

# AZTECH FG7003GRV(AC)

SingTel - Gigabit Ethernet DUAL-BAND Wireless AC Residential Gateway

SINGAPORE | JANUARY 2014

**Aztech**



## C O N T E N T S

1. About the Product	Page 3
2. Recommended Setup	Page 7
3. Connecting to the Internet	Page 8
4. Wireless Connection	Page 9
5. How to do WPS pairing	Page 13
6. Wireless Clients	Page 14
7. How to enjoy Wireless AC	Page 15
8. Firewall Configuration	Page 16
9. Voice Service Configuration	Page 33
10. Troubleshooting	
i. LED Troubleshooting	Page 37
ii. Wireless Troubleshooting	Page 42
iii. How to check existing FW version	Page 43
iv. How to Access Admin GUI	Page 44
14. FAQ	Page 45
15. Support Contact Info	Page 48

## Hardware Features

### WAN Connection

- ✧ 1-Port **Gigabit Ethernet WAN** Port for ONT (FTTH) Connection

### LAN Connection

- ✧ 4-Port **Gigabit Ethernet LAN**
- ✧ Built-in Wireless a/b/g/n/ac Dual Band Access Point (2.4GHz and 5Ghz)

### Others

- ✧ **2 FXS Ports** for connecting analog Phone sets
- ✧ WPS – Wifi Protected Setup button support
- ✧ LED Indicators for all interfaces and services

## Firmware Features

- ⌘ Out of the box pre-configuration to support **MIO TV**, **MIO Voice** and **SingNet Broadband**
- ⌘ TR069 Compliant Residential Gateway (auto configuration, remote monitoring/troubleshooting, remote firmware upgrade etc.)
- ⌘ **Zero configuration** Internet installation for **FTTH**
- ⌘ **Unique Wireless SSID** and **Wireless Key** for each of the unit (default wireless credentials are printed on the casing label sticker)
- ⌘ **Dynamic LAN Port mapping** for the **IPTV – STB**
- ⌘ Port Forwarding and DMZ support, configurable from the user mode pages
- ⌘ Standard support for Wireless Security / Encryption

# about the product

## Front Panel Indicators and Button

- ⊗ Power
- ⊗ Ethernet LAN Ports 1 to 4
- ⊗ Wifi (2.4GHz and 5GHz)
- ⊗ Voice 1 and 2 (Telephone)
- ⊗ USB
- ⊗ IPTV
- ⊗ Broadband (Ethernet WAN)
- ⊗ Internet
- ⊗ WPS Indicator and button



# about the product

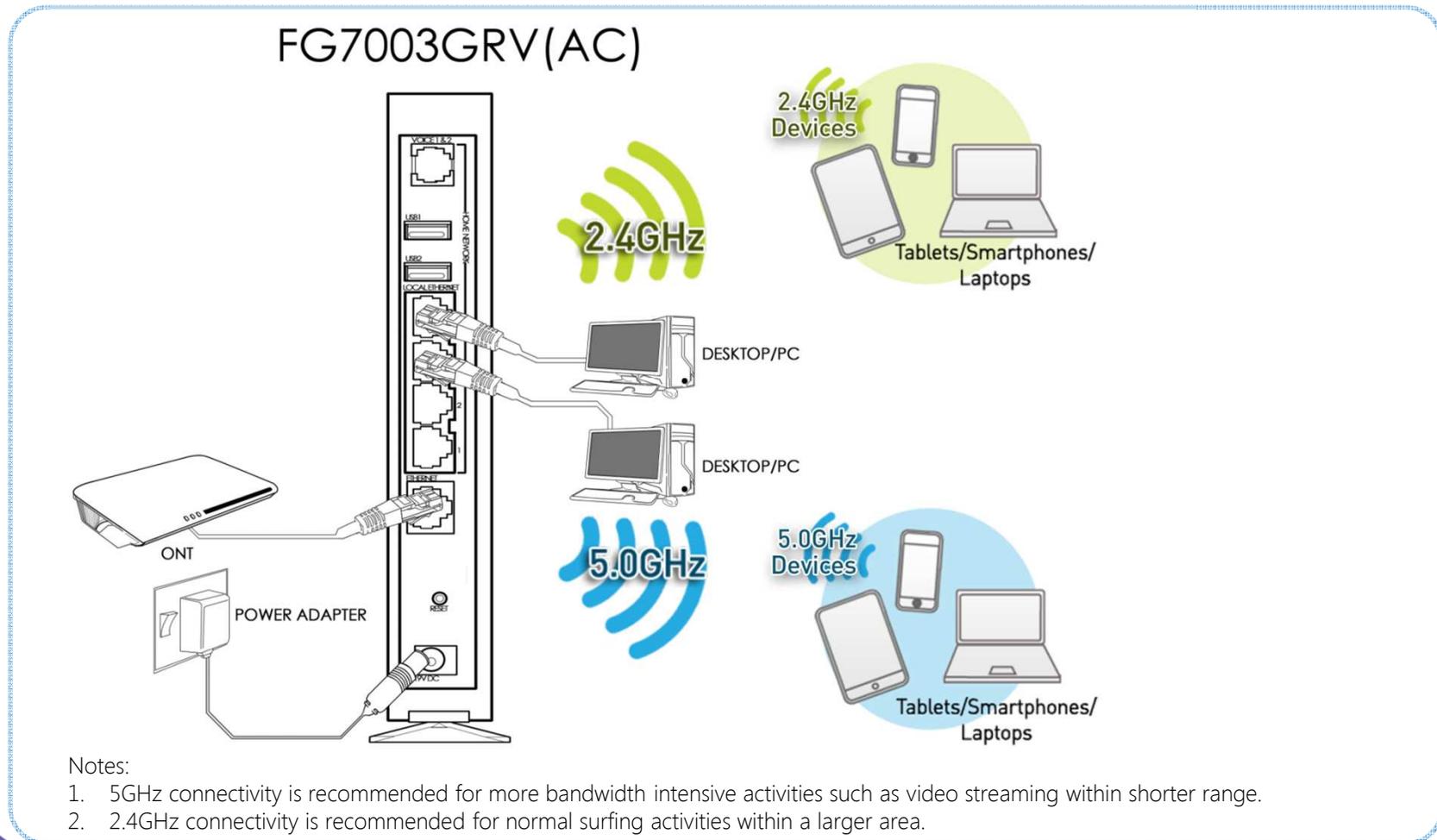
## Back Panel Ports and Button

- ⌘ Voice 1 and 2
- ⌘ USB 1
- ⌘ USB 2
- ⌘ Ethernet LAN Ports 1 to 4
- ⌘ Ethernet WAN Port
- ⌘ Reset button
- ⌘ Power Adapter Jack



