rule can be specified. By default the rule will be always enforced. Enabling "Scheduling", entering a start time and end time and selecting days of the week will only enforce the rule during the specified time.
16. Click "Save" to create the rule.

MAC Filtering

MAC Address Filtering allows you to block Internet access based on MAC addresses. When this feature is activated, you can specify the MAC addresses of the computers that will have Internet access blocked.

1. Check the "Enable MAC Filtering" box.
2. Enter a new MAC address or choose one from the list of existing clients and click "Add >".
3. Click "Save"



The MAC Filtering feature blocks the computers to access the network according to their MAC addresses. When this feature is enabled, users whose MAC addresses are listed, are blocked from modem and Internet access. Enter a new MAC address and click Add or select from the existing clients listed.

□ Enable MAC Filtering

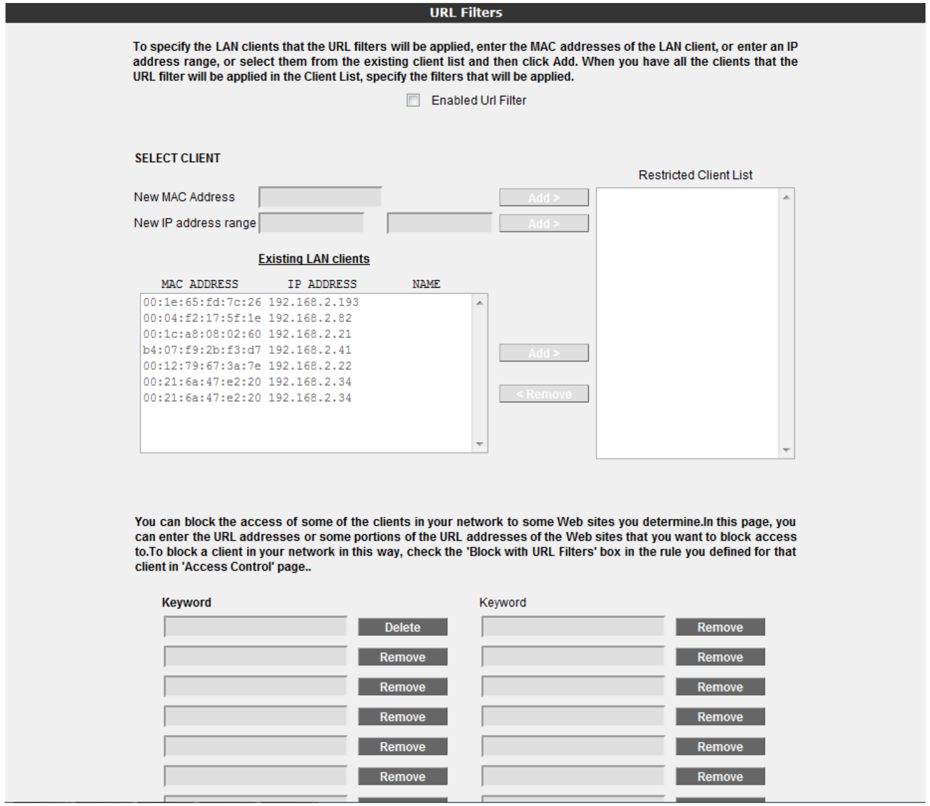
Existing LAN Clients

MAC ADDRESS	IP ADDRESS	NAME
00:1e:65:fd:7c:26	192.168.2.193	
00:04:f2:17:5f:1e	192.168.2.82	
00:1c:a8:08:02:60	192.168.2.21	
b4:07:f9:2b:f3:d7	192.168.2.41	
00:12:79:67:3a:7e	192.168.2.22	
00:21:6a:47:e2:20	192.168.2.34	
00:21:6a:47:e2:20	192.168.2.34	

URL Filters

You can block access from any computer on your local network to the websites you specify by entering the URL or any keyword that is part of the URL that you would like to block.

1. Check "Enable URL Filter".
2. Enter the IP address or MAC address of the computer that you want to provide URL filters for.



URL Filters

To specify the LAN clients that the URL filters will be applied, enter the MAC addresses of the LAN client, or enter an IP address range, or select them from the existing client list and then click Add. When you have all the clients that the URL filter will be applied in the Client List, specify the filters that will be applied.

☐ Enabled Url Filter

SELECT CLIENT

New MAC Address

New IP address range

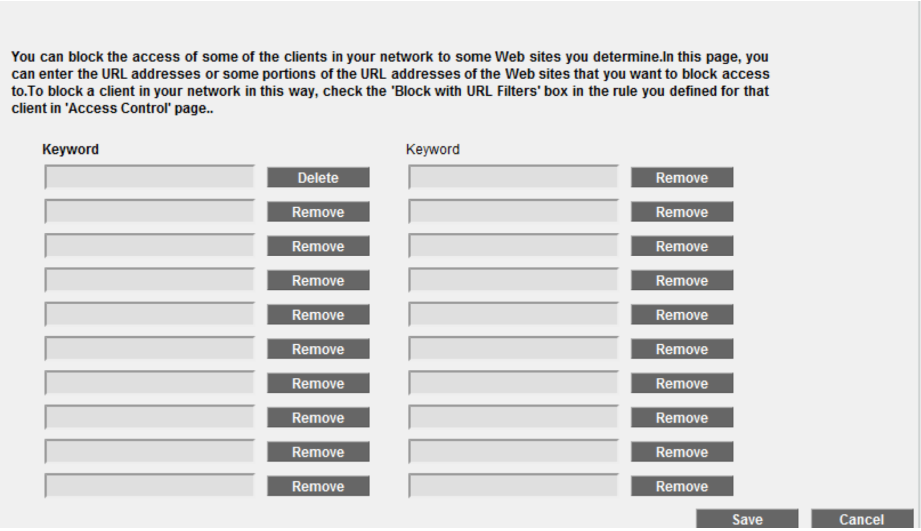
Existing LAN clients

```
  MAC ADDRESS       IP ADDRESS      NAME
00:1e:65:fd:7c:26 192.168.2.193
00:04:f2:17:5f:1e 192.168.2.82
00:1c:a8:08:02:60 192.168.2.21
b4:07:f9:2b:f3:d7 192.168.2.41
00:12:79:67:3a:7e 192.168.2.22
00:21:6a:47:e2:20 192.168.2.34
00:21:6a:47:e2:20 192.168.2.34
```

Restricted Client List

You can block the access of some of the clients in your network to some Web sites you determine.In this page, you can enter the URL addresses or some portions of the URL addresses of the Web sites that you want to block access to.To block a client in your network in this way, check the 'Block with URL Filters' box in the rule you defined for that client in 'Access Control' page..

3. In each of the boxes enter the keywords that you want to block or enter the compleye URL.
4. Click "Save" to save.

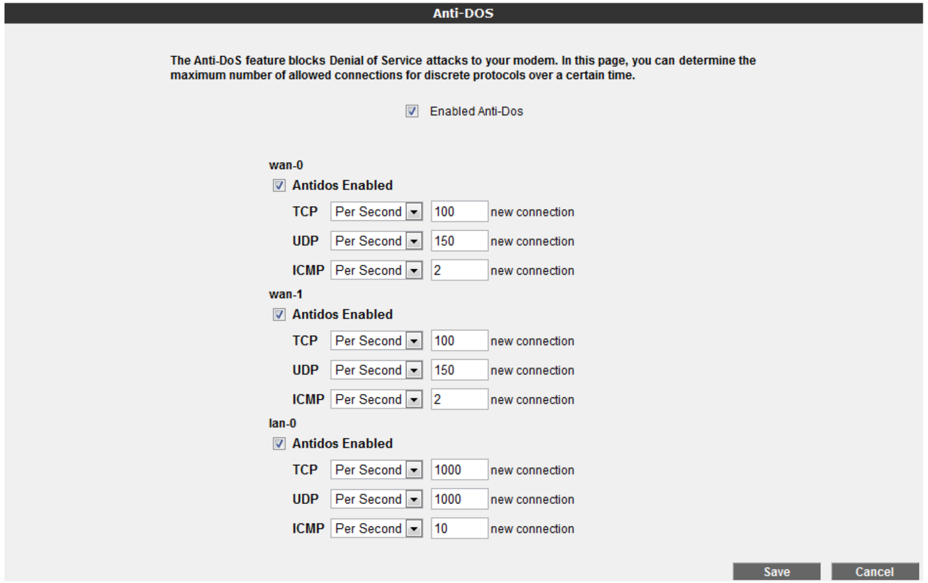


You can block the access of some of the clients in your network to some Web sites you determine.In this page, you can enter the URL addresses or some portions of the URL addresses of the Web sites that you want to block access to.To block a client in your network in this way, check the 'Block with URL Filters' box in the rule you defined for that client in 'Access Control' page..

Anti-DoS

The Anti-DOS feature prevents "Denial of Service" attacks that aim to disable your router by flooding it with connection requests. On this page, you can set the maximum number of connections that will be allowed from the Internet for a specified time interval for each protocol.

Anti-DOS is enabled by default.



Anti-DOS

The Anti-DoS feature blocks Denial of Service attacks to your modem. In this page, you can determine the maximum number of allowed connections for discrete protocols over a certain time.

☑ Enabled Anti-Dos

wan-0

☑ Antidos Enabled

TCP	Per Second	100	new connection
UDP	Per Second	150	new connection
ICMP	Per Second	2	new connection

wan-1

☑ Antidos Enabled

TCP	Per Second	100	new connection
UDP	Per Second	150	new connection
ICMP	Per Second	2	new connection

lan-0

☑ Antidos Enabled

TCP	Per Second	1000	new connection
UDP	Per Second	1000	new connection
ICMP	Per Second	10	new connection

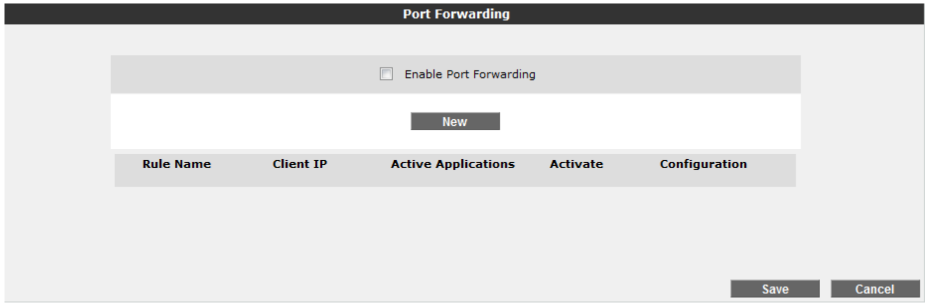
NAT

Network Address Translation (NAT) is a way to map an entire network to a single IP address. NAT allows multiple clients in your local network to access the Internet through a single global IP address assigned to you by your Internet Service Provider. NAT is commonly used together with Port Forwarding.

Port Forwarding

Port Forwarding is used in order for a host outside your local network to access a machine on your local network.

1. To enable Port Forwarding on a port, go to the "NAT" menu on the left menu bar of the Web interface of your device and click "Port Forwarding".
2. Check "Enable Port Forwarding".

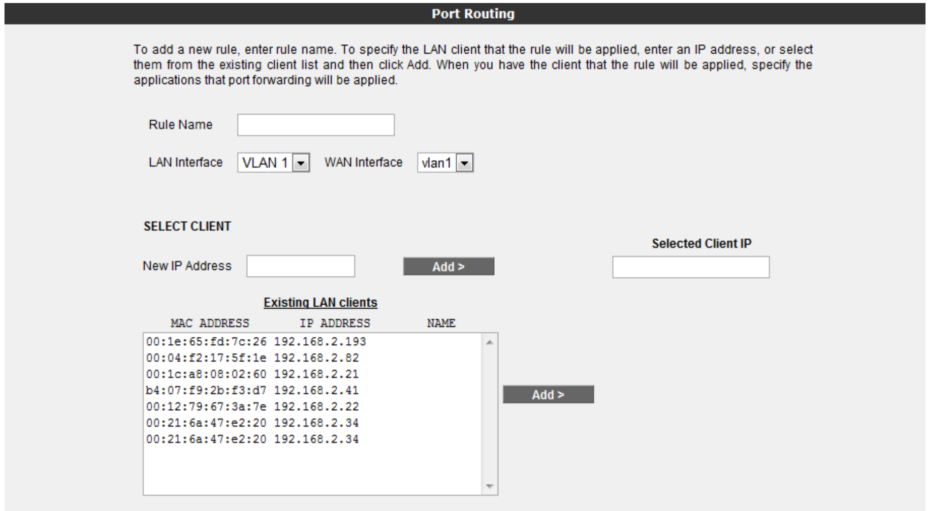


Port Forwarding

□ Enable Port Forwarding

Rule Name	Client IP	Active Applications	Activate	Configuration

" Click "New" to forward a port. " In the "Rule Name" field, assign a name for the Port Forwarding rule you are creating. " If use are using VLANs then select the VLAN that you want to apply the port forwarding rule for. If you are not using VLANs then take the default values. " Either select the client from the list of existing LAN clients or enter the IP address in the "New IP Address" field. Click "Add >"



Port Routing

To add a new rule, enter rule name. To specify the LAN client that the rule will be applied, enter an IP address, or select them from the existing client list and then click Add. When you have the client that the rule will be applied, specify the applications that port forwarding will be applied.

Rule Name

LAN Interface: VLAN 1 WAN Interface: vlan1

SELECT CLIENT

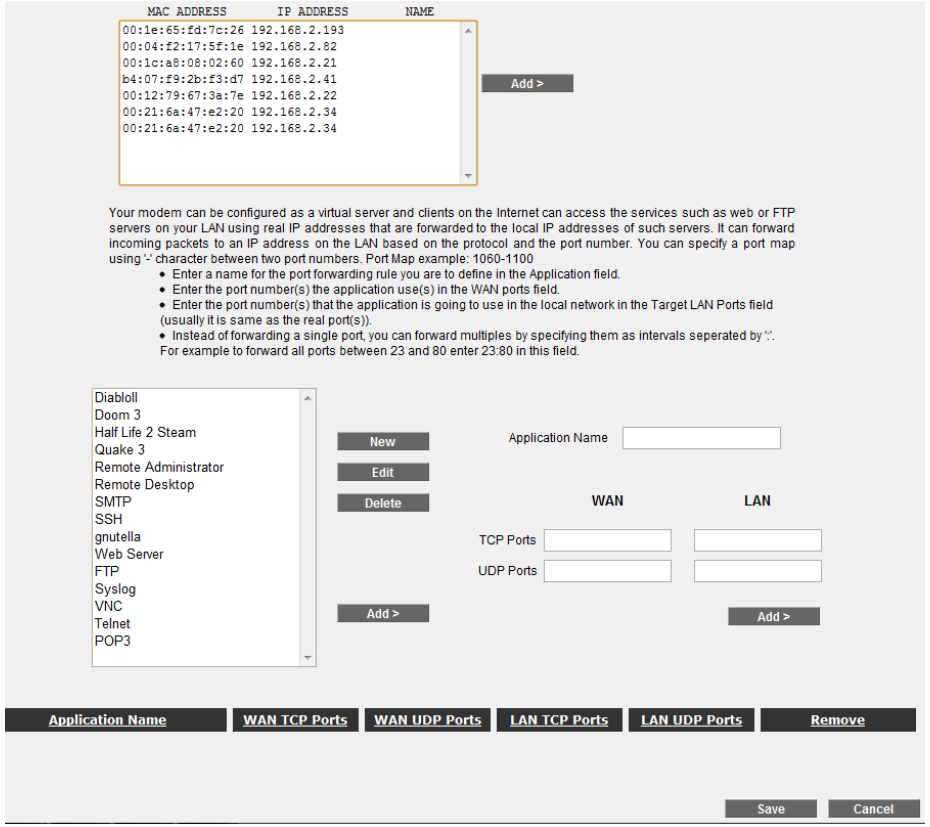
New IP Address

Selected Client IP

Existing LAN clients

```
  MAC ADDRESS       IP ADDRESS       NAME
00:1e:65:fd:7c:26 192.168.2.193
00:04:f2:17:5f:1e 192.168.2.82
00:1c:a8:08:02:60 192.168.2.21
b4:07:f9:2b:f3:d7 192.168.2.41
00:12:79:67:3a:7e 192.168.2.22
00:21:6a:47:e2:20 192.168.2.34
00:21:6a:47:e2:20 192.168.2.34
```

" From the Application List, select the application that want to use for port forwarding. If it is not present then you will manually enter the port configuration. " Enter an Application Name. " Enter the real port number used by the application in the WAN fields. " Enter the local port number for the application in the LAN fields, this can be the same as the Real Port. " To forward a range of ports instead of a single port, use a dash (-) sign in between. For example to forward all ports between 23 and 80, enter "23-80". " Click "Save" to save the port forwarding rule.



MAC ADDRESS	IP ADDRESS	NAME
00:1e:65:fd:7c:26	192.168.2.193	
00:04:f2:17:5f:1e	192.168.2.82	
00:1c:a8:08:02:60	192.168.2.21	
b4:07:f9:2b:f3:d7	192.168.2.41	
00:12:79:67:3a:7e	192.168.2.22	
00:21:6a:47:e2:20	192.168.2.34	
00:21:6a:47:e2:20	192.168.2.34	

Your modem can be configured as a virtual server and clients on the Internet can access the services such as web or FTP servers on your LAN using real IP addresses that are forwarded to the local IP addresses of such servers. It can forward incoming packets to an IP address on the LAN based on the protocol and the port number. You can specify a port map using '-' character between two port numbers. Port Map example: 1060-1100

- Enter a name for the port forwarding rule you are to define in the Application field.
- Enter the port number(s) the application use(s) in the WAN ports field.
- Enter the port number(s) that the application is going to use in the local network in the Target LAN Ports field (usually it is same as the real port(s)).
- Instead of forwarding a single port, you can forward multiples by specifying them as intervals seperated by ':'. For example to forward all ports between 23 and 80 enter 23:80 in this field.