# Recommended setup

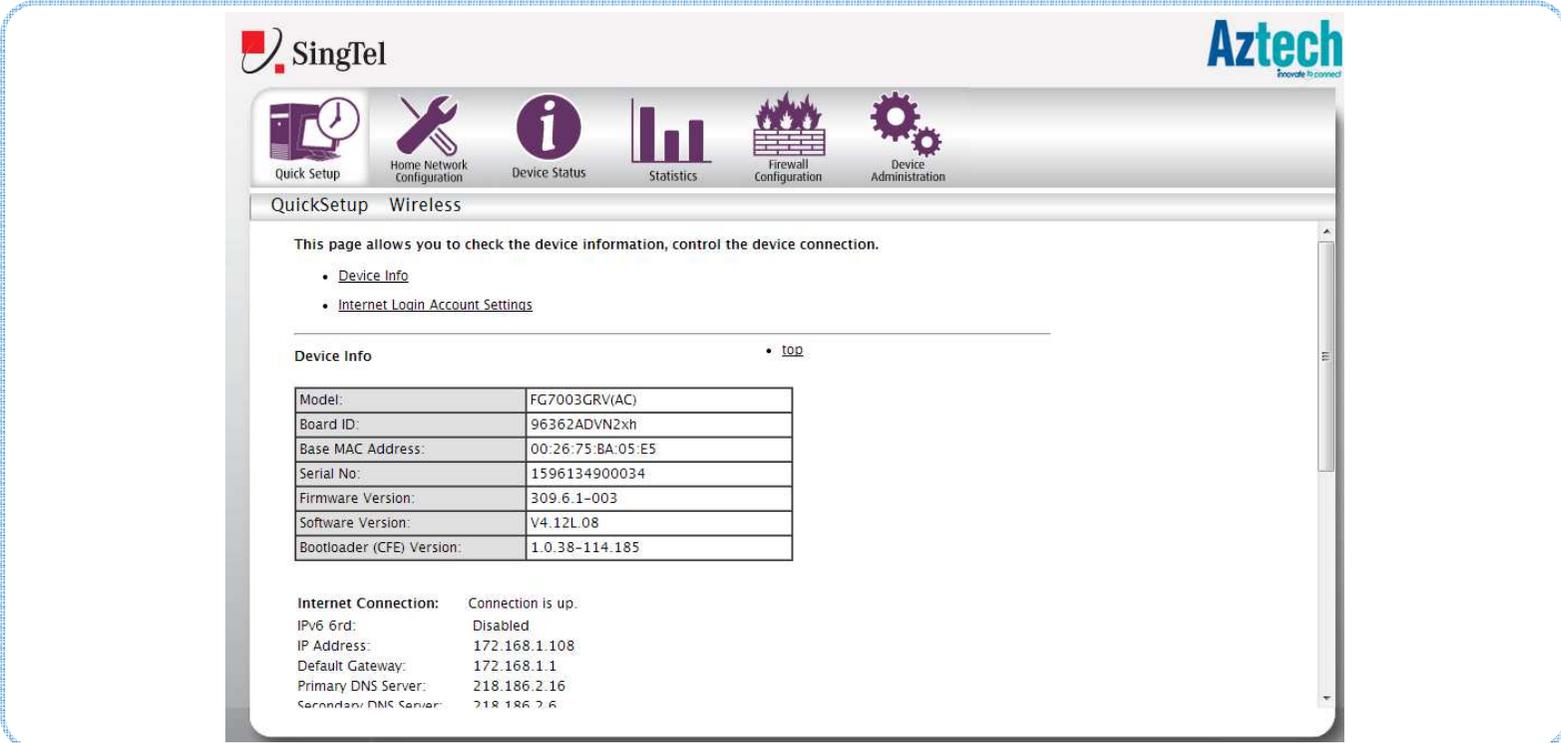
## Recommended Hardware Setup (FTTH)



# connecting to SingNet broadband

## FTTH

To check the Internet connection for FTTH , go to <http://192.168.1.254>, scroll down to Device Info> Internet Connection



The screenshot displays the web interface of the Aztech FG7003GRV(AC) Residential Gateway. The page features the SingTel logo on the left and the Aztech logo on the right. A navigation bar contains icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. The main content area is titled "QuickSetup Wireless" and includes a sub-header "Wireless". Below this, a message states: "This page allows you to check the device information, control the device connection." Two links are provided: "Device Info" and "Internet Login Account Settings". The "Device Info" section is expanded, showing a table with the following details:

Model:	FG7003GRV(AC)
Board ID:	96362ADV2xh
Base MAC Address:	00:26:75:BA:05:E5
Serial No:	1596134900034
Firmware Version:	309.6.1-003
Software Version:	V4.12L.08
Bootloader (CFE) Version:	1.0.38-114.185

Below the table, the "Internet Connection" status is shown as "Connection is up." Other network settings listed include: IPv6 6rd: Disabled, IP Address: 172.168.1.108, Default Gateway: 172.168.1.1, Primary DNS Server: 218.186.2.16, and Secondary DNS Server: 218.186.2.6.

## The Default Wireless Configuration

Each unit is preconfigured with a unique wireless network name and a unique password. The information on the default wireless can be found on the casing label sticker.



- ✘ The default wireless authentication is **Mixed WPA2/WPA-PSK**
- ✘ The wireless encryption is **TKIP + AES**
- ✘ Wireless channel is set to **Auto**
- ✘ The **WPS** is **enabled** by default.
- ✘ Both 2.4GHz and 5GHz SSIDs share the same network key by default.

## Changing the Wireless Settings

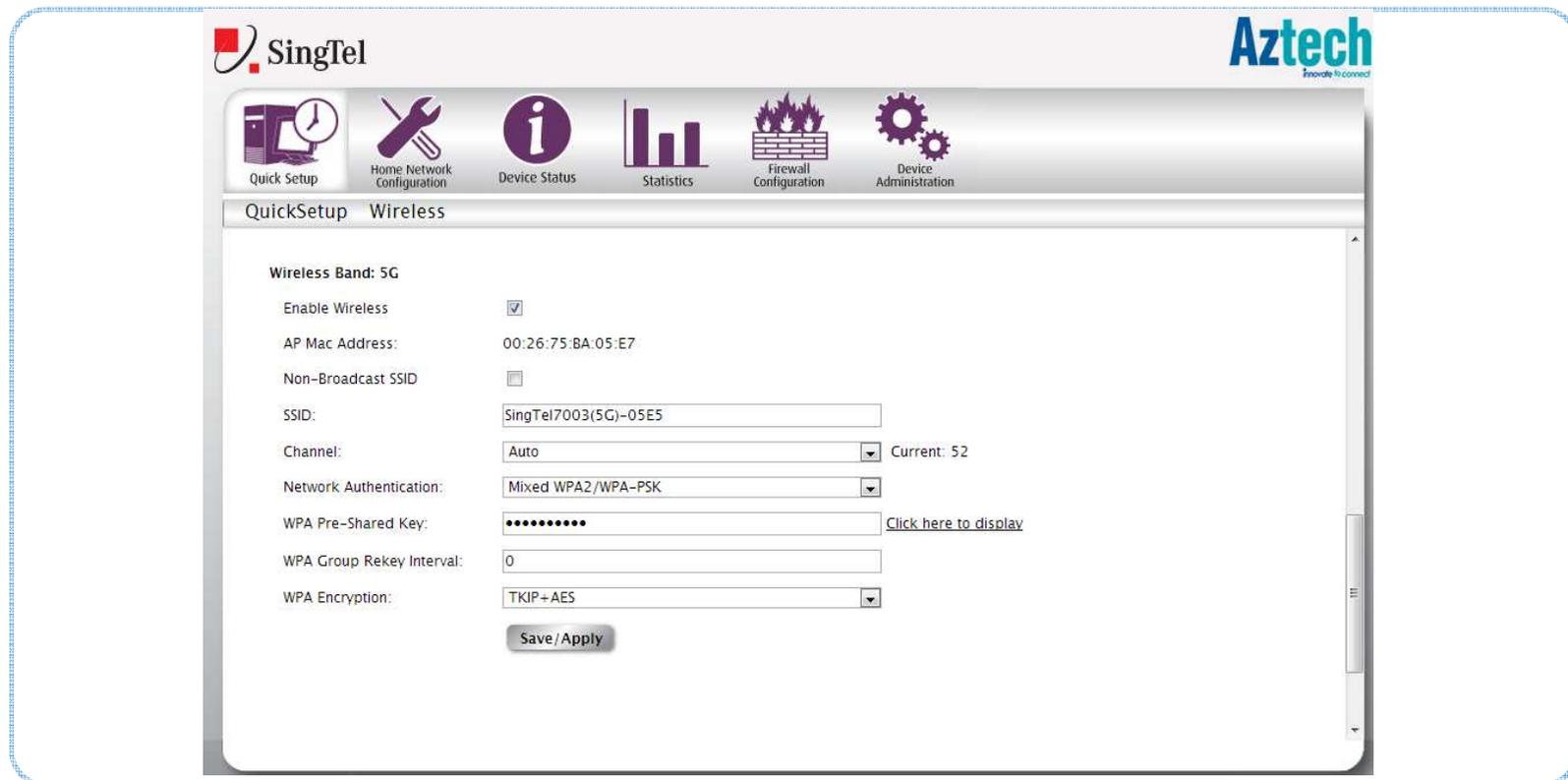
Open your web-browser (e.g. Internet Explorer) and go to <http://192.168.1.254>, click on Wireless link.