Diabloll
Doom 3
Half Life 2 Steam
Quake 3
Remote Administrator
Remote Desktop
SMTP
SSH
gnutella
Web Server
FTP
Syslog
VNC
Telnet
POP3

Application Name

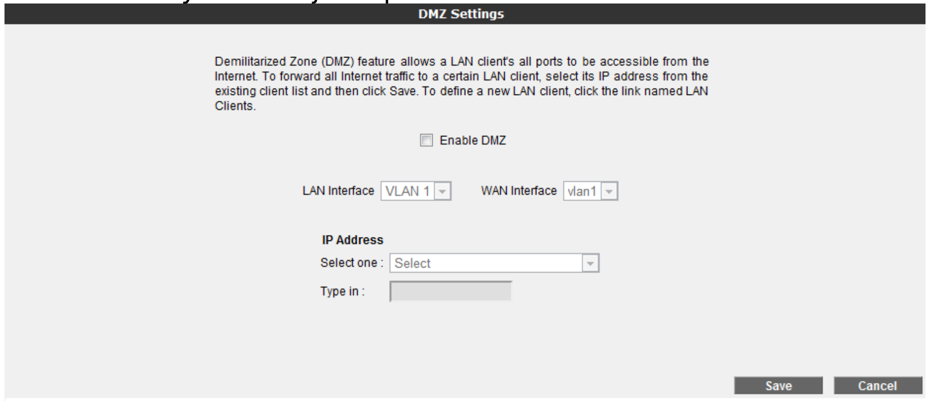
	WAN	LAN
TCP Ports		
UDP Ports		

Application Name	WAN TCP Ports	WAN UDP Ports	LAN TCP Ports	LAN UDP Ports	Remove

DMZ

The DeMilitarized Zone (DMZ) feature opens up all of the ports of a single local network host for unrestricted access from the Internet.

On your router DMZ is disabled by default. To enable DMZ go to the DMZ sub-menu under NAT menu of the Web UI. Check the Enable DMZ checkbox. Select the LAN and WAN interfaces. Select an IP address from the drop down menu where data will be forwarded to. Click Save to save your changes. From now all data sent to your WAN IP address (no matter what port) will be forwarded to the IP address that you have just specified.



DMZ Settings

Demilitarized Zone (DMZ) feature allows a LAN client's all ports to be accessible from the Internet. To forward all Internet traffic to a certain LAN client, select its IP address from the existing client list and then click Save. To define a new LAN client, click the link named LAN Clients.

☐ Enable DMZ

LAN Interface: VLAN 1   WAN Interface: vlan1

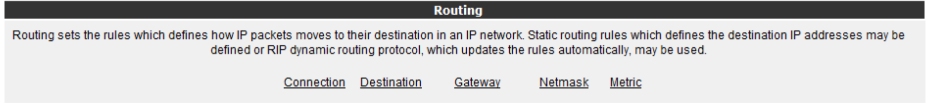
IP Address
Select one : Select
Type in :

ROUTING

Routing defines the rules which determine how IP packets reach their destination on the Internet. Rules can either by automatically created by using the Routing Informaton Protocol (RIP) or rules can be manualy created. By default your device is configured to automatically create routing rules.

Static Routing

If you want to manually create routing rules then go to the ROUTING menu. A list of static routing rules will be displayed.

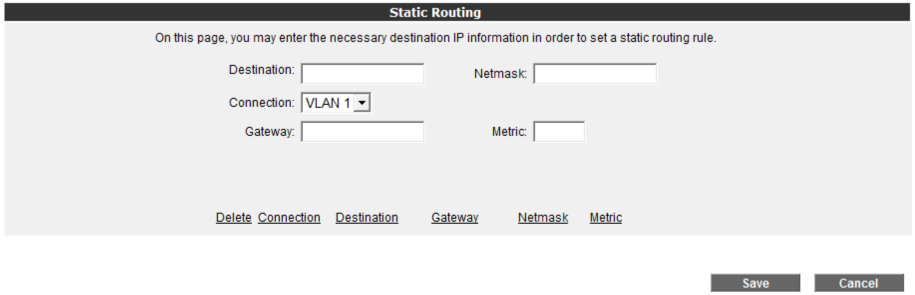


Routing

Routing sets the rules which defines how IP packets moves to their destination in an IP network. Static routing rules which defines the destination IP addresses may be defined or RIP dynamic routing protocol, which updates the rules automatically, may be used.

Connection	Destination	Gateway	Netmask	Metric

To create a static rule select Static Routing option from the ROUTING menu.


Static Routing

On this page, you may enter the necessary destination IP information in order to set a static routing rule.

Destination:		Netmask:	
Connection:	VLAN 1		
Gateway:		Metric:	

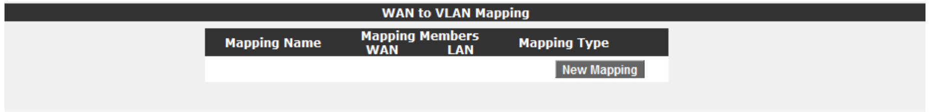
Delete	Connection	Destination	Gateway	Netmask	Metric

You need to enter a destination IP address and the route that will be taken to get there: Desitnation: Enter the IP address of the destinaton Netmark: Enter the netmask for the destination IP address. Connection: Select the network interface where the data will be sent. Gateway: Enter the IP address of the host that can transfer the data for the destination IP address. Metric: Specifiy the number of hops (how many gateways) the data needs to travel through. Click Save to save the static route. The static route will be displayed in the list. The static can be deleted by checking the delete checbox.

If your device supported WAN to VLAN Mapping, follow next steps below.

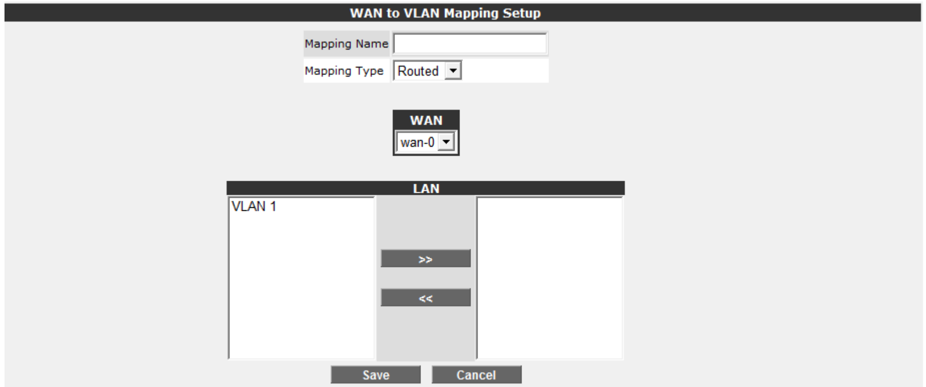
WAN to VLAN Mapping

It is possible to creating mappings to allow data from the different WANs to be sent to differernt VLANs on your LAN. To create a new WAN to VLAN mappig go to the WAN and VLAN Mappings menu under ROUTING menu.


WAN to VLAN Mapping

Mapping Name	Mapping Members WAN	 LAN	Mapping Type

Click NEW MAPPING.


WAN to VLAN Mapping Setup

Mapping Name	
Mapping Type	Routed

WAN: wan-0

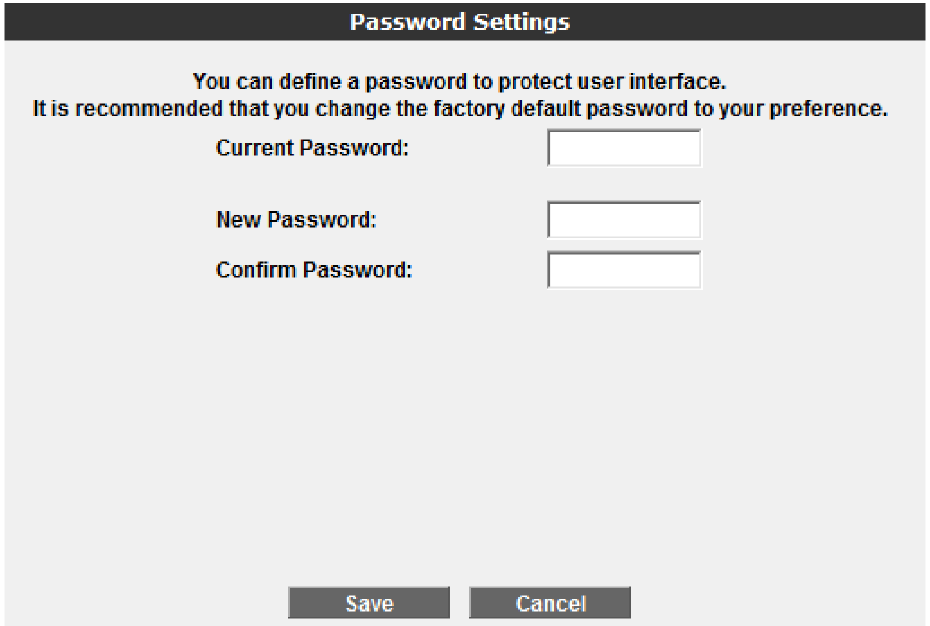
LAN: VLAN 1

Mapping Name: Give the mapping a name. Mapping Type: Select either Routed or Bridged. WAN: Select a WAN interface from the list. LAN: Select one or more LAN interfaces. Click Save to save your settings.

MANAGEMENT

From the MANAGEMENT menu you can configure how the device is managed.

To change the password used to protect the Web UI. Select Password Settings.