The screenshot displays the web interface of the Aztech FG7003GRV(AC) Residential Gateway. The page is titled "Wireless" and is part of the "QuickSetup" section. It features the SingTel logo on the left and the Aztech logo on the right. The navigation menu includes icons for Quick Setup, Home Network configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. The main content area is titled "Wireless - Settings" and provides instructions for configuring the wireless LAN interface. It includes a section for "Wireless Band: 2.4G" with the following settings:

- Enable Wireless:
- AP Mac Address: 00:26:75:BA:05:E6
- Non-Broadcast SSID:
- SSID: SingTel7003-05E5
- Channel: Auto (Current: 9)
- Network Authentication: Mixed WPA2/WPA-PSK

## 5GHz

The internet surfing experience is likely to improve on 5GHz with probably lesser wireless interference. Do take note that the 5GHz SSID can only be detected if your end device supports 5GHz wireless interface as well.



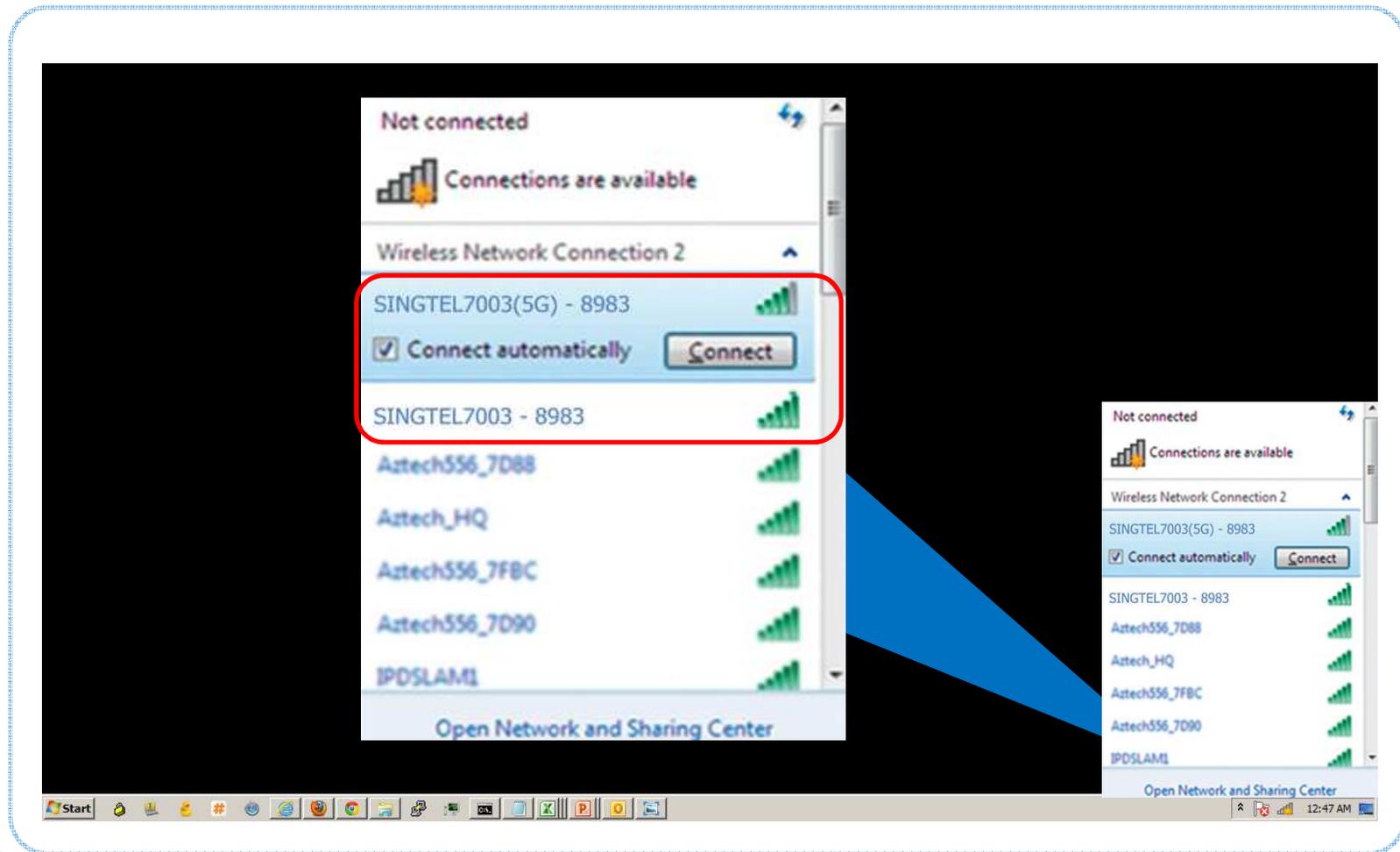
The screenshot displays the web interface for the Aztech FG7003GRV(AC) Residential Gateway. The interface is branded with SingTel and Aztech logos. A navigation bar includes icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. The main content area is titled "QuickSetup Wireless" and shows the following configuration options:

- Wireless Band: 5G
- Enable Wireless:
- AP Mac Address: 00:26:75:BA:05:E7
- Non-Broadcast SSID:
- SSID: SingTel7003(5G)-05E5
- Channel: Auto (Current: 52)
- Network Authentication: Mixed WPA2/WPA-PSK
- WPA Pre-Shared Key: •••••••• [Click here to display](#)
- WPA Group Rekey Interval: 0
- WPA Encryption: TKIP+AES

A "Save/Apply" button is located at the bottom of the configuration area.

# wireless connection

## Connecting to 2.4GHz and 5GHz Band



## How to do WPS Pairing

Step 1. Press the WPS button on the RG once,  
➤ upon pressed, WPS LED will start blinking green

Step 2. Press the WPS button on client device within 120 seconds from step 1 above.  
➤ Once the connection is authenticated and established, WPS LED will be solid green, followed by OFF within the next few seconds.

Note:

- WPS pairing is only available for 2.4GHz, and it is enabled by default

## Known wireless devices that supports 5GHz band

- iPhone 5
- iPhone 5S
- iPad 2
- iPad 3
- iPad 4
- iPad mini
- iPad Air
- HTC One
- HTC One S
- HTC One X
- Sony Xperia Z Ultra
- Sony Xperia Z1
- HTC Evo 4G LTE
- Samsung Galaxy S3
- Samsung Galaxy S4
- Samsung Galaxy Note 10.1
- Samsung Galaxy Tab 2 7.0 (GT-P3113)
- Samsung Galaxy Note 1
- Samsung Galaxy Note 2
- Samsung Galaxy Note 3
- Samsung Galaxy Note 8.0 with LTE
- Samsung Galaxy Note 10.1 2014 Edition (LTE)

Note: This list of devices that supports 5G does not necessarily support wireless AC.

## How to enjoy wireless AC

- Wireless Client: Wireless client need to be able to support wireless AC.
- List of wireless client adapters that support wireless AC:
  - Aztech WL592USB, WL593USB
  - Asus USB-AC53, USB-AC56, PCE-AC68
- List of mobile devices that supports wireless AC:
  - Sony Xperia Z1, Xperia Z Ultra
  - Samsung Galaxy Note 10.1 2014 Edition (LTE), Galaxy S4 with LTE (GT-I9505)

### Notes:

1. This list of devices that supports wireless AC is not exhaustive.
2. Wireless performance is also dependent on the client
3. For end devices which do not support wireless AC, it can still connect to the RG using other wireless mode e.g. a/b/g/n but will not be able to achieve the wireless AC speed.

## firewall configuration

## Incoming and Outgoing Firewall Settings

The screenshot displays the web interface for the Aztech FG7003GRV(AC) Residential Gateway. The interface is branded with SingTel and Aztech logos. A navigation bar includes icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. The 'Firewall Configuration' section is active, showing tabs for Settings, Port Forwarding, Port Triggering, and DMZ. The 'Firewall Settings' section explains that outgoing traffic is allowed by default but can be blocked, and incoming traffic is blocked by default but can be accepted. It provides instructions to use 'Add' or 'Remove' to configure filters. Below this is the 'IP Filtering List' configuration form, which includes fields for Filter Name, Direction (set to Incoming), Protocol, Source IP address, Source Subnet Mask, Source Port, Destination IP address, Destination Subnet Mask (with a checkbox), and Destination Port. A note at the bottom states that WAN interfaces must be selected for the rule to apply.

**SingTel** **Aztech**  
Innovate to connect

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

Settings Port Forwarding Port Triggering DMZ

**Firewall Settings**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Meanwhile, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure outgoing/incoming IP filters.

**IP Filtering List**

Filter Name:

Direction:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
Select at least one or multiple WAN interfaces displayed below to apply this rule.

# How To Set IP Filtering

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Click on Firewall Configuration Button

The screenshot displays the web interface of the Aztech FG7003GRV(AC) Residential Gateway. The browser address bar shows [192.168.1.254](http://192.168.1.254). The page header includes the SingTel logo on the left and the Aztech logo on the right. A navigation bar contains several icons: Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration (highlighted with a red box), and Device Administration. Below this, a sub-navigation bar includes Settings (highlighted with a red box), Port Forwarding, Port Triggering, and DMZ. The main content area is titled "Firewall Settings" and contains the following text:

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Meanwhile, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure outgoing/incoming IP filters.

The "IP Filtering List" section contains the following form fields:

- Filter Name:
- Direction:
- Protocol:
- Source IP address:
- Source Subnet Mask:
- Source Port (port or port:port):
- Destination IP address:
- Destination Subnet Mask:
- Destination Port (port or port:port):

At the bottom, there is a section for "WAN Interfaces (Configured in Routing mode and with firewall enabled only)" with the instruction: "Select at least one or multiple WAN interfaces displayed below to apply this rule."

## How To Set IP Filtering

Step 3. Fill in the fields required (Filter Name, traffic Direction, Protocol, Source IP Address and its port number information as well as Destination IP Address and its port number information).

Step 4. Click on Save/Apply button.

**IP Filtering List**

Filter Name:	<input type="text" value="MyFilterName"/>
Direction	<input type="text" value="Incoming"/>
Protocol:	<input type="text" value="TCP/UDP"/>
Source IP address:	<input type="text" value="10.1.10.130"/>
Source Subnet Mask:	<input type="text" value="255.255.0.0"/>
Source Port (port or port:port):	<input type="text" value="75"/>
Destination IP address:	<input type="text" value="192.168.1.15"/>
<input checked="" type="checkbox"/> Destination Subnet Mask:	<input type="text" value="255.255.255.0"/>
Destination Port (port or port:port):	<input type="text" value="50:90"/>

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
Select at least one or multiple WAN interfaces displayed below to apply this rule.

- Select All
- INTERNET/eth0.1
- quickstart/ppp0

## How To Set IP Filtering

Step 5. The rule keyed in will be added in the list

*Note: There is a default SingTel rule created in the list, please do not remove.*

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

INTERNET/eth0.1

quickstart/ppp0

Filter Name	Direction	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Singtel	Outgoing	UDP				67:68	<input type="checkbox"/>
MyFilterName	Incoming	TCP or UDP	10.1.10.130/16	75	192.168.1.15/24	50:90	<input type="checkbox"/>

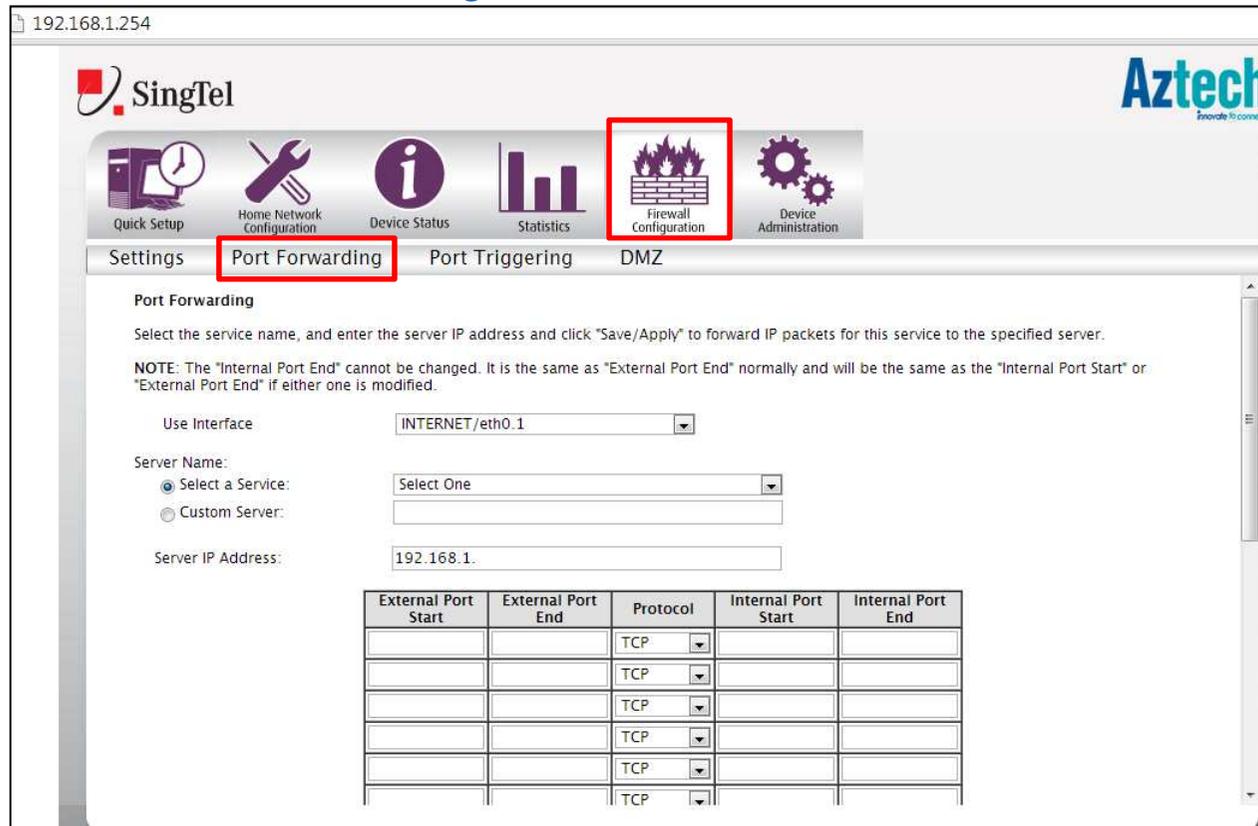


# How To Set Port Forwarding

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Click on Firewall Configuration Button