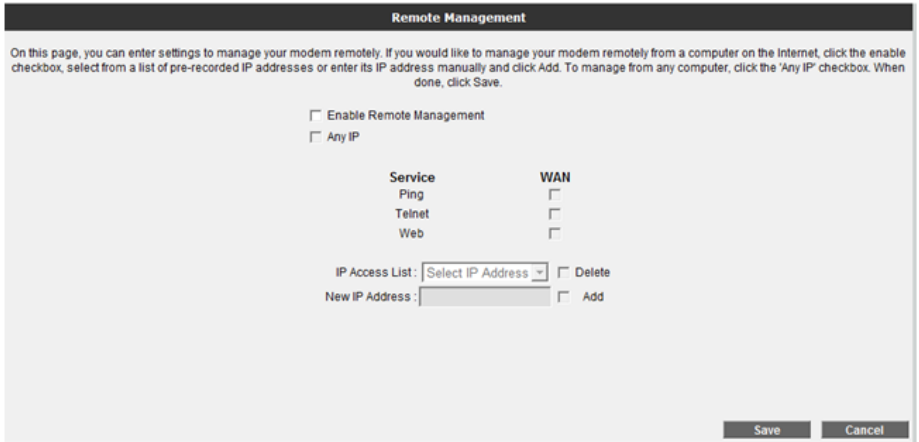
Password Settings

You can define a password to protect user interface.
It is recommended that you change the factory default password to your preference.

Current Password:	
New Password:	
Confirm Password:	

Enter the current password and the new password twice. Select Save to save your settings. The new password will be required next time you access the device settings. AirTies Network Assistant will also request this password to allow for the device to be monitored and managed.

To allow remote management from the Internet select Remote Management.



Remote Management

On this page, you can enter settings to manage your modem remotely. If you would like to manage your modem remotely from a computer on the Internet, click the enable checkbox, select from a list of pre-recorded IP addresses or enter its IP address manually and click Add. To manage from any computer, click the 'Any IP' checkbox. When done, click Save.

□ Enable Remote Management
□ Any IP

Service	WAN
Ping	□
Telnet	□
Web	□

IP Access List : Select IP Address □ Delete
New IP Address : □ Add

Please note that allowing remote management should only be performed by experienced users. To enable remote management of your device, first click the "Enable Remote Management" check box. If you check the "Any IP" box, your router can be managed remotely from any computer that has a WAN IP.

If "Any IP" is not checked, you have to add the WAN IP address of the computer from which you would like to remotely manage your device to the "IP Access List". To do this, enter the WAN IP address in the "New IP Address" field and click the "Add" box.

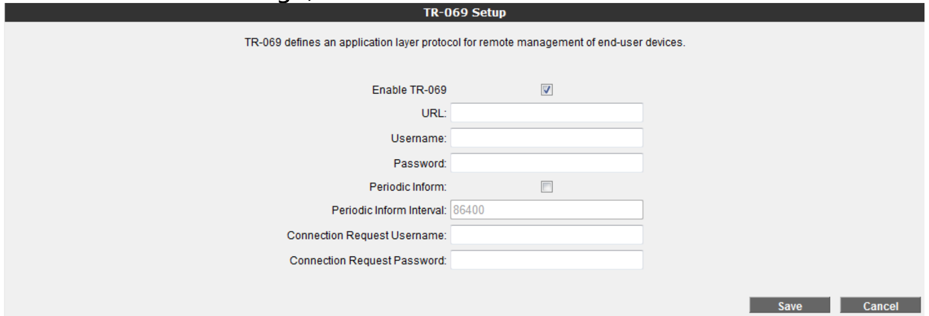
After saving, the WAN IP address you have entered will appear in the "IP Access List". If you select this address from the list and click "Save", remote management will be activated for this address. If you want to remove an IP address from the list, select the address from the list, click on the "Delete" checkbox and then click "Save".

You can also specify which services will be available to the remote management computers on this page.

TR-069 defines an application layer protocol for remote management of end-user devices. With TR-069, all kind of settings that you can do with local area network connection, can be set automatically with auto-configuration server (ACS). Click "TR-069" submenu from the "MANAGEMENT" for doing automatically configuration.

- Enable TR-069: To enable TR-069 protocol, click "Enable TR-069" check box.
- URL:Auto-configuration address (ACS)that your device will connect. (It is given by the ACS provider to the user.)
- Username: The username that must be entered for connecting to (ACS) the automatic configuration server. (It is given by the ACS provider to the user.)
- Password: The password that must be entered for connecting to (ACS) the automatic configuration server. (It is given by the ACS provider to the user.)
- Periodic Inform Interval: This shows that the device and (ACS) auto-configuration server's reciprocal link status and time in seconds of controlling intervals. This time is set to 86400 sn by default in your device.
- Connection Request Username: The username that auto-configuration server (ACS) must use when connecting to the device.
- Connection Request Password: The password that auto-configuration server (ACS) must use when connecting to the device.

After all these settings, click "Save".



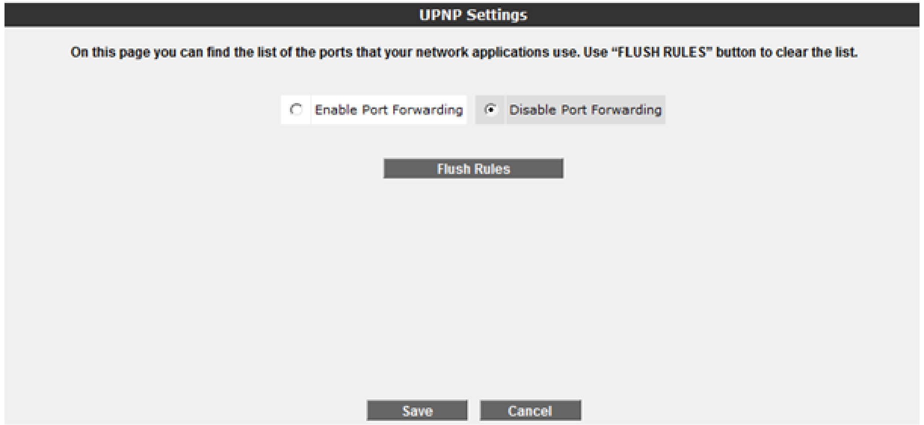
TR-069 Setup

TR-069 defines an application layer protocol for remote management of end-user devices.

Enable TR-069 ☑
URL:
Username:
Password:
Periodic Inform: □
Periodic Inform Interval: 86400
Connection Request Username:
Connection Request Password:

UPNP

Universal Plug and Play is a protocol that allows devices on the network automatically interoperate with each other. To enable UPnP port forwarding select UPNP Settings under the UPNP menu.



UPNP Settings

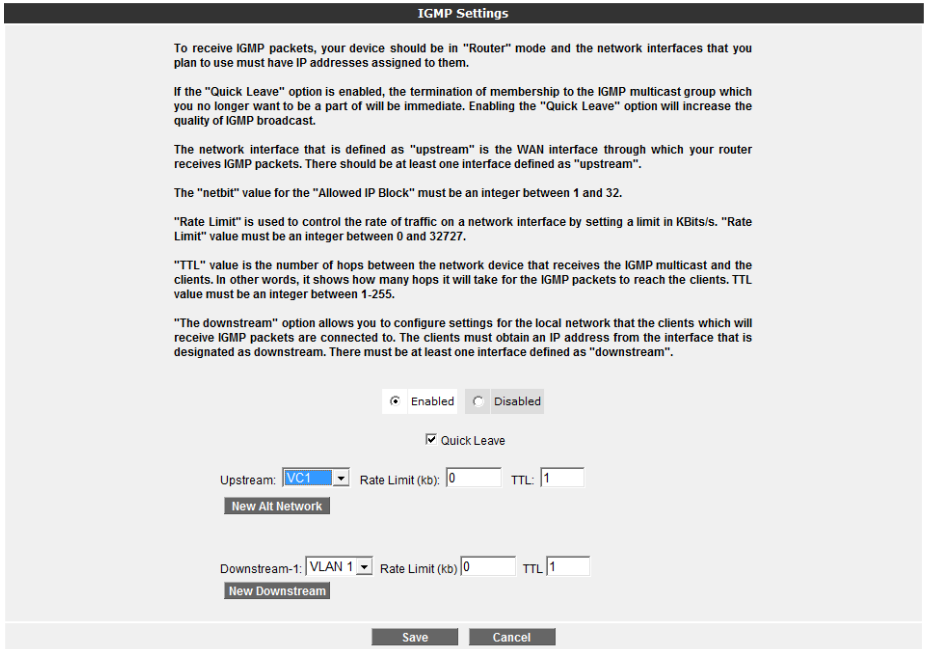
On this page you can find the list of the ports that your network applications use. Use "FLUSH RULES" button to clear the list.

○ Enable Port Forwarding ● Disable Port Forwarding

Select Enable Port Forwarding. Click Save to save your settings.

IGMP

IGMP settings are required if you want to use an IPTV service on your home network. To enable and configure IGMP go to the IGMP menu on your Web UI. Check Enable.



IGMP Settings

To receive IGMP packets, your device should be in "Router" mode and the network interfaces that you plan to use must have IP addresses assigned to them.

If the "Quick Leave" option is enabled, the termination of membership to the IGMP multicast group which you no longer want to be a part of will be immediate. Enabling the "Quick Leave" option will increase the quality of IGMP broadcast.

The network interface that is defined as "upstream" is the WAN interface through which your router receives IGMP packets. There should be at least one interface defined as "upstream".

The "netbit" value for the "Allowed IP Block" must be an integer between 1 and 32.

"Rate Limit" is used to control the rate of traffic on a network interface by setting a limit in KBits/s. "Rate Limit" value must be an integer between 0 and 32727.

"TTL" value is the number of hops between the network device that receives the IGMP multicast and the clients. In other words, it shows how many hops it will take for the IGMP packets to reach the clients. TTL value must be an integer between 1-255.

"The downstream" option allows you to configure settings for the local network that the clients which will receive IGMP packets are connected to. The clients must obtain an IP address from the interface that is designated as downstream. There must be at least one interface defined as "downstream".

● Enabled ○ Disabled

☑ Quick Leave

Upstream: VC1 Rate Limit (kb): 0 TTL: 1

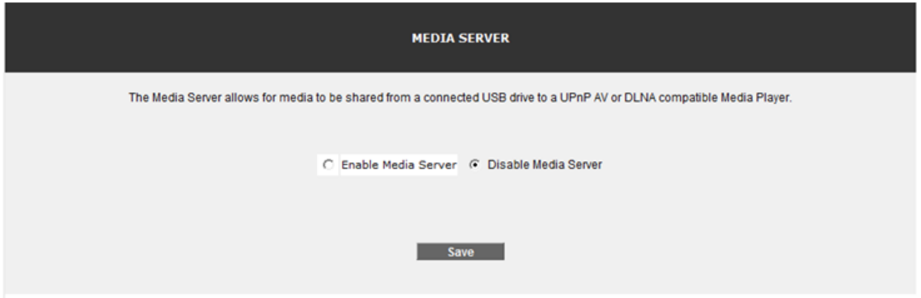
Downstream-1: VLAN 1 Rate Limit (kb) 0 TTL 1

Check Quick Leave if you want to enable immediate termination of IGMP multicast group. This will improve the quality of your IGMP broadcast. Select the upstream network interface. This is the WAN interface that that your router will receive IGMP packets with. There must be at least one interface defined as upstream. The Rate Limit sets a limit on the rate of data on the network interface. This must be a value between 0 and 32727. The TTL value is the number of hops on the network between the network device and the client that will receive the IGMP packets. This must be a value between 1 and 255. The downstream network interface is the LAN interface that the client receiving IGMP data is connected to. At least one downstream network interface must be selected and Rate Limit and TTL set.

AirTies Media Server

The Media Server will share videos, music and photos from a USB disk attached to the Air device's USB port. Media can be viewed on a DLNA / UPnP AV compatible Media Player, which is connected to the same network as the AirTies device, by locating the AirTies media server named Airxxxx, where xxxx is the product number, and browsing and playing the contents. Media Server can be configured from the Web interface of your device:

1. Go to the "MEDIA SERVER" menu of your device. From here you can enable or disable the Media Server. By default the Media Server is enabled.



MEDIA SERVER

The Media Server allows for media to be shared from a connected USB drive to a UPnP AV or DLNA compatible Media Player.

○ Enable Media Server ● Disable Media Server

2. Click "Save" to complete the Media Server settings for your device.

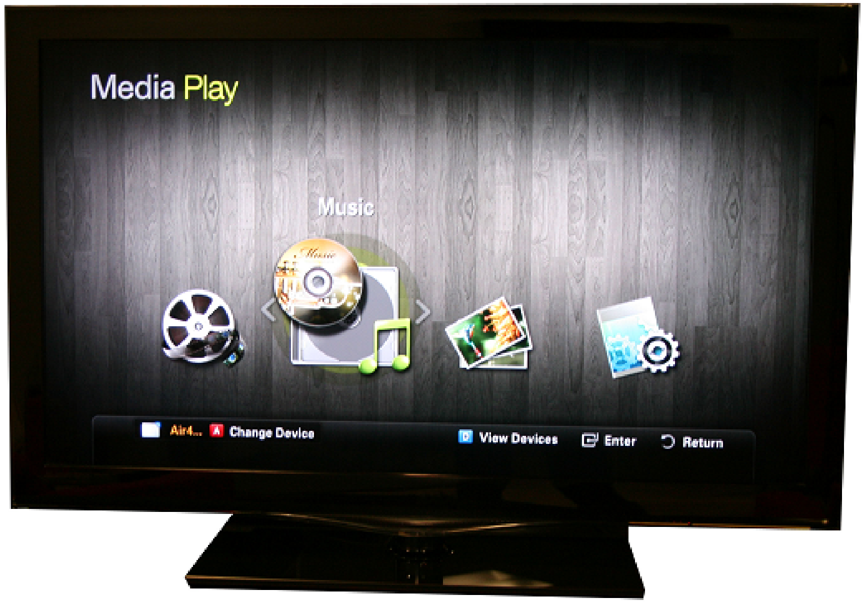
Note that the Media Server requires a USB disk to be inserted into the USB port of your device otherwise the service will not be enabled.

The contents of the drive can be managed using AirTies Network Assistant or via a network path (see USB Host instructions). Any new media placed on the drive will be shared by the Media Server.

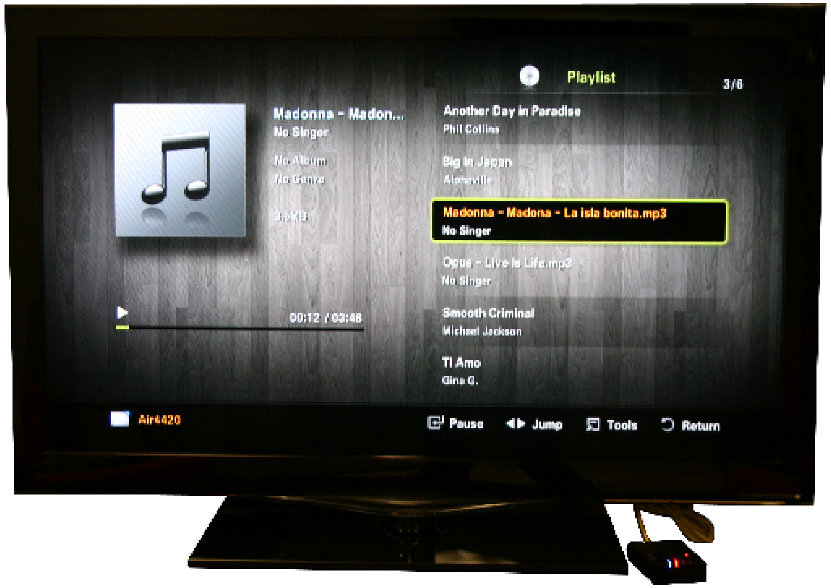
Media Servers include DLNA / UPnP AV compatible TVs, Set Top Boxes, Blue-ray player and PlayStation 3s. Connect your DLNA / UPnP AV player to the same network as your AirTies device.

For Samsung DLNA compatible TVs

Turn on the TV and press the MEDIA.P or W.LINK button on your remote control.



On the Media Player menu on your TV you will see Photo, Video and Music icons. Under each of these you will see the AirTies device. Select the AirTies device to list the media that is contained on the attached USB disk. Selecting a Photo, Video or Music file will play or display the media on the television.



You can stop the media by pressing the 'stop' button on your remote control.

For Sony PlayStation 3

Turn on the PlayStation 3, Media Servers on the same network are automatically detected and icons for the detected servers are displayed under Photo, Music and Video icons.

Select the AirTies device to list the media that is contained on the attached USB disk.

Selecting a Photo, Video or Music file will play or display the media on the television. You can stop the media by pressing the circle button on your controller. For movies you can see thumbnails of the movie by pressing the square button on your controller. You can skip to the movie by selecting the thumbnail and pressing the X button on your controller.

Top Gear - [14x01] - 2009.11.15 [FoV].avi.files
30/1 9:57
Eyyvah.Eyvah.2009.DVD.XviD.avi
Peter and the wolf.avi
Sleeper Cell - 1x07 - Immagrant.avi
Top Gear - [14x01] - 2009.11.15 [FoV].avi
Yahsi Bati DVDRip XviD-LTRG.avi
: Options

If you cannot see any devices or files you may need to scan for the DLNA devices which are on the network. To do this select 'search for Media Servers' under either the Photo, Music or Video icons.

For Sony Bravia DLNA compatible televisions

Turn on your TV and press the 'home' button on your remote control to open the media menu.

Scroll across the media menu and you will see Photo, Video and Music icons. Under each of these you will see the AirTies device. Select the AirTies device to list the media that is contained on the attached USB disk. Selecting a Photo, Video or Music file will play or display the media on the television.

You can stop the media by pressing the 'stop' button on your remote control.