Step 3. Click on Port Forwarding Button



192.168.1.254

SingTel Aztech  
Innovate to connect

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

Settings **Port Forwarding** Port Triggering DMZ

**Port Forwarding**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server.

**NOTE:** The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.

Use Interface: INTERNET/eth0.1

Server Name:  
 Select a Service: Select One  
 Custom Server: [Text Field]

Server IP Address: 192.168.1.[Text Field]

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		

## How To Set Port Forwarding

Step 4. Check and confirm the IP Address of the device where the port forwarding rule will be pointed to. Fill in the filed Server IP Address field.

Step 5. Check Custom Server radio button and fill in the application name for easy reference.

Step 6. Fill in the respective port numbers to be forwarded to the server.

**Port Forwarding**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server.

**NOTE:** The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.

Use Interface:

Server Name:

Select a Service:

Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text" value="91"/>	<input type="text" value="92"/>	<input type="text" value="TCP"/>	<input type="text" value="91"/>	<input type="text" value="92"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>

# How To Set Port Forwarding

Step 7. Click on Save/Apply button.

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
91	92	TCP	91	92
		TCP		

# How To Set Port Forwarding

Step 8. Added rule will be shown

		TCP		

**Save/Apply**

Remaining number of entries that can be configured:31

**Port Forwarding list**

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
MyPortForwardingRule	91	92	TCP	91	92	192.168.1.91	<input type="checkbox"/>

**Remove**

## Port Triggering Settings

**SingTel** **Aztech**  
Provide to connect

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

Settings Port Forwarding **Port Triggering** DMZ

**NAT -- Port Triggering**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Use Interface:

Application Name:

Select an application:

Custom application:

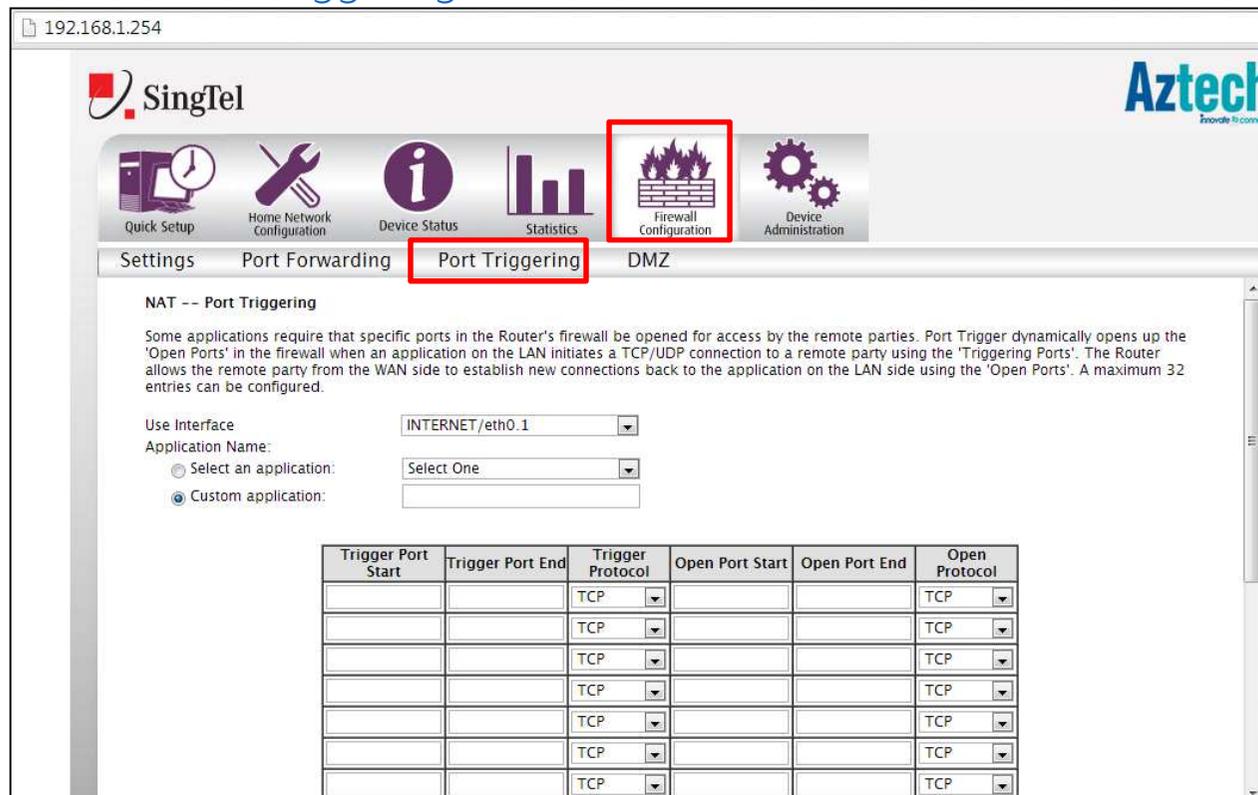
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

# How To Set Port Triggering

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Click on Firewall Configuration Button

Step 3. Click on Port Triggering button



The screenshot shows the web interface of the Aztech FG7003GRV(AC) Residential Gateway. The address bar displays [192.168.1.254](http://192.168.1.254). The page features the SingTel logo on the left and the Aztech logo on the right. A navigation bar contains icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration (highlighted with a red box), and Device Administration. Below the navigation bar, the 'Port Triggering' tab is selected and highlighted with a red box. The main content area is titled 'NAT -- Port Triggering' and includes a descriptive paragraph about the feature. Below the text, there are configuration options: 'Use Interface' set to 'INTERNET/eth0.1', and 'Application Name' with radio buttons for 'Select an application' (set to 'Select One') and 'Custom application'. At the bottom, there is a table for configuring port triggering rules.

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

## How To Set Port Triggering

Step 4. Check Custom Application radio button and fill in the application name for easy reference.

Step 5. Fill in the respective port numbers and protocol type.

**NAT -- Port Triggering**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
91	92	TCP/UDP	91	92	TCP/UDP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

## How To Set Port Triggering

Step 6. Click on Save/Apply button.

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
91	92	TCP/UDP	91	92	TCP/UDP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

**Save/Apply**

Step 7. Created rule will be shown in the list

**Port Triggering list**

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		
MyPortTriggeringRule	TCP/UDP	91	92	UDP	91	92	eth0.1	<input type="checkbox"/>

**Remove**

## How To Set Port Triggering

Step 8. Added rule will be shown

		TCP		

**Save/Apply**

Remaining number of entries that can be configured:31

**Port Forwarding list**

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
MyPortForwardingRule	91	92	TCP	91	92	192.168.1.91	<input type="checkbox"/>

**Remove**

## firewall configuration

## DMZ

192.168.1.254

SingTel Aztech  
know to connect

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

Settings Port Forwarding Port Triggering DMZ

**DMZ Host**

The Residential gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Click "Remove" to deactivate the DMZ host.

Hostname	MAC Address	IP Address	Expires In	Interface
My PC Name	f0:4d:a2:d0:22:cb	192.168.1.1	3 hours, 14 minutes, 45 seconds	LAN

DMZ Host IP Address:

Save/Apply Remove

## How To Set DMZ

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Click on Firewall Configuration Button

Step 3. Click on DMZ button

The screenshot shows the web interface of the Aztech Residential Gateway. The browser address bar displays [192.168.1.254](http://192.168.1.254). The page features the SingTel logo on the left and the Aztech logo on the right. A navigation bar contains several icons: Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration (highlighted with a red box), and Device Administration. Below this, a sub-menu bar includes Settings, Port Forwarding, Port Triggering, and DMZ (also highlighted with a red box). The main content area is titled "DMZ Host" and contains the following text:

The Residential gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Click "Remove" to deactivate the DMZ host.

Hostname	MAC Address	IP Address	Expires In	Interface
My PC Name	f0:4d:a2:d0:22:cb	192.168.1.1	3 hours, 14 minutes, 45 seconds	LAN

DMZ Host IP Address:

Buttons: Save/Apply, Remove

## How To Set DMZ

Step 4. Copy the IP Address value from list of clients table.

Step 5. Paste on the DMZ Host IP Address field.

Step 6. Click on Save/Apply button

**DMZ Host**

The Residential gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Click "Remove" to deactivate the DMZ host.

Hostname	MAC Address	IP Address	Expires In	Interface
Hariato	f0:4d:a2:d0:22:cb	192.168.1.1	3 hours, 9 minutes, 8 seconds	LAN

DMZ Host IP Address:

# voice service configuration

## Configuring the VOIP Username and Password

The voip username and password can be configured on the [admin page](#). It's under [Home Network > Voice](#).

**SingTel** **Aztech**  
provide to connect

**Voice - SIP Settings**

Enter the SIP parameters and click Save button to save the parameters and start the voice application.

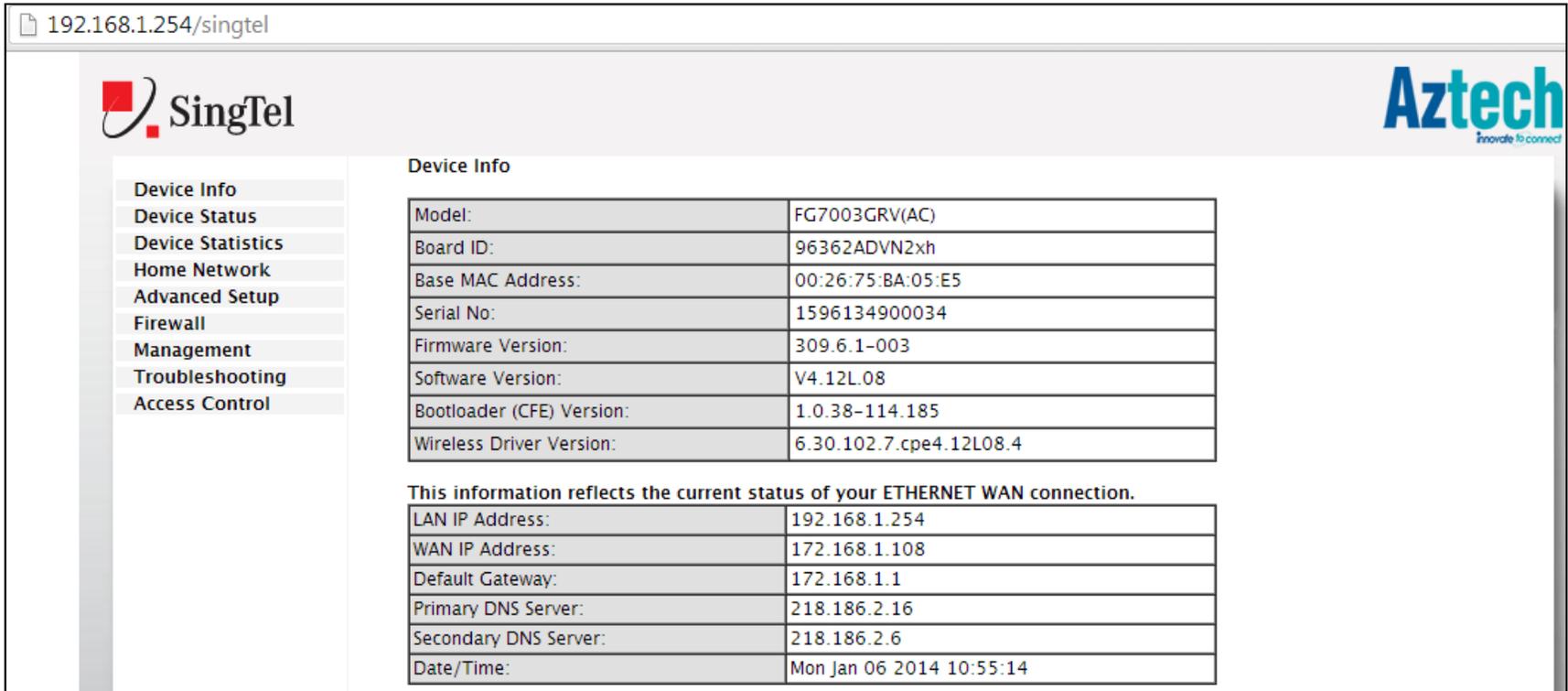
Line	Enable	Username	Password	Status
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unregistered
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unregistered

**Navigation Menu:** Device Info, Device Status, Device Statistics, Home Network, ARP, Settings, Voice, WLAN, Advanced Setup, Firewall, Management, Troubleshooting, Access Control

## How To Set MioVoice

Step 1. Launch an internet browser and go to <http://192.168.1.254/singtel>

Step 2. Enter admin / H3ll0t3ch when prompted for username and password respectively.



The screenshot shows a web browser window with the address bar displaying [192.168.1.254/singtel](http://192.168.1.254/singtel). The page features the SingTel logo on the left and the Aztech logo on the right. A navigation menu on the left includes links for Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, Management, Troubleshooting, and Access Control. The main content area is titled "Device Info" and contains two tables. The first table lists device specifications, and the second table, titled "This information reflects the current status of your ETHERNET WAN connection.", lists network parameters.

Device Info	
Model:	FG7003GRV(AC)
Board ID:	96362ADV2xh
Base MAC Address:	00:26:75:BA:05:E5
Serial No:	1596134900034
Firmware Version:	309.6.1-003
Software Version:	V4.12L.08
Bootloader (CFE) Version:	1.0.38-114.185
Wireless Driver Version:	6.30.102.7.cpe4.12L08.4

This information reflects the current status of your ETHERNET WAN connection.	
LAN IP Address:	192.168.1.254
WAN IP Address:	172.168.1.108
Default Gateway:	172.168.1.1
Primary DNS Server:	218.186.2.16
Secondary DNS Server:	218.186.2.6
Date/Time:	Mon Jan 06 2014 10:55:14

## How To Set MioVoice

Step 3. On the left hand navigation bar, click on Home Network

Step 4. Click on Voice

The screenshot shows the Aztech web interface for the SingTel Residential Gateway. The left navigation bar includes 'Home Network' and 'Voice', both highlighted with red boxes. The main content area is titled 'Voice - SIP Settings' and contains a table for configuring SIP lines. The table has columns for Line, Enable, Username, Password, and Status. Two lines are listed, both with 'Unregistered' status. Below the table are 'Save' and 'Refresh' buttons.

Line	Enable	Username	Password	Status
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unregistered
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unregistered

## How To Set MioVoice

Step 5. Check Enable checkbox

Step 6. Fill in the respective MioVoice account(s) and click on Save button

**SingTel** **Aztech**  
Innovate to connect

**Voice - SIP Settings**

Enter the SIP parameters and click Save button to save the parameters and start the voice application.

Line	Enable	Username	Password	Status
1	<input checked="" type="checkbox"/>	65941111	••••••••	Unregistered
2	<input checked="" type="checkbox"/>	65941112	••••••••	Unregistered

## LED Troubleshooting

### Power

- ⌘ Steady Red – reset button is pressed
- ⌘ Steady Red – unit is booting up or unit failed to boot
- ⌘ Green – firmware is loaded to the RAM / unit has successfully booted up
- ⌘ Off – no power or PSU faulty

### Ethernet LAN 1-4

- ⌘ Blinking Green – indicates activity on the port
- ⌘ Steady Green – Ethernet device is connected to the port
- ⌘ Off – there is no Ethernet device plugged in to the port or the cable is faulty

## LED Troubleshooting

### Wireless

- ⌘ Steady Green – wireless device(s) associated to the wireless AP
- ⌘ Blinking Green – indicates wireless activity
- ⌘ Off – no wireless device associated with the AP or AP is not activated

### Voice 1 and 2

- ⌘ Steady Green – voice account is registered
- ⌘ Blinking Green – indicates an on going call or the phone is off hook
- ⌘ Off – voice account is not set or account registration failed

## LED Troubleshooting

### USB

- ⌘ Steady Green – USB device is connected to the port
- ⌘ Off – no device is connected

### Broadband on FTTH

- ⌘ Steady Green – WAN ethernet port is connected to the ONT or an ethernet device
- ⌘ Off – No connection on the WAN ethernet port

## LED Troubleshooting

### IPTV

- ⌘ Steady Green – IPTV service is working, STB is plugged in and streaming
- ⌘ Steady Red – STB is not connected to the RG or  
STB in on DRA mode (if STB is connected to the RG) or  
STB is rebooting (if STB is connected to the RG) or  
IPTV service failed (if STB is connected to the RG) or  
no multicast streams coming (if STB is connected to the RG)
- ⌘ Off – no service or service is down

## LED Troubleshooting

### Internet on FTTH

- ⌘ Steady Green –connection is up and the interface is with an IP address
- ⌘ Off - no internet connection

### WPS

- ⌘ Steady Green – WPS is activated and a client is authenticated
- ⌘ Blinking Green – WPS is ready to connect
- ⌘ Off - WPS not activated

## Wireless Troubleshooting

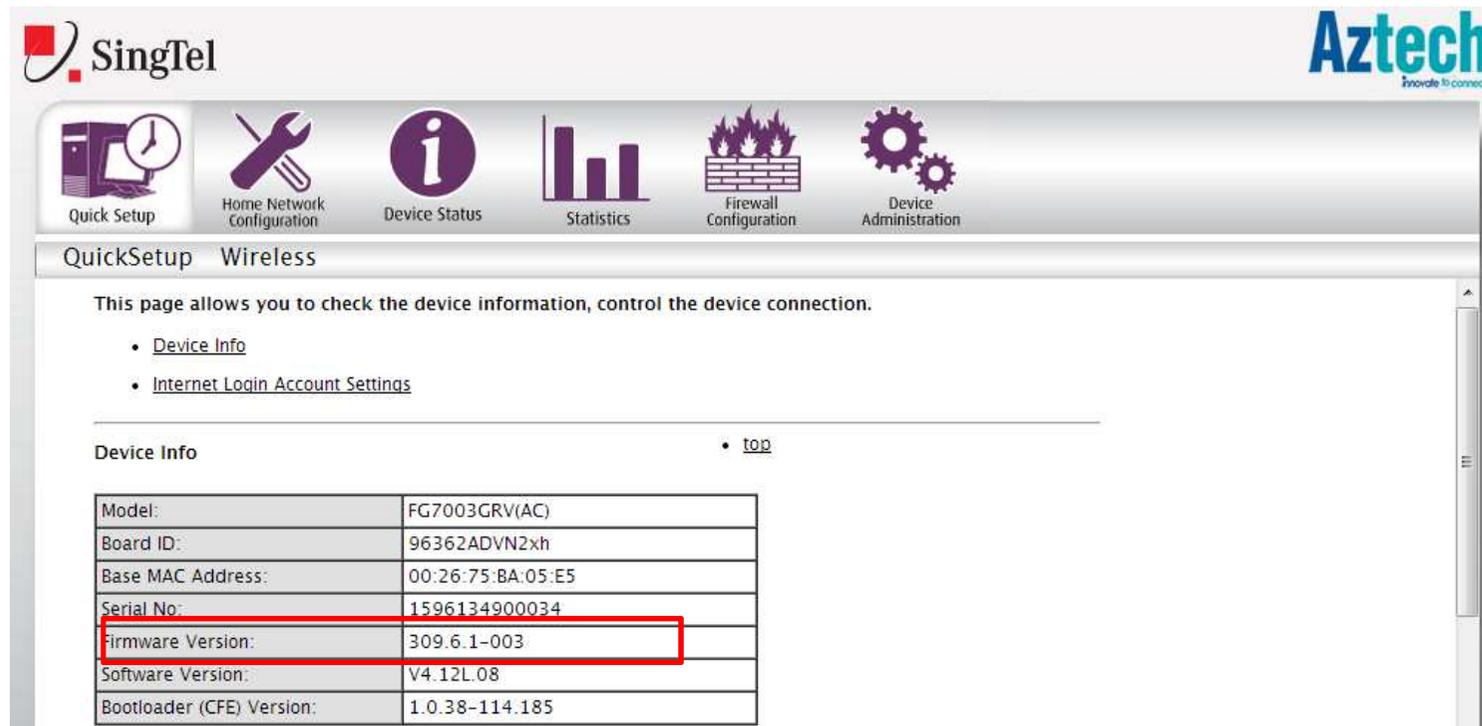
1. Always start with checking the wireless credentials, SSID and wireless security, if the wireless clients cannot connect to the AP
2. Think of the possibility of wireless channel congestion
  - ⌘ Please ensure wireless channel setting is set as "Auto" at all times. Should channel congestion is suspected, it is recommended to reboot the RG.
  - ⌘ If the wireless channel is so congested, the wireless client may get an IP address but might not be able to, from time to time, surf the internet or use the wireless network resource
3. Place the RG on a flat surface away from:
  - ⌘ Blockage such as artificial barriers
  - ⌘ Electronic devices such as bluetooth devices, microwave ovens and cordless telephones
  - ⌘ Water containing equipment filled with water

## Where to Check Firmware Version

Step 1. Launch an Internet Browser

Step 2. Fill in the Address bar <http://192.168.1.254> and enter

Step 3. Firmware version information is located on the web page under the Device Info



The screenshot displays the web interface of the Aztech FG7003GRV(AC) Residential Gateway. The page features the SingTel logo on the top left and the Aztech logo on the top right. A navigation bar contains icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. The main content area is titled "QuickSetup Wireless" and includes a sub-header "This page allows you to check the device information, control the device connection." Below this, there are links for "Device Info" and "Internet Login Account Settings". The "Device Info" section is expanded, showing a table with the following details:

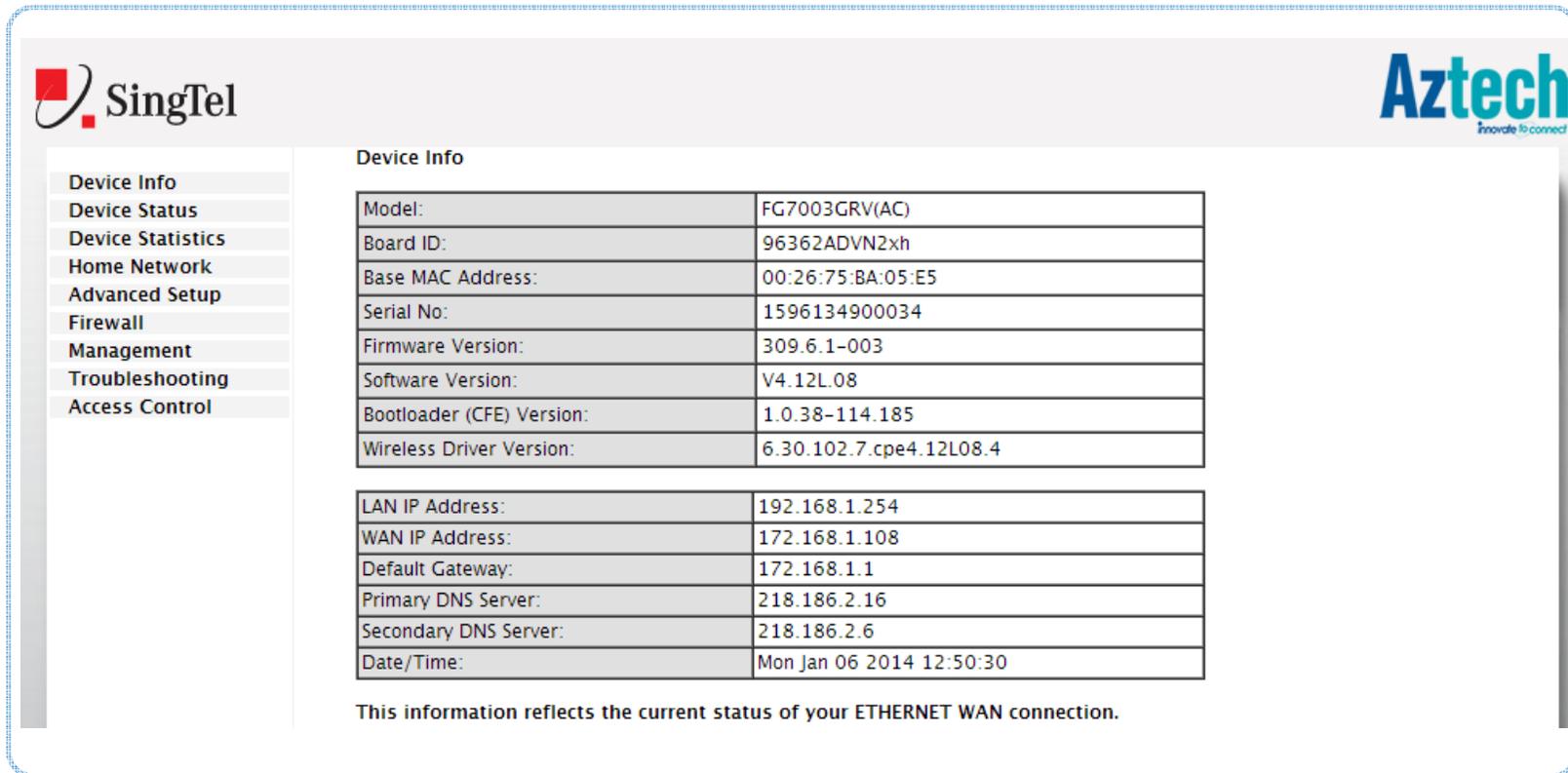
Model:	FG7003GRV(AC)
Board ID:	96362ADV2xh
Base MAC Address:	00:26:75:BA:05:E5
Serial No:	1596134900034
Firmware Version:	309.6.1-003
Software Version:	V4.12L.08
Bootloader (CFE) Version:	1.0.38-114.185

## Accessing the Admin GUI

<http://192.168.1.254/singtel>

Username: admin

Password: H3ll0t3ch



The screenshot displays the SingTel Aztech FG7003GRV(AC) Admin GUI. The interface features a navigation menu on the left with options: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, Management, Troubleshooting, and Access Control. The main content area is titled "Device Info" and contains two tables. The first table lists device specifications, and the second table lists network configuration details. The Aztech logo is visible in the top right corner.

Device Info	
Model:	FG7003GRV(AC)
Board ID:	96362ADVN2xh
Base MAC Address:	00:26:75:BA:05:E5
Serial No:	1596134900034
Firmware Version:	309.6.1-003
Software Version:	V4.12L.08
Bootloader (CFE) Version:	1.0.38-114.185
Wireless Driver Version:	6.30.102.7.cpe4.12L08.4

LAN IP Address:	192.168.1.254
WAN IP Address:	172.168.1.108
Default Gateway:	172.168.1.1
Primary DNS Server:	218.186.2.16
Secondary DNS Server:	218.186.2.6
Date/Time:	Mon Jan 06 2014 12:50:30

This information reflects the current status of your ETHERNET WAN connection.

## Frequently Asked Questions

CAN I USE BOTH 2.4GHz AND 5GHz BAND AT THE SAME TIME?

Yes, both bands are enable by default. Please note that the same client can only connect to either one of the band available at any point of time.

WHAT IS THE MAXIMUM NUMBER OF CLIENT IT CAN SUPPORT FOR WIRELESS?

30 for 2.4ghz band and 30 for 5ghz band.

CAN I CONFIGURE MAC FILTERING ON FG7003GRV(AC)?

No, MAC filtering feature is currently not supported.

# Frequently Asked Questions

## RG COMPARISON

Main Features	Feature	Aztech DSL7000GRV(S) (Current)	Aztech DSL7002GRV(S) (Current)	Aztech FG7003GRV(AC) (New)
Services Supported	ADSL	Yes	Yes	Not Available
	FTTH	Yes	Yes	Yes
	mioVoice	Yes	Yes	Yes
	mioTV	Yes	Yes	Yes
Operating Frequency	2.4 GHz	Yes	Yes	Yes
	5.0 GHz	No	Yes	Yes
Wireless Connection Mode		Wireless b/g/n	Wireless a/b/g/n	Wireless a/b/g/n/ac
MAC Filtering		Not supported	Not Supported	Not Supported <sup>1</sup>
WPS Push Button (2.4GHz only)		Disabled by default	Yes <sup>2</sup>	Yes (enabled by default)
Gigabit Ethernet LAN		4	4	4
Voice Ports (FXS)		2	2	2
USB Host Support		Disabled by default	Disabled by default	Disabled by default
DDNS		Not Supported	Not Supported	Not Supported <sup>1</sup>

Notes:

1. Under development
2. Firmware dependant

## Frequently Asked Questions

HOW CAN I TELL IF MY WIRELESS CLIENT (i.e. the mobile / wireless device) SUPPORTS 5GHZ BAND?

- By doing wireless SSID scanning, if the client supports 5GHz band, you will be able to see the default 5GHz SSID, with prefix of SingTel7003(5G)-xxxx as illustrated below.



Please note that if the wireless client/adaptor is able to see the 5GHz SSID, it does not necessarily mean that it is a Wireless AC client. There is a need to check against the hardware specifications if it really is a wireless AC client.

# support contact info

## Service Center Address:

31 Ubi Road 1 Aztech Building

Lobby B 5th Floor

Singapore 408694

## Hotline:

6594 2297

## Email:

[support@aztech.com](mailto:support@aztech.com)

## Operating Hours

Monday to Friday: 9:00 AM to 6:15 PM

Saturday: 9:00 AM to 1:00 PM

(Except Public Holidays)

Thank You

**Aztech**