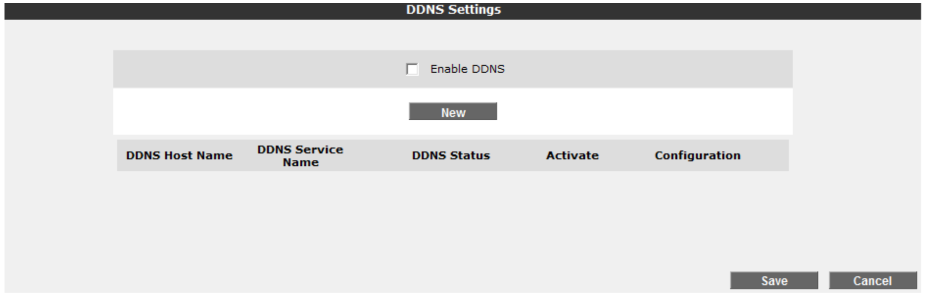
If you cannot see any devices or files you may need to scan for the DLNA devices which are on the network. To do this, go to 'Settings' menu then scroll to 'Network Settings' > 'Server Display Settings' and then press 'Options' on your remote and select 'Update list'. The television will scan the network and find your AirTies Media Server.

The files that can be played on your Media Player depends upon the codec and file container support offered by your Media Player. Please consult your Media Player's documentation for a list of codecs and file containers that it supports.

AirTies Media Server has been tested for interoperability on a number of Media Players. Please visit www.airties.com for a current list of tested devices.

DDNS

Dynamic DNS (DDNS) ensures that your hostname and IP address in the Internet name servers are always current. It's primarily used to associate a domain name with a dynamic IP address, making it possible to access a computer with a dynamic IP address over the Internet. This also allows you to run a server on a computer that has a dynamic IP address. DDNS Settings To configure the DDNS settings on your device go to DNS Settings under the DDNS menu of the Web User Interface. You will see the current DDNS account information if one is present.

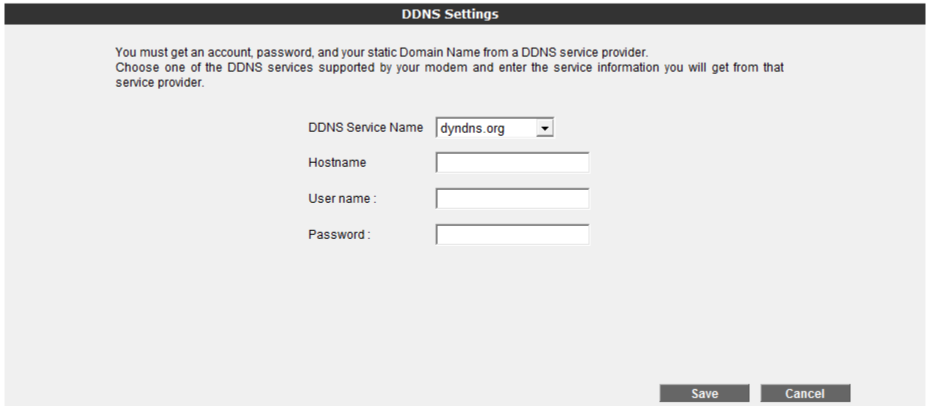


DDNS Settings

☐ Enable DDNS

DDNS Host Name	DDNS Service Name	DDNS Status	Activate	Configuration

To use the Dynamic DNS feature you need to setup an account with a DDNS service provider. To create a new DDNS account click New.

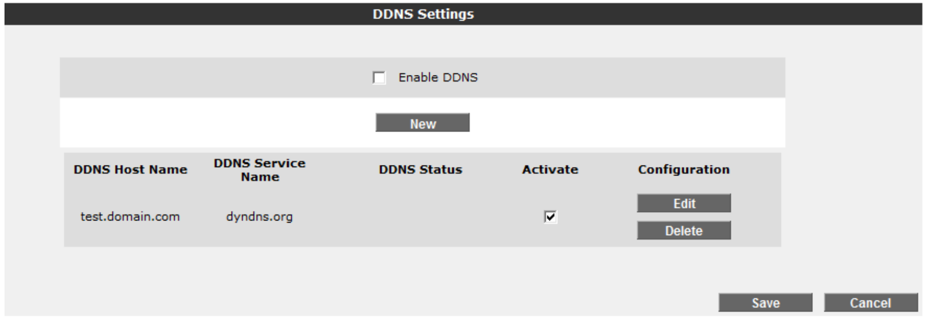


DDNS Settings

You must get an account, password, and your static Domain Name from a DDNS service provider. Choose one of the DDNS services supported by your modem and enter the service information you will get from that service provider.

DDNS Service Name: dyndns.org
Hostname:
User name :
Password :

Enter the following information DDNS Service Name: Select the DDNS service provider. Hostname: Your hostname you want to associate with your dynamic IP address. User name: The username provider from your DDNS service provider. Password: The password provider from your DDNS service provider. Click Save to create the DDNS account. You will return to the DDNS Settings page again will see your DDNS account and status. You can add additional DDNS accounts or can edit and remote DDNS accounts.



DDNS Settings

☐ Enable DDNS

New

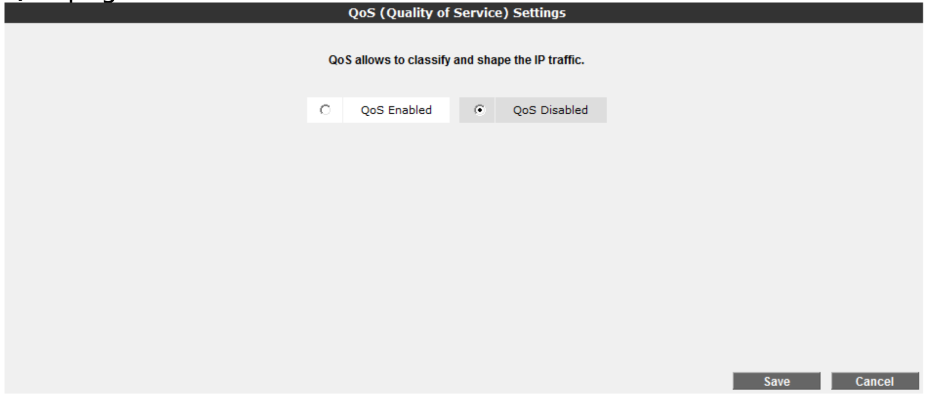
DDNS Host Name	DDNS Service Name	DDNS Status	Activate	Configuration
test.domain.com	dyndns.org		☑	Edit Delete

Save Cancel

To enable DDNS check the Enable DDNS check box and click Save.

QoS

Quality Of Service (QoS) allows you to pioritise data for certain applications to get the best possible service for these applications. Applications that are time senstive to the data the receive, such as IPTV or VOIP, require QoS to be configured. To enable QoS go to the QoS page on the Web UI.



QoS (Quality of Service) Settings

QoS allows to classify and shape the IP traffic.

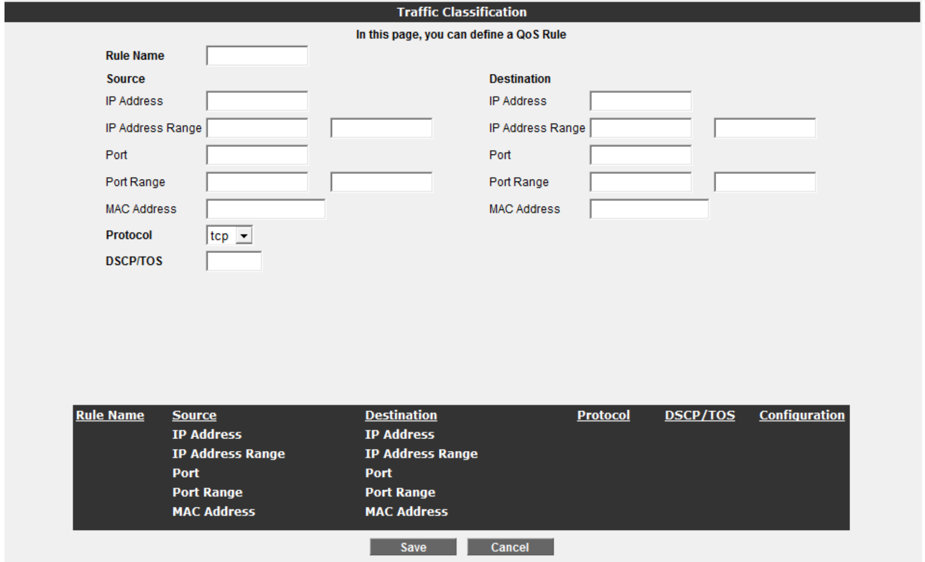
○ QoS Enabled ● QoS Disabled

Save Cancel

Select QoS Enabled to enable QoS and click Save.

Traffic Classification

Rules can be created to classify data. To create, edit or delete rules to to Traffic Classification under QoS option on the menu. To create a new rule add some of the following information in the fields.



Traffic Classification

In this page, you can define a QoS Rule

Rule Name					
Source			Destination		
IP Address			IP Address		
IP Address Range			IP Address Range		
Port			Port		
Port Range			Port Range		
MAC Address			MAC Address		
Protocol	tcp				
DSCP/TOS					

Rule Name	Source	Destination	Protocol	DSCP/TOS	Configuration
	IP Address IP Address Range Port Port Range MAC Address	IP Address IP Address Range Port Port Range MAC Address			

Save Cancel

Rule Name Source: Enter a rule name for the rule

IP Address: Enter the source address that the data will come from.

IP Address Range: Enter a range of addresses that the data will come from.

Port: Enter the source port that the data will come from.

Port Range: Enter a range of ports that the data will come from.

MAC Address Destination: Enter the source MAC address that the data will come from.

IP Address: Enter the destination address that the data will be sent to.

IP Address Range: Enter a range of addresses that the data will be sent to.

Port: Enter the destination port that the data will be sent to.

Port Range: Enter a range of ports that the data will be sent to.

MAC Address: Enter the destination MAC address that the data will be sent to.

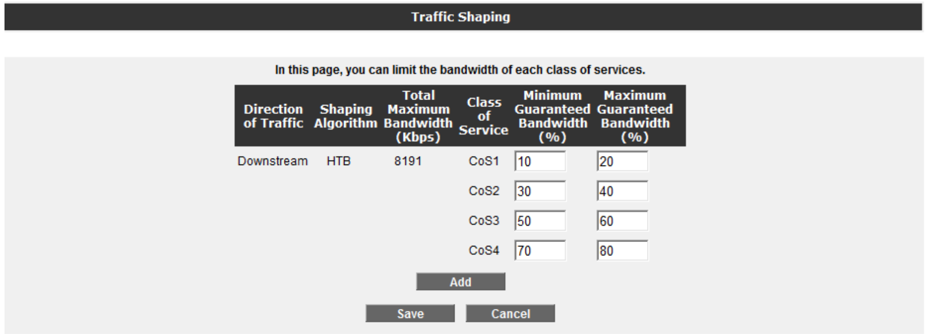
Protocol: Enter the protocol of the data

DSCP/TOS: Enter the QoS values that the data will have.

Click Save to create a new rule. The rule will appear in the table.

Traffic Shaping

In the traffic shaping page you can limit the bandwidth of each Class of Service. Go to the Traffic Shaping menu under the QoS menu.



Traffic Shaping

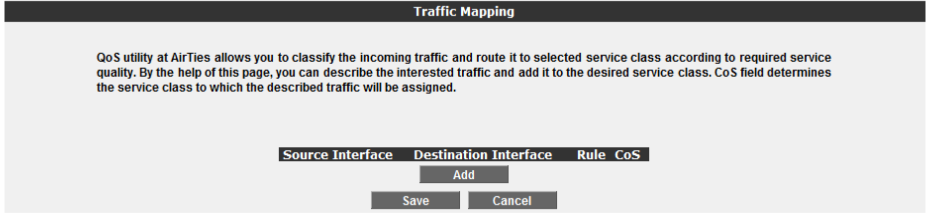
In this page, you can limit the bandwidth of each class of services.

Direction of Traffic	Shaping Algorithm	Total Maximum Bandwidth (Kbps)	Class of Service	Minimum Guaranteed Bandwidth (%)	Maximum Guaranteed Bandwidth (%)
Downstream	HTB	8191	CoS1	10	20
			CoS2	30	40
			CoS3	50	60
			CoS4	70	80

There are already four Class of Services defined. The bandwidth for each Class of Service is limited so that CoS4 is guaranteed the highest amount of bandwidth. The minimum and maximum amount of bandwidth of each CoS can be changed. Please note that changing these is only recommended for advanced users. Additional Class of Service can be created by clicking Add. The minimum and maximum guaranteed bandwidth should be entered. Click Save to save your settings.

Traffic Mapping

Traffic Mapping is where rules are matched to Class of Services. Select Traffic Mapping from the QoS menu.

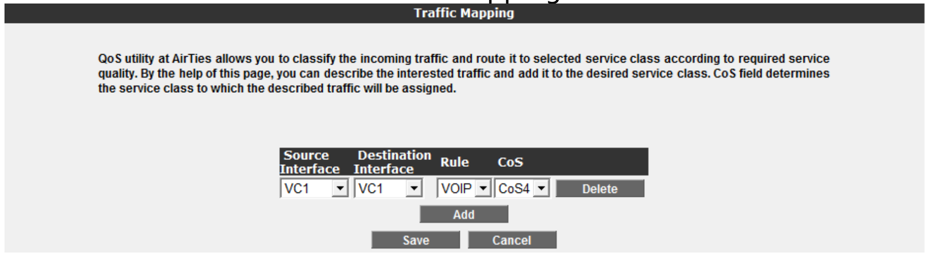


Traffic Mapping

QoS utility at AirTies allows you to classify the incoming traffic and route it to selected service class according to required service quality. By the help of this page, you can describe the interested traffic and add it to the desired service class. CoS field determines the service class to which the described traffic will be assigned.

Source Interface	Destination Interface	Rule	CoS

Click Add to create a new Traffic Mapping.



Traffic Mapping

QoS utility at AirTies allows you to classify the incoming traffic and route it to selected service class according to required service quality. By the help of this page, you can describe the interested traffic and add it to the desired service class. CoS field determines the service class to which the described traffic will be assigned.

Source Interface	Destination Interface	Rule	CoS	
VC1	VC1	VOIP	CoS4	Delete

Enter the following information:

Source Interface: The interface on the device where the data is coming from. For incoming traffic this will be a WAN interface and for outgoing traffic this be a LAN interface.

Destination Interface: The interface on the device where the data is going to. For incoming traffic this will be a LAN interface and for outgoing traffic this be a WAN interface.

Rule: Select a rule that you previously configured on the Traffic Classification page.

Cos: Select a Class of Service.

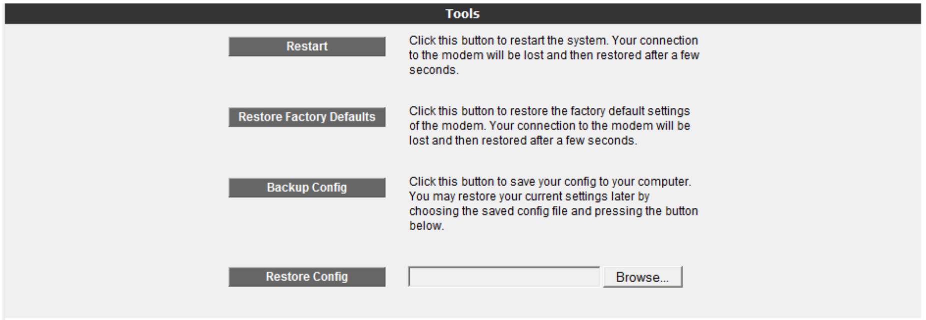
Click Save to save your settings.

Traffic to and from the specified interfaes that match the rule will be prioritieed bandwidth according to the Class of Service.

Tools

On this page, you can restart your device, reset it to factory defaults, backup its current configuration or restore from a previous backup. To get to the Tools screen, select TOOLS from the main menu of the Web interface. * The Restart button restarts your router remotely. During this operation, your connection to the router will be lost. You can reconnect after the router comes back up. * The Restore Factory Defaults button allows you to reset your router back to factory defaults remotely. This will clear all the current settings on your router. * Backup Config lets you save the current settings of your router onto your computer. When you click the Backup Config button, your router will create a file called config.bin to be saved on your computer. You can restore this configuration later using the Restore Config button.

- Restore Config lets you restore a previously saved configuration onto your router. Click the Browse button to locate the config.bin file that was previously saved, and then press the Restore Config button to restore your settings from this file onto your router.



Click this button to restart the system. Your connection to the modem will be lost and then restored after a few seconds.

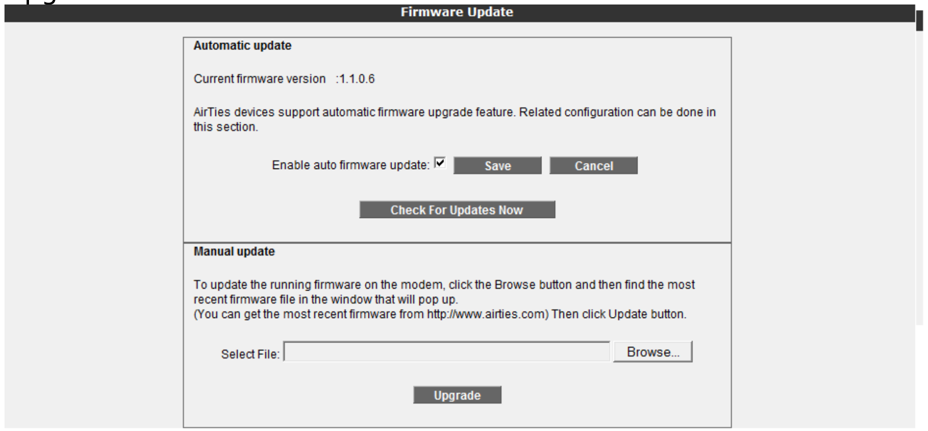
Click this button to restore the factory default settings of the modem. Your connection to the modem will be lost and then restored after a few seconds.

Click this button to save your config to your computer. You may restore your current settings later by choosing the saved config file and pressing the button below.

Firmware Update

Your device is configured to automatically check for updates and update itself if it finds an update. The process to check for updates approximately every 30 days. By default this is enabled. You can disable this by unchecking the Enable auto firmware update and clicking Save. You can check for updates by clicking Check For Updates Now. The device will contact AirTies to see if there are updates. If there are updates then they will be downloaded and the device will upgrade. After the firmware is successfully installed, the system will restart automatically. Therefore, connection to the device will be lost. You will need to reconnect if you would like to reconfigure any settings. Your router must stay ON during the upgrade.

If you want to manually update the firmware running on the device, go to Firmware Upgrade under the TOOLS menu. Click Browse and locate the most recent router firmware file on your computer in the pop-up window that appears. (You can download the most recent firmware file from the AirTies website www.airties.com). Then click Upgrade.



Current firmware version :1.1.0.6

AirTies devices support automatic firmware upgrade feature. Related configuration can be done in this section.

Enable auto firmware update: ☑

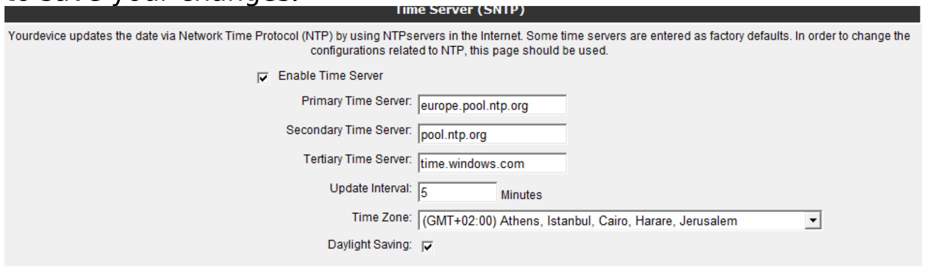
To update the running firmware on the modem, click the Browse button and then find the most recent firmware file in the window that will pop up.
(You can get the most recent firmware from http://www.airties.com) Then click Update button.

Select File:

After the firmware is successfully installed, the system will restart automatically. Therefore, connection to the device will be lost. You will need to reconnect if you would like to reconfigure any settings. Your router must stay ON during the upgrade.

Time Setting

Your device gets the current time and date from Internet time servers using SNTP protocol. Default factory settings include some time servers. To change the time servers used by your device go to Time Settings under the TOOLS menu. In the Time Server (SNTP) window that come up, enter the time server information. Click Save to save your changes.



Time Server (SNTP)

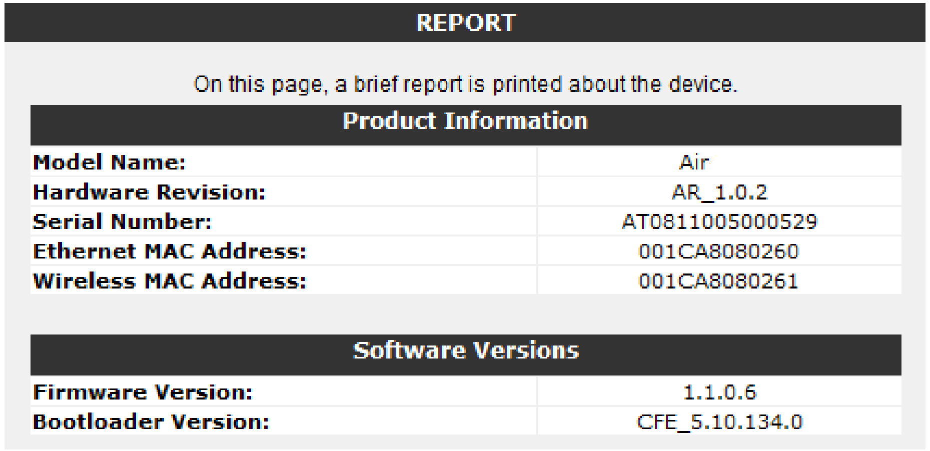
Yourdevice updates the date via Network Time Protocol (NTP) by using NTPservers in the Internet. Some time servers are entered as factory defaults. In order to change the configurations related to NTP, this page should be used.

☑ Enable Time Server

Primary Time Server:	europe.pool.ntp.org
Secondary Time Server:	pool.ntp.org
Tertiary Time Server:	time.windows.com
Update Interval:	5 Minutes
Time Zone:	(GMT+02:00) Athens, Istanbul, Cairo, Harare, Jerusalem
Daylight Saving:	☑

REPORT

The REPORT menu displays information about the main characteristics of your device such as product information and software versions.



REPORT

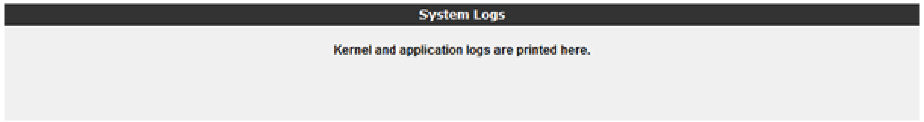
On this page, a brief report is printed about the device.

Product Information	
Model Name:	Air
Hardware Revision:	AR_1.0.2
Serial Number:	AT0811005000529
Ethernet MAC Address:	001CA8080260
Wireless MAC Address:	001CA8080261

Software Versions	
Firmware Version:	1.1.0.6
Bootloader Version:	CFE_5.10.134.0

System Logs

The System Logs under REPORT menu displays detailed system logs about the system activity and the applications that were active since the device last started.

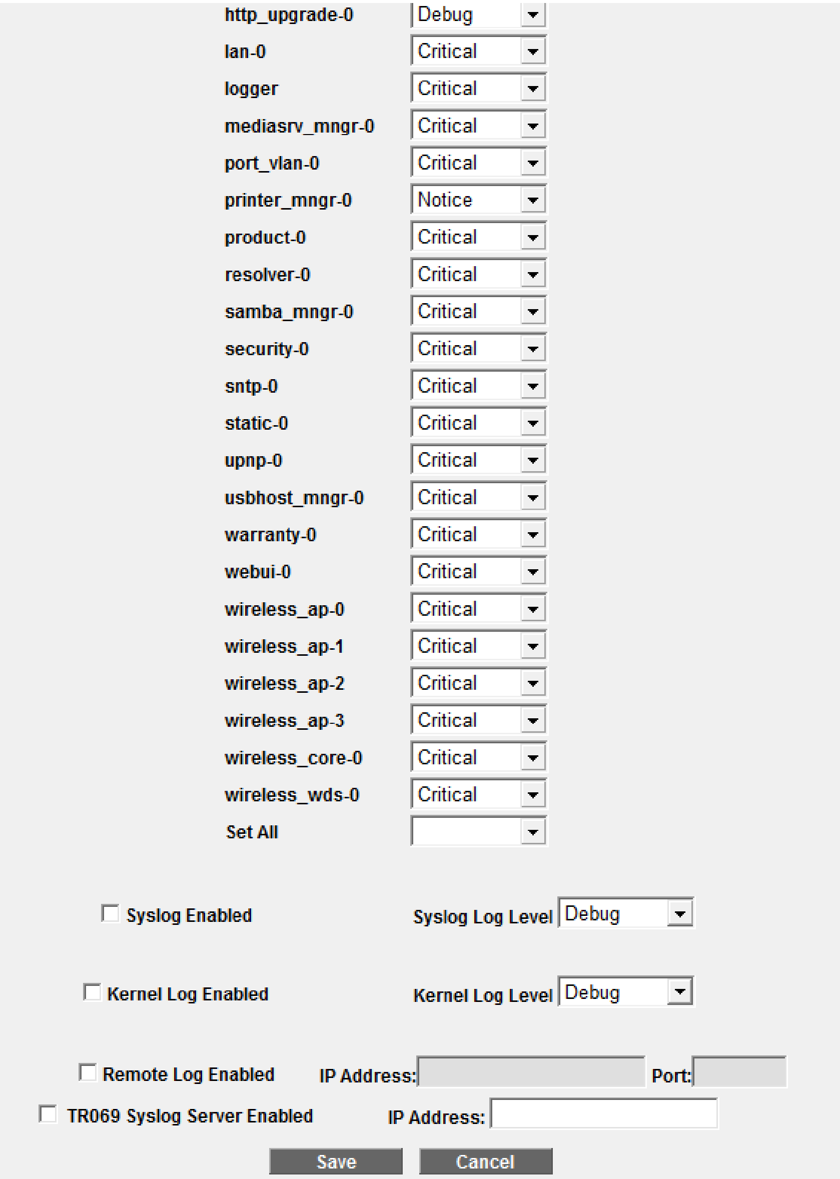


System Logs

Kernel and application logs are printed here.

Log Settings

Log Settings screen allows you to set detail levels for application logs. You can also specify a remote logging destination.



http_upgrade-0	Debug
lan-0	Critical
logger	Critical
mediasrv_mngr-0	Critical
port_vlan-0	Critical
printer_mngr-0	Notice
product-0	Critical
resolver-0	Critical
samba_mngr-0	Critical
security-0	Critical
sntp-0	Critical
static-0	Critical
upnp-0	Critical
usbhost_mngr-0	Critical
warranty-0	Critical
webui-0	Critical
wireless_ap-0	Critical
wireless_ap-1	Critical
wireless_ap-2	Critical
wireless_ap-3	Critical
wireless_core-0	Critical
wireless_wds-0	Critical
Set All	

☐ Syslog Enabled Syslog Log Level Debug

☐ Kernel Log Enabled Kernel Log Level Debug

☐ Remote Log Enabled IP Address: Port:

☐ TR069 Syslog Server Enabled IP Address: