



EMINENT



EM4720
Dual Band Gigabit AC1750 Router

en

Manual

EM4720 - Dual Band Gigabit AC1750 Router

Table of contents

1.0 Introduction	3
1.1 Packing contents	3
2.0 Device overview	4
Front Panel.....	4
Rear panel.....	5
2.1 Connecting the router wired.....	6
2.2 Configuring the router for connection with the Internet via DHCP.....	6
2.3 Configuring the router for connection with the Internet via Static IP	8
2.4 Configuring the router for connection with the Internet via PPPoE	9
2.5 Configuring the router for connection with the Internet via PPTP	10
2.6 Configuring the router for connection with the Internet via L2TP	11
3.0 Securing a wireless network	13
3.1 WPA2 AES security for 5GHz.....	13
3.2 WEP security	18
3.3 WPA2 AES security 2.4GHz	19
3.4 WEP security for 2.4GHz	22
3.5 Access Control	23
3.6 Finishing the installation procedure of your wireless router	26
4.0 Setting up a secured connection using WPS	26
4.1 Using the WPS button (Router and Wireless WPS adapter)	26
5.0 Multi SSID – Guest network.....	28
6.0 Operation mode.....	31
6.1 Access Point (AP).....	31
6.2 Repeater	36
7.0 Parental Control	42
8.0 Firewall.....	43
8.1 QOS	43
8.2 URL Filtering	46
8.3 IP Filtering	47
8.4 MAC Filtering.....	49
8.5 Port Filtering.....	52
8.6 Port Forwarding	54
8.7 DMZ	55
9.0 Management	57
9.1 Admin.....	57
9.2 Time and Date.....	58
9.3 System	58
9.4 Upgrade	59
10.0 Frequently Asked Questions and other related information.....	60
11.0 Service and support.....	60
12.0 Warning and points of attention	60

13.0 Warranty conditions	62
--------------------------------	----

1.0 Introduction

Congratulations with the purchase of this high-quality Eminent product! This product has undergone extensive testing by Eminent's technical experts. Should you experience any problems with this product, you are covered by Eminent warranty. Please keep this manual and the receipt in a safe place.

Register your product now on www.eminent-online.com and receive product updates!

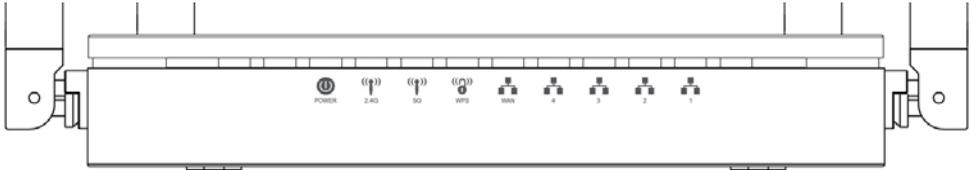
1.1 Packing contents

The following parts need to be present in the packing:

- EM4720 Concurrent Dual Band AC Gigabit Router
- Power adapter
- UTP network cable
- Quick install guide

2.0 Device overview

Front Panel



Label	Color	Function
POWER	Green	On: device is powered on Off: device is powered off
WAN	Green	On: WAN link established and active Off: No LAN link Flashing: Ethernet packets being transferred
2.4GHz/5GHz	Green	On: WLAN link established and active Flashing: Wireless packet being transferred
WPS	Green	Off: WPS link isn't established and active Flashing: WPS packets being transferred
LAN 1/2/3/4	Green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred

Rear panel

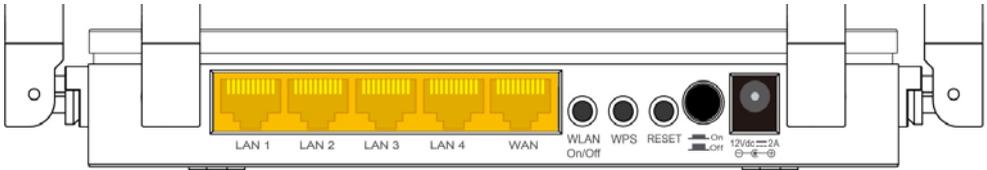


Figure 1: Rear Panel Connections

Label	Function
ANTENNA (Optional)	4 fixed dual band antenna
ON/OFF SWITCH	Power on/off the device
POWER	Connects to the supplied power adaptor
LAN 4/3/2/1	Connects the device via LAN Ethernet to up to 4 PCs
WAN	Connects the device via WAN Ethernet to xDSL / Cable Modem
WPS	Press this button for at least 3 full seconds and the WPS LED will flash to start WPS. Now go to the wireless adapter or device and press its WPS button. Make sure to press the button within 120 seconds (2 minutes) after pressing the router's WPS button.
WLAN	Press this button for at least 3 full second to turn off/on wireless signals
RESET	Reset button. RESET the 802.11ac WLAN Router to its default settings. Press this button for at least 6 full seconds to RESET device to its default settings.

2.1 Connecting the router wired

1. Turn off your computer.
2. Connect the router to a wall outlet using the supplied power adapter.
3. Connect the supplied UTP network cable to the '**WAN**' port of the router.
4. Connect the other end of the UTP network cable to the '**LAN**' port of your cable modem.
5. Connect a UTP network cable to one of the four '**LAN**' ports of your router.
6. Connect the other end of the UTP network cable to the network adapter in your computer.

Do I have a proper network connection? Turn on the computer and verify if the LED on the router, corresponding with the LAN-port to which you connected the UTP networking cable, is lit. The LED on the network adapter of your computer should also be lit.

2.2 Configuring the router for connection with the Internet via DHCP

Before you can configure the router for a connection with the Internet, you will first need to connect to the router. Follow the instructions below to connect to the router.

1. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on "**OK**" button.
3. Click on "**Setup Wizard**".

Current Status



SETUP WIZARD

4. Please make sure WAN Access Type "**DHCP Client**" is selected and press "**Next**"

SELECT WAN CONNECTION TYPE

WAN Access Type: DHCP Client

Host Name (Optional):

MAC Address (Optional): 000000000000 **CLONE MAC**

Primary DNS Address: 0.0.0.0

Secondary DNS Address: 0.0.0.0 (Optional)

Special Requirement from ISP

NEXT

5. If your provider requires you to make a connection by using a Static IP-address, then please proceed with chapter 2.3.
If your provider requires you to make a connection by using PPPoE (with username and password), then please proceed with chapter 2.4.
For PPTP internet connection, please proceed with chapter 2.5.
For L2TP internet connection, please proceed with chapter 2.6.
6. Fill out a Wireless Network Name (SSID). Default this is Eminent for 2.4GHz and Eminent_5G for 5GHz. Click on "**APPLY & REBOOT**". Wait until the internet configuration is completed



ENTER WIRELESS NETWORK NAME AND SECURITY KEY

2.4GHz Wireless Network Name (SSID) :
Eminent (Maximum 32 characters)

2.4GHz Wireless Security Key :
NNvARdRxpDAHc9qA (Minimum 8 characters)

5GHz Wireless Network Name (SSID) :
Eminent_5G (Maximum 32 Characters)

5GHz Wireless Security Key :
NNvARdRxpDAHc9qA (Minimum 8 characters)

BACK APPLY & REBOOT

7. Your router will apply the settings and reboot.
8. The internet configuration is now completed.

2.3 Configuring the router for connection with the Internet via Static IP

1. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browser's address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on "OK" button.
3. Click on "Setup Wizard".

Current Status

SETUP WIZARD

- Please make sure WAN Access Type "**Static IP**" is selected. Enter IP Address, Subnet Mask, Default Gateway and DNS which was given by your Internet Service Provider (ISP) and click on "**Next**"

SELECT WAN CONNECTION TYPE

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

Primary DNS Address: 0.0.0.0

Secondary DNS Address: 0.0.0.0 (Optional)

NEXT

- Your router will apply the settings and reboot.
- The internet configuration is now completed.

2.4 Configuring the router for connection with the Internet via PPPoE

- Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
- Please enter the User Name: **admin** and Password: **admin** and then click on "**OK**" button.
- Click on "**Setup Wizard**".

Current Status

SETUP WIZARD

- Please make sure WAN Access Type "**PPPoE**" is selected. Enter User Name and Password which was given by your Internet Service Provider (ISP) and click on "**Next**".



SELECT WAN CONNECTION TYPE

WAN Access Type: PPPoE

User Name:

Password:

Special Requirement from ISP

NEXT

- Your router will apply the settings and reboot.
- The internet configuration is now completed.

2.5 Configuring the router for connection with the Internet via PPTP

- Launch your internet web browser on your computer and type `http://192.168.8.1` in your browser's address bar.
- Please enter the User Name: **admin** and Password: **admin** and then click on "**OK**" button.
- Click on "**Setup Wizard**".

Current Status

SETUP WIZARD

- Please make sure WAN Access Type “**PPTP**” is selected. Enter your Servers’s IP address including “**User Name**” and “**Password**” and click on “**Next**”.

SELECT WAN CONNECTION TYPE

WAN Access Type: **PPTP**

PPTP Mode: Dynamic IP (DHCP) Static IP

PPTP Server Mode: Domain Name IP Address

Domain Name:

Server IP Address:

User Name:

Password:

NEXT

- Your router will apply the settings and reboot.
- The configuration is now completed.

2.6 Configuring the router for connection with the Internet via L2TP

- Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
- Please enter the User Name: `admin` and Password: `admin` and then click on “**OK**” button.
- Click on “**Setup Wizard**”.

Current Status

SETUP WIZARD

- Please make sure WAN Access Type "**L2TP**" is selected. Enter your Servers's IP address including "**User Name**" and "**Password**" and click on "**Next**".

SELECT WAN CONNECTION TYPE

WAN Access Type: L2TP

L2TP Mode: Dynamic IP (DHCP) IP Static IP

L2TP Server Mode: Domain Name IP Address

Domain Name:

Server IP Address: 172.1.1.1

User Name:

Password:

NEXT

- Your router will apply the settings and reboot.
- The configuration is now completed.

3.0 Securing a wireless network

To avoid having uninvited guests probing your wireless network we strongly recommend securing your wireless network. There are several security methods which can secure the network at different levels. To apply a method to your network it is required that all wireless network devices support this method. The strongest method of security is WPA2 (WiFi Protected Access).

The strongest method of security is WPA2 AES. It is recommended to use this type of security. However, it is possible that (older) wireless hardware is not able to use this type of security, but can only use WPA-TKIP or WEP. Refer to the documentation of your hardware to be sure if your hardware can use WPA2 AES.

If you wish to use WPA2 AES security, continue with paragraph 3.1 (recommended). If you wish to use WEP security, continue with paragraph 3.2

3.1 WPA2 AES security for 5GHz

1. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on **“OK”** button.
3. From the left-hand menu, click on **“Setting”** - **“WIRELESS 5G”**.



4. You will see the following screen:



Wireless Settings

This page is to configure the wireless settings of your device.

5GHz

Status: ON

Wi-Fi Network Name (SSID):

Broadcast SSID:

Wireless Mode:

Channel Width:

Channel:

Maximum Downlink: Mbps (1-1000,0:no restriction)

Maximum Uplink: Mbps (1-1000,0:no restriction)

[Security](#) [Advance](#) [Access Control](#) [Multi SSID](#) [WPS](#) [Wireless Schedule](#)

5. This page is to configure the 5GHz wireless settings of your router. See below figure for wireless network description:

Field	Description
Status	Enable or Disable the Wireless LAN Interface. Default: ON
Wi-Fi Network Name (SSID)	Specify your 5GHz network name. Default: Eminent_5G Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). If you keep default network name (SSID) Eminent_5G , then this is the network you want to connect to using your mobile device. You are also free to change the SSID name. This new made network name will then be the one to make a wireless connection with.
Broadcast SSID	Disable SSID broadcasting to hide the network name and make it more secure. Please note, if you disable this function then you have to manually add a wireless network connection in your mobile device.
Wireless Mode	Specify the WLAN Mode. Supported = A/N/AC
Channel Width	Choose a Channel Width from the pull-down menu. Supported = 20/40/80MHz
Channel Number	Choose a Channel Number from the pull-down menu. Select between channel 36 and 112 to determine what will be the most stable channel for your wireless 5Ghz network. Select " Auto " to let the router determine the most stable connection.
Maximum Downlink	Adds a restriction for the maximum downlink throughput speed. At default = 0 , which means no restriction.
Maximum Uplink	Adds a restriction for the maximum uplink throughput speed. At default = 0 , which means no restriction.

6. Select **"Security"** to open the security settings. You will see the following screen:



Wireless Settings

This page is to configure the wireless settings of your device.

5GHz

Status: ON

Wi-Fi Network Name (SSID):

Broadcast SSID: ▼

Wireless Mode: ▼

Channel Width: ▼

Channel: ▼

Maximum Downlink: Mbps (1-1000,0:no restriction)

Maximum Uplink: Mbps (1-1000,0:no restriction)

Security + Advance + Access Control + Multi SSID + WPS + Wireless Schedule +

7. At the field 'Encryption' select **"WPA2"**.

The screenshot shows the 'SECURITY (5GHZ)' configuration interface. At the top, there is a blue header with the text 'SECURITY (5GHZ)'. Below the header, the 'Select SSID' dropdown menu is set to 'Root AP - Eminent_5G'. The 'Encryption' dropdown menu is set to 'WPA-Mixed'. Under 'Authentication Mode', the 'Personal' radio button is selected. For both 'WPA Cipher Suite' and 'WPA2 Cipher Suite', the 'TKIP' and 'AES' checkboxes are checked. The 'Pre-Shared Key' field contains a series of dots, and there is a small eye icon to its right. At the bottom of the page, there are two blue buttons: 'SAVE AND REBOOT LATER' on the left and 'SAVE AND REBOOT NOW' on the right.

8. At default is the SSID Eminent_5GHz network password protected. This password is also printed at the bottom label of your EM4720 router. At the field “Pre-Shared Key” is the password. You can enter another password for your 5GHz wireless network if you like.

Please note, if you change the password for this wireless network all the wireless devices which were already connected to this wireless network need to be connected again with the new chosen password.

9. Click on “**SAVE AND REBOOT NOW**” to let the router save and apply the settings. If you want to make other changes first for this wireless network, then please select “**SAVE AND REBOOT LATER**”. Once you are ready please do not forget to click on “**SAVE AND REBOOT NOW**”.

3.2 WEP security

If you would like to use WEP security, please follow the above security steps in paragraph 3.1 and select ‘**WEP**’ at step 7.

You can select ‘**Key Length: 64 bits or 128 bits**’. For WEP key **64-bits** please enter maximum of 5 characters. For WEP key **128-bits** please enter maximum of 13 characters. For WEP encryption you are only allowed to use numbers from 0 till 9 and the letters a till z. Do not enter special characters or space bar.

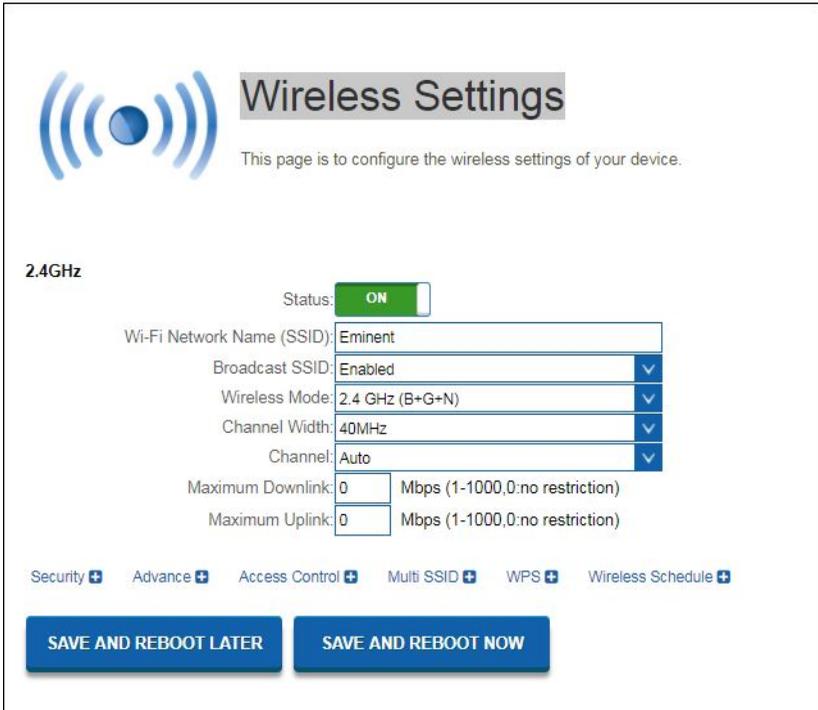
Please note, if you have chosen WEP as wireless encryption, the WPS functionality will be disabled.

3.3 WPA2 AES security 2.4GHz

1. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on “**OK**” button. You will see the following screen:
3. From the left-hand menu, click on “**Setting**” - “**WIRELESS 2.4G**”.



4. You will see the following screen:



Wireless Settings

This page is to configure the wireless settings of your device.

2.4GHz

Status: ON

Wi-Fi Network Name (SSID):

Broadcast SSID: ▼

Wireless Mode: ▼

Channel Width: ▼

Channel: ▼

Maximum Downlink: Mbps (1-1000,0: no restriction)

Maximum Uplink: Mbps (1-1000,0: no restriction)

[Security +](#)
[Advance +](#)
[Access Control +](#)
[Multi SSID +](#)
[WPS +](#)
[Wireless Schedule +](#)

5. This page is to configure the 2.4GHz wireless settings of your router. See below figure for wireless network description:

Field	Description
Status	Enable or Disable the Wireless LAN Interface. Default: ON
Wi-Fi Network Name (SSID)	Specify your 2.4GHz network name. Default: Eminent Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). If you keep default network name (SSID) Eminent , then this is the network you want to connect to using your mobile device. You are also free to change the SSID name. This new made network name will then be the one to make a wireless connection with.
Broadcast SSID	At default = Enabled. Disable SSID broadcasting to hide the network name and make it more secure. Please note, if you disable this function then you have to manually add a wireless network connection in your mobile device.
Wireless Mode	Specify the WLAN Mode. Supported = B/G/N
Channel Width	Choose a Channel Width from the pull-down menu. Supported = 20/40 MHz
Channel Number	Choose a Channel Number from the pull-down menu. Select between channel 1 and 13, depending which channel width is selected, to determine what will be the most stable channel for your wireless 2.4GHz network. Select " Auto " to let the router determine the most stable connection.
Maximum Downlink	Adds a restriction for the maximum downlink throughput speed. At default = 0 , which means no restriction.
Maximum Uplink	Adds a restriction for the maximum uplink throughput speed. At default = 0 , which means no restriction.

6. Select **"Security"** to open the security settings. You will see the following screen:

SECURITY (2.4GHZ)

Select SSID: Root AP - Eminent

Encryption: WPA-Mixed

Authentication Mode: Enterprise Personal

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key:

SAVE AND REBOOT LATER SAVE AND REBOOT NOW

7. At the field 'Encryption' select **"WPA2"**.
8. At default is the SSID Eminent_2.4GHz network password protected. This password is also printed at the bottom label of your EM4720 router. At the field "Pre-Shared Key" is the password listed. You can enter another password for your 2.4GHz wireless network if you like.

Please note, if you change the password for this wireless network all the wireless devices which were already connected to this wireless network need to be connected again with the new chosen password.

9. Click on **"SAVE AND REBOOT NOW"** to let the router save and apply the settings. If you want to make other changes first for this wireless network, then please select **"SAVE AND REBOOT LATER"**. Once you are ready please do not forget to click on **"SAVE AND REBOOT NOW"**.

3.4 WEP security for 2.4GHz.

If you would like to use WEP security, please follow the above security steps in paragraph 3.2 and select **'WEP'** at step 7.

You can select **'Key Length: 64 bits or 128 bits'**. For WEP key **64-bits** please enter maximum of 5 characters. For WEP key **128-bits** please enter maximum of 13

characters. For WEP encryption you are only allowed to use numbers from 0 till 9 and the letters a till z. Do not enter special characters or space bar.

Please note, if you have chosen WEP as wireless encryption, the WPS functionality will be disabled.

3.5 Access Control

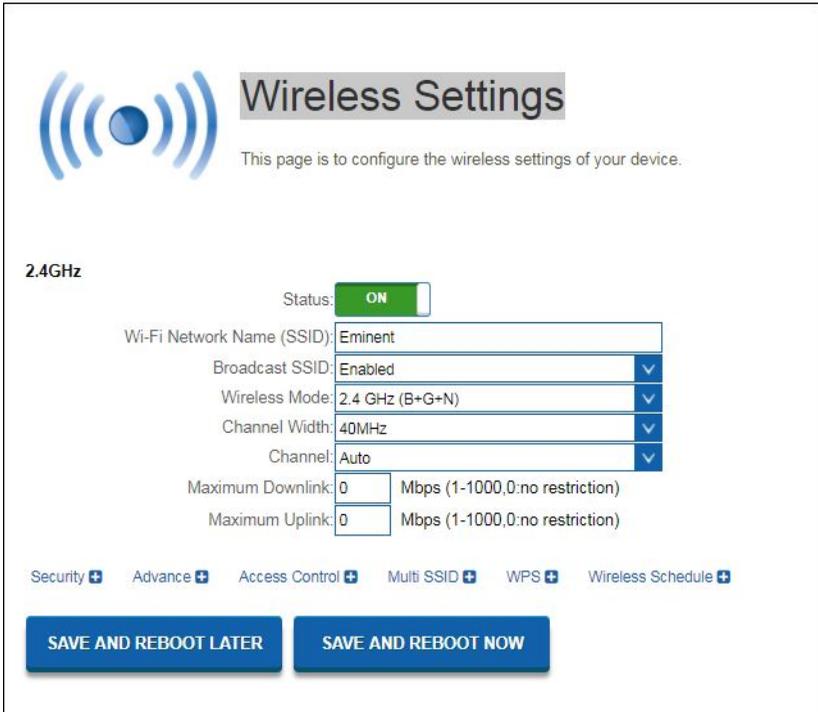
A MAC Address Access List (ACL)has the ability to let only authorized clients connect to the network. MAC addresses can be added/deleted and edited from the ACL list depending on the MAC Access Policy.

If you choose '**Allowed Listed**', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your router. When '**Deny Listed**' is selected, these wireless clients on the list will not be able to connect to your router. To access the *Wireless NetworkAccess Control*:

The below instruction will be the same for 2.4GHz and 5GHz.

1. Launch your internet web browser on your computer and type <http://192.168.8.1> in your browsers address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on "**OK**" button.
3. From the left-hand menu, click on "**Setting**" - "**WIRELESS 2.4G**".
4. You will see the following screen:





The image shows a web interface for configuring wireless settings. At the top left is a blue wireless signal icon. To its right is the title 'Wireless Settings' in a grey box. Below the title is a subtitle: 'This page is to configure the wireless settings of your device.' The main section is titled '2.4GHz'. It features a 'Status' toggle switch set to 'ON'. Below this are several configuration fields: 'Wi-Fi Network Name (SSID)' with the value 'Eminent', 'Broadcast SSID' set to 'Enabled', 'Wireless Mode' set to '2.4 GHz (B+G+N)', 'Channel Width' set to '40MHz', and 'Channel' set to 'Auto'. At the bottom of this section are two rows for 'Maximum Downlink' and 'Maximum Uplink', both set to '0' Mbps. Below these fields are five expandable sections: 'Security', 'Advance', 'Access Control', 'Multi SSID', 'WPS', and 'Wireless Schedule'. At the very bottom are two blue buttons: 'SAVE AND REBOOT LATER' and 'SAVE AND REBOOT NOW'.

Wireless Settings

This page is to configure the wireless settings of your device.

2.4GHz

Status: ON

Wi-Fi Network Name (SSID):

Broadcast SSID: ▼

Wireless Mode: ▼

Channel Width: ▼

Channel: ▼

Maximum Downlink: Mbps (1-1000,0:no restriction)

Maximum Uplink: Mbps (1-1000,0:no restriction)

[Security](#) + [Advance](#) + [Access Control](#) + [Multi SSID](#) + [WPS](#) + [Wireless Schedule](#) +

[SAVE AND REBOOT LATER](#) [SAVE AND REBOOT NOW](#)

5. Select Access Control. You will see the following screen:

ACCESS CONTROL (5GHZ)

Policy: ▼

MAC Address:

Comment:

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

- At the field "**Policy**" choose to "**Allow or Deny Listed MAC Addresses**" by clicking the down arrow .
- Fill out the MAC address of the client you wish you add to the Access Control List (ACL).
- Once you have finished the settings press "**SAVE AND REBOOT NOW**". The router will now reboot and save and apply the settings.

3.6 Finishing the installation procedure of your wireless router

After following chapter 2 and 3, you can finish the installation procedure by following the next steps:

1. Remove the UTP network cable from your computer.
2. Remove the UTP networking cable from the LAN port of your router.
3. Restart your computer.
4. You have now properly installed and secured your router.

Write down the security method, the network name and the key:

WPA2 AES WEP

Network name: _____

Key: _____

4.0 Setting up a secured connection using WPS

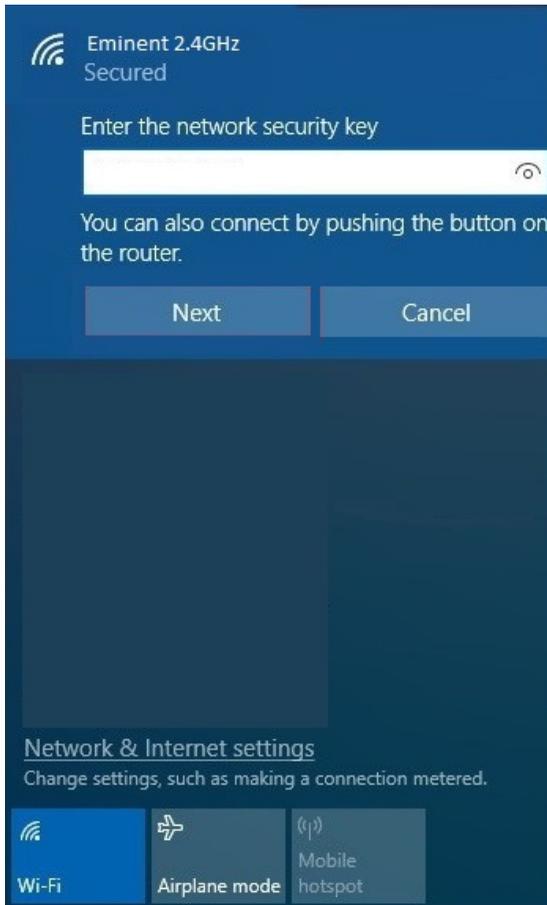
The EM4720 can be secured using WPS. WPS is an easy feature, which allows you to secure your wireless network by pressing the WPS button on both your Eminent router and your wireless WPS device. The Eminent router and your wireless WPS device will then automatically 'agree' to use a SSID and WPA2 AES security key. The connection between the Eminent wireless router and your WPS device will be established automatically.

Make sure the wireless WPS adapter is installed on your computer.

4.1 Using the WPS button (Router and Wireless WPS adapter)

Note: The following steps are created using Windows 10.

1. Make sure your computer has been started and your Wireless WPS adapter is installed on your computer. Also make sure your Wireless Eminent router has an internet connection.
2. If correct, an icon of the wireless connection () will be added to your taskbar.
3. Click the icon . A list of available wireless networks will be listed.
4. Select the network you want to connect to and click 'Connect'.



5. If correct, Windows will now ask you to fill out your wireless security key. It also shows you to push the WPS button on the router.
6. Press the WPS button on the Eminent router for approximately 3 seconds until the WPS led will start flashing.
7. Press the WPS button on your wireless WPS adapter. Refer to the manual of your wireless WPS adapter for the exact amount of time you need to press the WPS connection.
8. The connection between the Eminent router and your wireless WPS adapter will be established automatically.

Hint: Some WPS adapters and Windows versions require you to use the supplied WPS adapter software. If so, the steps described above can differ from your own situation. Please refer to the manual of the wireless WPS adapter for the exact steps.

Hint: When connecting a dual band receiver by WPS, the connection will be established for the strongest signal, either on 2,4GHZ or 5GHz.

5.0 Multi SSID – Guest network

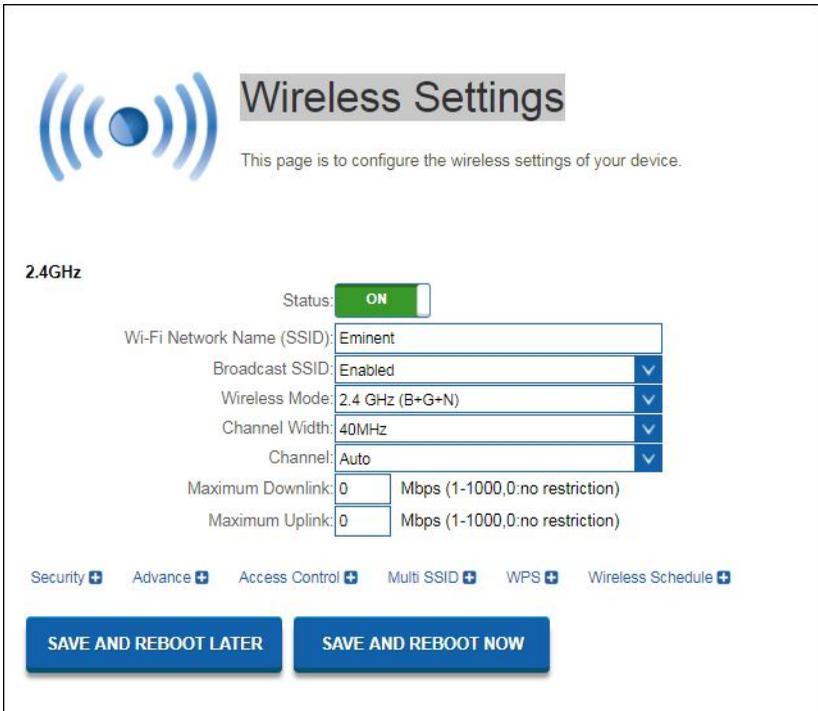
The *Multi SSID* page allows you to configure up to 4 guest networks per Wi-Fi band. So in total you can create up to 8 guest networks.

The main advantage of creating a guest network is because of the increased security it offers. You can setup a wireless guest network with as example for visiting clients, customers while your primary wireless network password remains secret. You can also setup this guest account to have only Internet access. This will keep your private LAN secured.

1. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on “**OK**” button.
3. From the left-hand menu, click on “**Setting**” - “**WIRELESS 2.4G**”.



4. You will see the following screen:



Wireless Settings

This page is to configure the wireless settings of your device.

2.4GHz

Status: ON

Wi-Fi Network Name (SSID): Eminent

Broadcast SSID: Enabled

Wireless Mode: 2.4 GHz (B+G+N)

Channel Width: 40MHz

Channel: Auto

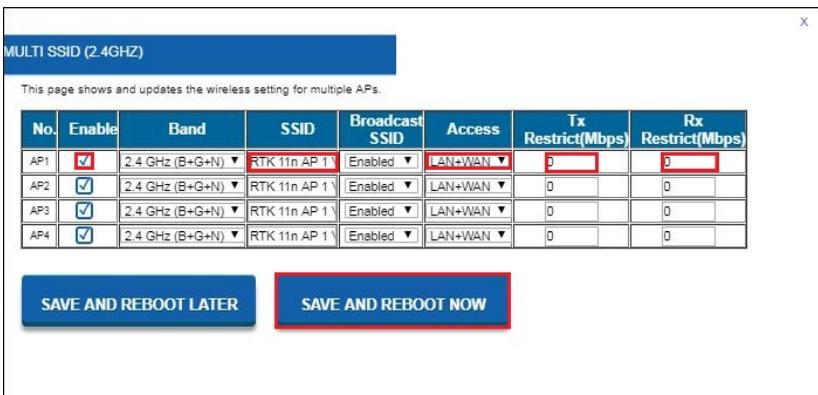
Maximum Downlink: 0 Mbps (1-1000,0:no restriction)

Maximum Uplink: 0 Mbps (1-1000,0:no restriction)

Security + Advance + Access Control + Multi SSID + WPS + Wireless Schedule +

SAVE AND REBOOT LATER **SAVE AND REBOOT NOW**

5. Click on “**Multi SSID settings**”. You will see the following screen:



MULTI SSID (2.4GHz)

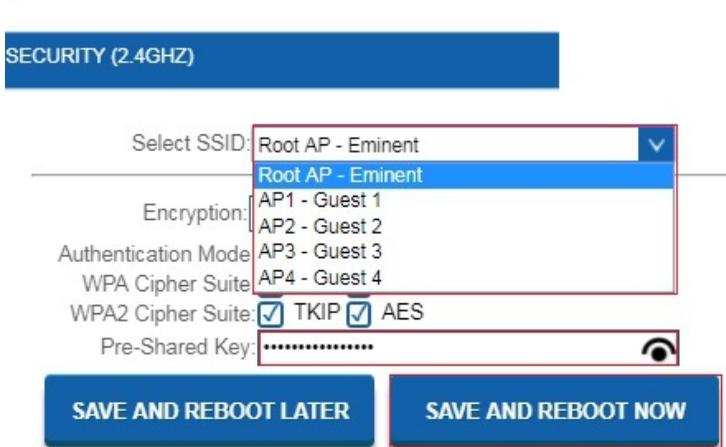
This page shows and updates the wireless setting for multiple APs.

No.	Enable	Band	SSID	Broadcast SSID	Access	Tx Restrict(Mbps)	Rx Restrict(Mbps)
AP1	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP 1	Enabled	LAN+WAN	0	0
AP2	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP 1	Enabled	LAN+WAN	0	0
AP3	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP 1	Enabled	LAN+WAN	0	0
AP4	<input checked="" type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP 1	Enabled	LAN+WAN	0	0

SAVE AND REBOOT LATER **SAVE AND REBOOT NOW**

6. Enable at least one of the four AP's to unlock and change the settings.

7. At the field SSID select your desired network name which will be used for this guest network.
8. Select which access the client should have when connecting to this guest network. "**LAN+WAN**" means internet plus LAN access. By selecting only "**WAN**" the client only has access to the Internet.
9. To make sure this guest network will not use the complete amount of Bandwidth speed, you can add a bandwidth speed restriction for both download (TX) and upload (RX) speed.
10. Once you have finished the settings, please select "**SAVE AND REBOOT NOW**" The router will now reboot and save and apply the settings.
11. Now that all of the multiple SSID's (guest) networks have been created you have the option to add a wireless encryption per guest network.
12. At the Wireless Settings page, click on "**Security**". You will see the following screen:



SECURITY (2.4GHZ)

Select SSID: Root AP - Eminent

Encryption: AP1 - Guest 1

Authentication Mode: AP2 - Guest 2

WPA Cipher Suite: AP3 - Guest 3

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key:

SAVE AND REBOOT LATER SAVE AND REBOOT NOW

13. At the field "**Select SSID**" select the new made guest network by clicking the down arrow .
14. At the field "Pre-Shared Key" you can now add a password to secure the selected guest network.
15. Once you have finished the settings, please select "**SAVE AND REBOOT NOW**" The router will now reboot and save and apply the settings.

6.0 Operation mode

This chapter describes how to configure the way that your device connects to the Internet. We will discuss the options in **“Operation Mode”**:

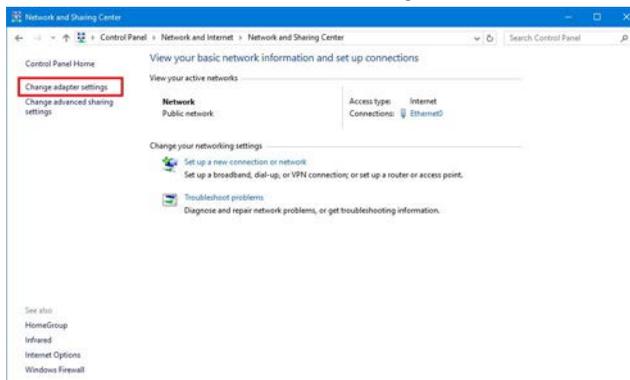
- **Router** (Selected mode as default setting)
- **Access Point (AP)**
- **Repeater**

In the following instructions we will inform you how to setup your router as Access Point or Repeater.

6.1 Access Point (AP)

Important! Before we change the operation mode to Access Point we need to provide a static IP address to our network adapter, while the DHCP server from the EM4720 will be disabled. If you did not have a static IP address you cannot longer login to your router due to no IP address will be provided anymore from your router. We will use Windows 10 to show you the instructions how to add a static IP address to your network adapter.

1. Make sure your modem or router is not connected to your EM4720. Connect your EM4720 via LAN port to your LAN port of your PC or Laptop by using a network cable.
2. Click on the Windows start menu icon, type **“Control Panel”** in the search bar and click on **“Control Panel”**. You will see the following screen:
3. Click the link **“View network status and tasks”** under the **“Network and Internet”** header. You will see the following screen:



4. Click on the link at the left side of the window labeled **“Change adapter settings”**.
5. You will now see the available network adapters.

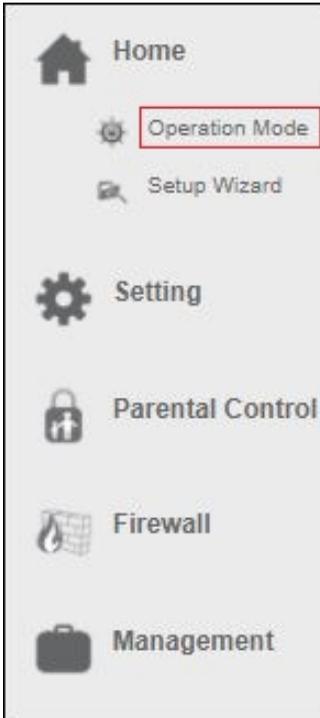


6. Select the network adapter you wish to add the static IP address and select Properties with your right mouse button.
7. Select "Internet Protocol version 4 (TCP/IPv4) and click on Properties.

Obtain an IP address automatically
 Use the following IP address:

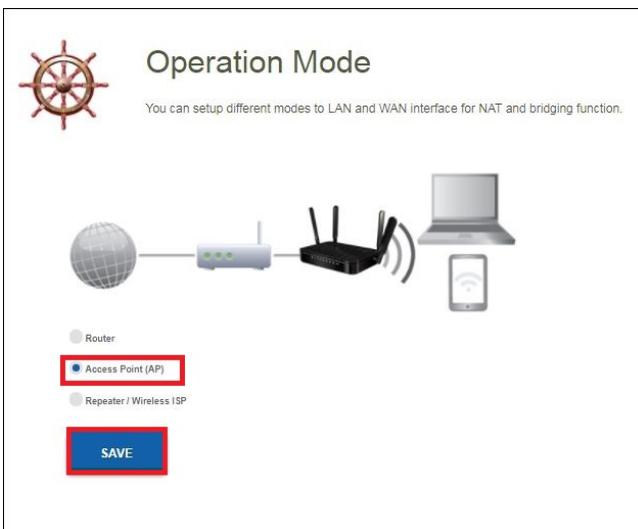
IP address:
 Subnet mask:
 Default gateway:

8. Select "Use the following IP address" and make sure you enter an ip address in the same range as the router.
9. For example: **IP-Address** = 192.168.8.100
10. For **Subnet mask** fill out: 255.255.255.0
11. Press "**OK**" and close the properties.
12. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
13. Please enter the User Name: **admin** and Password: **admin** and then click on "**OK**" button.
14. From the left-hand menu, click on "**Home**" and "**Operation Mode**".



You will see the following screen:

15. Select **“Access Point” (AP)** and click on the **“Save”** button. Your router will reboot and apply the settings. You will see the following screen:





16. Click on “**Setup Wizard**”. You will see the following screen:

ENTER WIRELESS NETWORK NAME AND PASSWORD X

2.4GHz Wireless Network Name (SSID) :

(Maximum 32 characters)

2.4GHz Wireless Security Key :

(Minimum 8 characters)

5GHz Wireless Network Name (SSID) :

(Maximum 32 Characters)

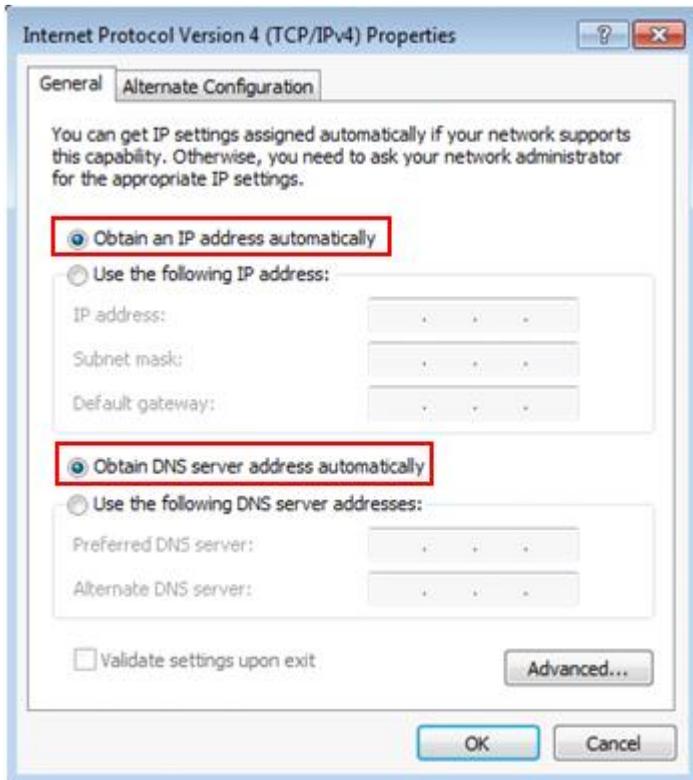
5GHz Wireless Security Key :

(Minimum 8 characters)

APPLY & REBOOT

17. You can choose to keep the default SSID name and password or you can change this to any SSID network name you prefer. For example we will use Eminent_AP and Eminent_5G_AP. Once you have finished these settings, click on “**Apply & Reboot**”.

18. You will see the note: **Success!**, press **“OK”**.
19. The router will now reboot and save and apply the settings.
20. Power off your EM4720 router. Connect your modem or other router to one of the four LAN ports of the EM4720. Please make sure you do not connect the WAN port. Turn on your router again.
21. Change from Static IP setting back to Obtain automatically an IP address. Please follow again steps 2 up to 8. At step 8 you choose for **“Obtain Automatically an IP address”**.



22. Your router is now configured as Access Point.

6.2 Repeater

1. Please make sure that the WAN port from your EM4720 is not connected.
2. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
3. Please enter the User Name: **admin** and Password: **admin** and then click on **“OK”** button.
4. From the left-hand menu, click on **“Home”** and **“Operation Mode”**.



You will see the following screen:



Operation Mode

You can setup different modes to LAN and WAN interface for NAT and bridging function.

Router

Access Point (AP)

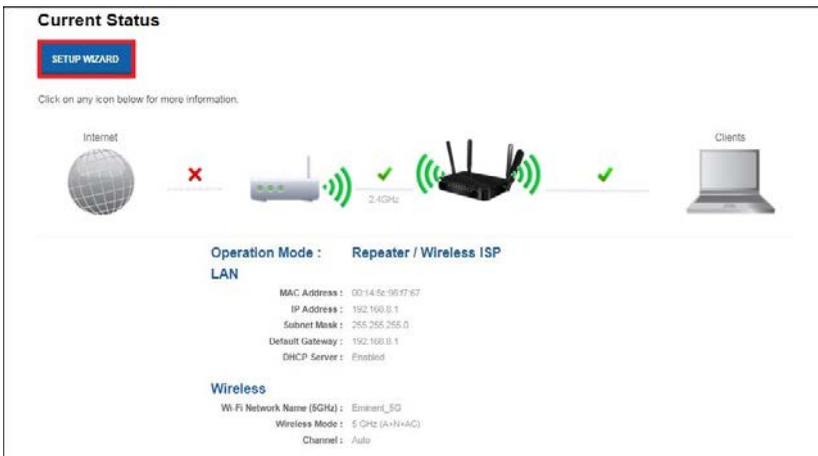
Repeater / Wireless ISP

2.4Ghz 5Ghz

SAVE

The image shows a configuration interface for a router. At the top left is a ship's wheel icon. The title is 'Operation Mode'. Below the title is a diagram showing a globe connected to a small router, which is connected to a larger black router. The larger router is connected to a laptop and a smartphone. The text '2.4GHz' is placed between the two routers. Below the diagram are three radio button options: 'Router', 'Access Point (AP)', and 'Repeater / Wireless ISP'. The 'Repeater / Wireless ISP' option is selected and highlighted with a red box. Below it are two radio button options for frequency: '2.4Ghz' (selected) and '5Ghz'. At the bottom is a blue 'SAVE' button, also highlighted with a red box.

5. Select **“Repeater”** and choose which Wi-Fi band you wish to configure as repeater. As example we will use 2.4GHz.
6. Click on the **“Save”** button. Your router will reboot and save the settings. You will see the following screen:



Current Status

SETUP WIZARD

Click on any icon below for more information.

Internet

2.4GHz

Clients

Operation Mode : Repeater / Wireless ISP

LAN

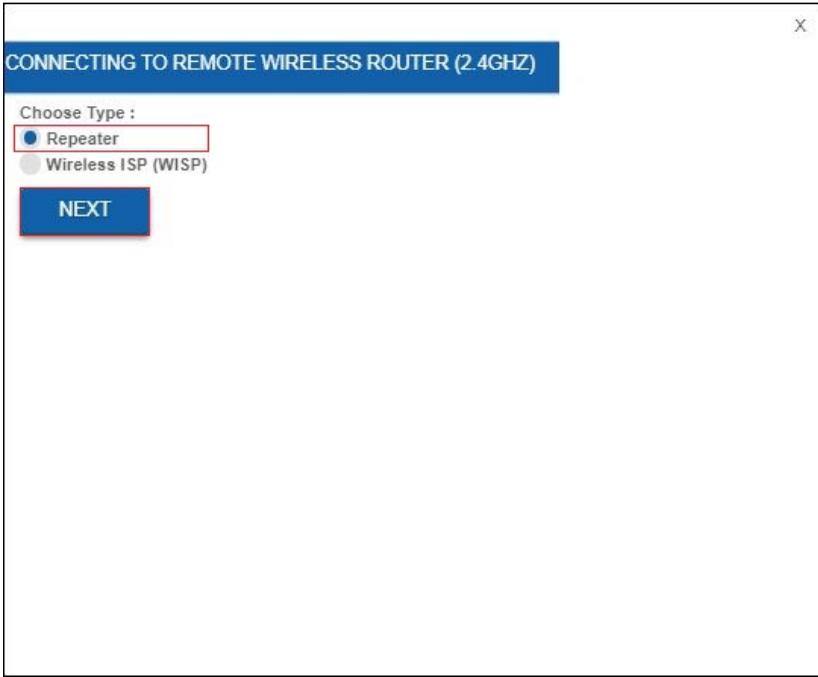
MAC Address : 00:14:5c:98:17:67
 IP Address : 192.168.8.1
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.8.1
 DHCP Server : Enabled

Wireless

Wi-Fi Network Name (5GHz) : Emmerit_5G
 Wireless Mode : 5 GHz (A+N+AC)
 Channel : Auto

The image shows the 'Current Status' screen of a router. At the top left is a 'SETUP WIZARD' button. Below it is a message: 'Click on any icon below for more information.' There are three icons: 'Internet' (globe), a router icon with a red 'X' and a green checkmark, and 'Clients' (laptop). The router icon is labeled '2.4GHz'. Below the icons is the 'Operation Mode' section, which shows 'Repeater / Wireless ISP' selected. Underneath are the 'LAN' settings: MAC Address (00:14:5c:98:17:67), IP Address (192.168.8.1), Subnet Mask (255.255.255.0), Default Gateway (192.168.8.1), and DHCP Server (Enabled). Below that is the 'Wireless' section: Wi-Fi Network Name (5GHz) (Emmerit_5G), Wireless Mode (5 GHz (A+N+AC)), and Channel (Auto).

7. Click on **“Setup Wizard”**. You will see the following screen:



8. Choose “**Repeater**” and click “**Next**”. You will see the following screen.
9. You have the option to keep the same SSID network name, but we suggest to change the SSID for both 2.4GHz and 5GHz to check if you have properly configured the router as repeater.
10. For example we will use SSID name Eminent_5GHz_R and Eminent_R.

ENTER LOCAL WIRELESS NETWORK NAME AND SECURITY KEY (5GHZ)X

5GHz Wireless Network Name (SSID) :
 (Maximum 32 characters)

5GHz Wireless Security Key :
 (Minimum 8 characters)

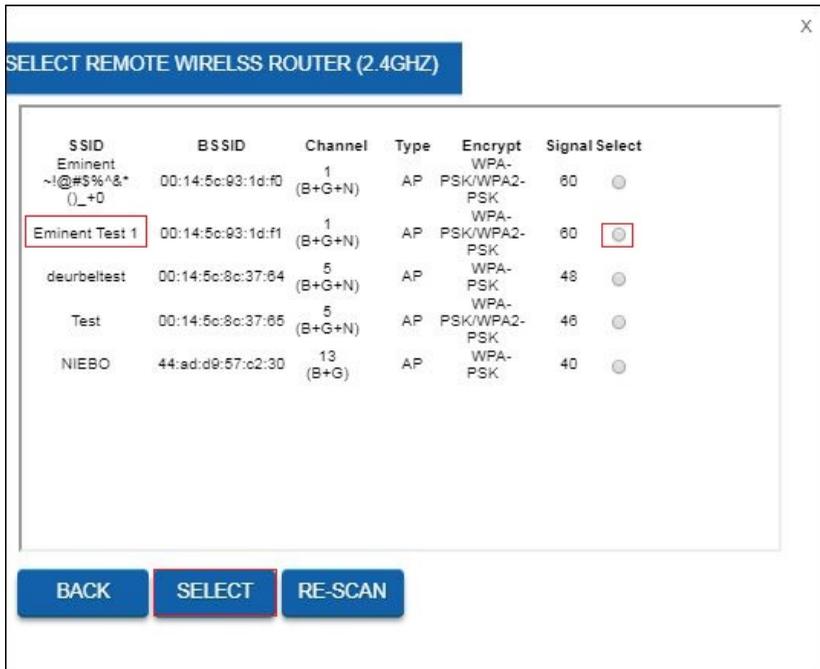
2.4GHz Wireless Network Name (SSID) :
 (Maximum 32 characters)

2.4GHz Wireless Security Key :
 (Minimum 8 characters)

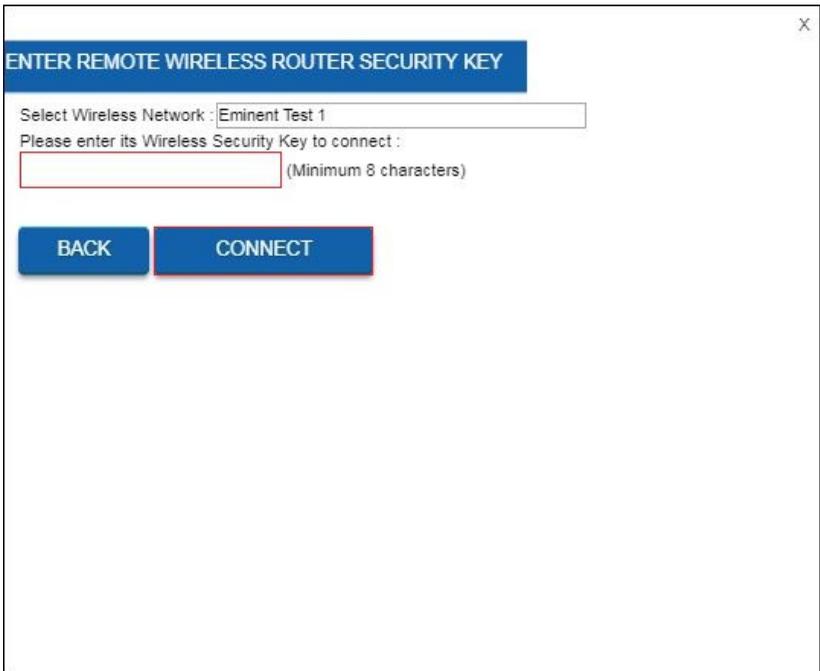
Click **Next** to find available wireless router.

BACKNEXT

11. Click **"Next"**.
12. Your router will reboot and switch to repeater mode.
13. You will now be able to connect the repeater to your existing wireless network.



14. Select your 2.4GHz wireless network name and click on **"Select"**.



ENTER REMOTE WIRELESS ROUTER SECURITY KEY

Select Wireless Network : Eminent Test 1

Please enter its Wireless Security Key to connect :
 (Minimum 8 characters)

BACK CONNECT

15. Please enter the wireless security key to connect the repeater to your wireless 2.4GHz network. Click "**Connect**".
16. After approx. 10-20 seconds your router will notice you that you have connected successfully. If this notification will not popup then you will most likely entered the incorrect wireless encryption key.



Connect successfully!

Reboot Now

17. Click "**Reboot Now**".
18. The router will now reboot and save and apply the settings.

7.0 Parental Control

With the Parental Control function you can add an internet rule so your children will have limited time for internet surfing. You add the rule for a specific device with a specific block and start time.

1. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
2. Please enter the User Name: **admin** and Password: **admin** and then click on **“OK”** button.
3. From the left-hand menu, click on Parental Control. You will see the following screen.

Parental Control

This page allows you to restrict the time for a client's network usage.

Enable Parental Control: ON OFF

User Name:

Specified PC: IP Address MAC Address

IP Address: -

MAC Address:
(ex. 00e086710502)

Controlled Days: Sun Mon Tue Wed Thu Fri Sat

Start Blocking time: :00

End Blocking time: :00

Current Parent Control Table

4. Click on **“Enable Parental Control”** On/Off to enable the parental control function. Click on **“Apply”**.
5. At the **“User Name”** field add for example the user name of your child or the name of the device that will be used to rule.
6. For the specified device, add at the field **“Specified PC”** if you want to make the rule by **“IP-Address”** or **“Mac Address”**. You can enter these details in the below fields **“IP-Address”** or **“Mac Address”**.
7. Select which day you want to use the Parental Control Rule. Click on the day to enable this day.

8. Add a **“Start Blocking time”** so the router knows when to start with blocking the Internet access for the chosen device.
9. Add a **“End Blocking time”** so the router knows when to resume the Internet access for the chosen device.

8.0 Firewall

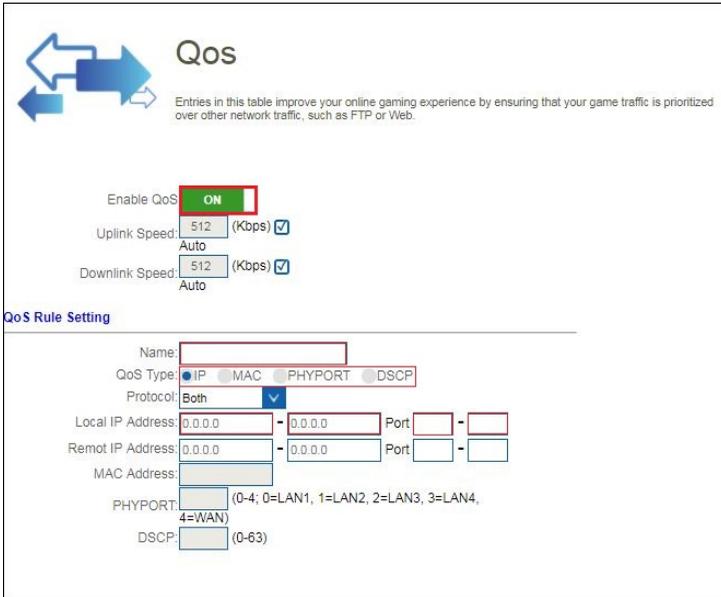
8.1 QoS

Thanks to QoS (Quality Of Service) you can make sure that a specific program or computer gets priority above other programs. By using this feature, you are certain that you will not get ‘lag’ in games or hitches during video playback, in case one of the computers starts to download.

10. Launch your internet web browser on your computer and type `http://192.168.8.1` in your browsers address bar.
11. Please enter the User Name: **admin** and Password: **admin** and then click on **“OK”** button.
12. From the left-hand menu, click on **“Firewall”** – **“QoS”**



You will see the following screen:



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Enable QoS: ON

Uplink Speed: (Kbps)

Auto

Downlink Speed: (Kbps)

Auto

QoS Rule Setting

Name:

QoS Type: IP MAC PHYPORT DSCP

Protocol:

Local IP Address: - Port: -

Remot IP Address: - Port: -

MAC Address:

PHYPORT: (0-4; 0=LAN1, 1=LAN2, 2=LAN3, 3=LAN4, 4=WAN)

DSCP: (0-63)

13. Enable **“QOS”**
14. Enter QOS Rule Name, for example PS4.
15. You have the option to make a QOS rule by **“IP address”**, **“Mac address”**, **“Physical LAN port”** and **“DSCP”**.
16. Once you have made the selection, select a QOS **“Mode”**.



Mode

Mode:

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

remark

remark dscp: (0-63)

SAVE

17. You can select **“Guaranteed minimum bandwidth”** so you are sure that your QOS rule always have a minimum bandwidth. Or you can select **“Restricted maximum bandwidth”** which means that this QOS will not exceed the maximum bandwidth which will be setup for this QOS rule.
18. Once you have selected the mode, please enter the **Up** and **Downlink Bandwidth** speed. This speed is listed in Kbps.
For example: 10Mbps = 10000Kbps
19. Click **“Save”** to add the QOS rule.

8.2 URL Filtering

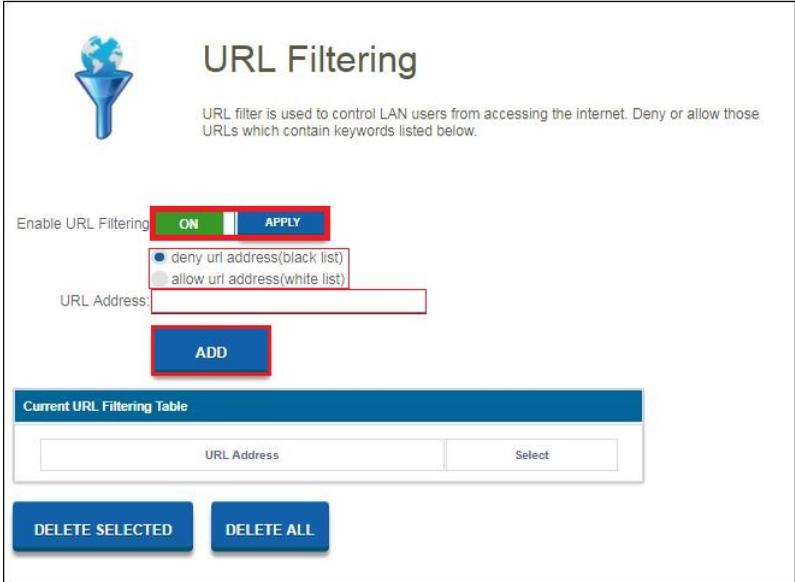
In some cases you will want to block access to the Internet. If, for instance, you have children, you may want to block some explicit websites. You can do this using the built-in URL filtering method.

Hint! For your own security the Firewall is enabled by default. We do however advise you to also use a virus scanner and always keep it up to date.

1. From the left-hand menu, click on **"Firewall" – "URL Filtering"**.



You will see the following screen:



URL Filtering

URL filter is used to control LAN users from accessing the internet. Deny or allow those URLs which contain keywords listed below.

Enable URL Filtering: ON OFF

deny url address(black list)
 allow url address(white list)

URL Address:

Current URL Filtering Table	
<input type="text"/>	<input type="text"/>
URL Address	Select

2. Click on the **On/Off** switch in the field **“Enable URL-Filtering”** and click **“Apply”**.
3. You have the option to **“deny”** (blacklist) or **“allow”** (whitelist) an URL address.
4. Enter the URL address which you want to whitelist or blacklist and click **“ADD”**.

8.3 IP Filtering

IP Filtering is a great way to limit access to your network for specific groups of IP addresses. For example if you had an attack from a certain IP address or you simple

do not want to grant access to Internet in your work facility you can easily add an IP filter so this IP address will be blocked and does not have access to your network.

1. From the left-hand menu, click on **“Firewall”** – **“IP Filtering”**.



You will see the following screen.



IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address:

Protocol:

Comment:

ADD

Current IP Filter Table			
Local IP Address	Protocol	Comment	Select

DELETE SELECTED

DELETE ALL

2. Click the On/Off switch in the field “**Enable IP filtering**”.
3. Enter the IP address which needs to be filtered.
4. You can also add a comment so you always know why this IP address needs to be filtered.
5. Once you have finished the settings, click “**ADD**”

8.4 MAC Filtering

With Mac filtering you will have more control over your network and who you will grant access to your network and internet.

1. From the left-hand menu, click on **"Firewall"** – **"MAC Filtering"**.



You will see the following screen.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering: ON OFF

MAC Address:

Comment:

Current MAC Filter Table		
MAC Address	Comment	Select

2. Click the On/Off switch in the field “**Enable MAC filtering**”. Click “**Apply**”
3. Enter the MAC address which needs to be filtered.
4. You can also add a comment so you always know why this MAC address needs to be filtered.
5. Once you have finished the settings, click “**ADD**”

8.5 Port Filtering

By Port filtering you can for example block a service to your network. For example if you want to block the access to the internet you can add a port filter so the clients on this network will not be able to browse on the internet.

1. From the left-hand menu, click on **“Firewall”** – **“Port Filtering”**.



You will see the following screen.

PORT Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering ON

Port Range: ~

Protocol: ▼

Comment:

ADD

Current Port Filter Table			
Port Range	Protocol	Comment	Select
<p>DELETE SELECTED DELETE ALL</p>			

2. Click the On/Off switch in the field **“Port filtering”**. Click **“Apply”**
3. Enter the Port range which needs to be filtered.
4. You can also add a comment so you always know why this Port needs to be filtered.
5. Once you have finished the settings, click **“ADD”**

8.6 Port Forwarding

The EM4720 has a built in firewall that protects your network by blocking unwanted traffic from the Internet. By Port Forwarding you instruct the router that all the data packets that come in on a specific port need to be forwarded to a specific device.

Examples:

- allow Internet users to browse or download on your local network (for example, by providing an FTP or HTTP server)
- play certain games which require accessibility from the Internet.

1. From the left-hand menu, click on “**Firewall**” – “**Port Forwarding**”.



You will see the following screen.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding: ON

Port Forwarding Table					
Local IP Address	Protocol	Internal Port	Remote IP Address	External Port	Comment
<input type="text"/>	Both	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="ADD"/>					

Current Port Forwarding Table							
Local IP Address	Protocol	Internal Port	External Port	Remote IP Address	Comment	Status	Select
<input type="button" value="DELETE SELECTED"/> <input type="button" value="DELETE ALL"/>							

2. Click the On/Off switch in the field **“Enable Port Forwarding”**. Click **“Apply”**
3. In the field **“Local IP address”** you can fill out the IP address of the computer for which you want to open the specific ports.
4. Enter the port of the service that need to be forwarded in the field **“Internal Port”**.
5. Fill out the same port in the **“External Port”** field.
6. You can also add a comment so you always know why this Port needs to be filtered.
7. Once you have finished the settings, click **“ADD”**.

Be aware, if you have connected your EM4720 behind another modem/router that your External IP address first needs to be forwarded in your modem/router otherwise your modem/router will still be the one that blocks the ports that you just have opened through your EM4720.

8.7 DMZ

A demilitarized zone (DMZ) is a security method for separating the internal LAN from untrusted external networks. So if you enable DMZ this will result that all ports will be opened from external network, example playing online games or transferring files via internet.

1. From the left-hand menu, click on **“Firewall”** – **“DMZ”**.



You will see the following screen.



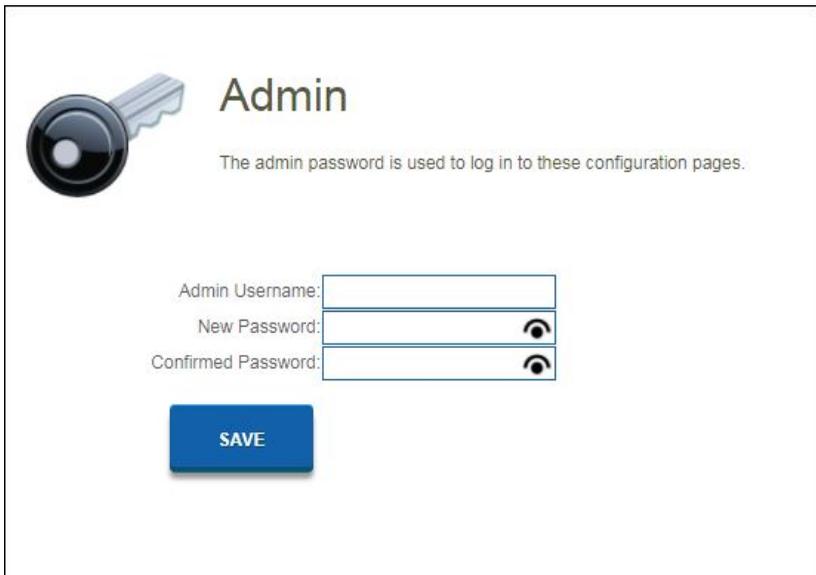
2. Click "**Enable DMZ**" if you want to open all ports to a specific computer and enter the IP-address of the computer in the field "**DMZ Host IP Address**"

3. Click "**Save** and **Reboot Now**".

9.0 Management

9.1 Admin

The admin password is used to log in to the routers configuration page.



The image shows a screenshot of a web interface for configuring the admin password. On the left is a key icon. The title "Admin" is displayed in a large font. Below the title is a descriptive sentence: "The admin password is used to log in to these configuration pages." There are three input fields: "Admin Username:" followed by a text box, "New Password:" followed by a text box with a visibility toggle icon (an eye), and "Confirmed Password:" followed by a text box with a visibility toggle icon. Below the input fields is a blue button labeled "SAVE".

9.2 Time and Date

You can maintain the system time by synchronizing with a public time server over the internet. You can manually add a time server or choose between the build-in time servers.



Time and Date

You can maintain the system time by synchronizing with a public time server over the Internet.

Manual

Enable NTP Server

• Server:

• Manual:

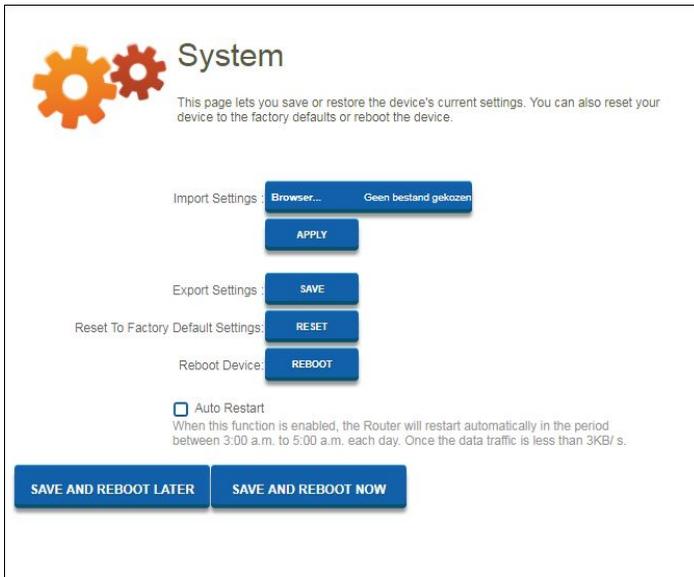
Automatically Adjust Daylight Saving

Time Zone:

Local Time: Tue Oct 31 11:53:11 2017

9.3 System

This page lets you save or restore the device's current settings. You can also reset your device to factory defaults or reboot your device.

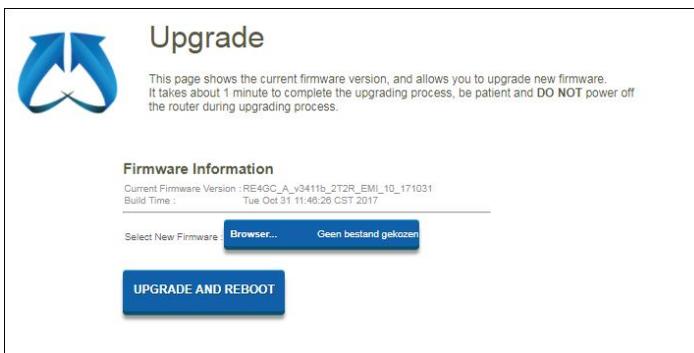


9.4 Upgrade

This page shows the current firmware version and allows you to upgrade to a newer version.

You can check our website <http://www.eminent-online.com> if there is a new FW version available. Once available you can download the file and open the file via the “**Browse**” button on the Upgrade page. Select the FW file which you have downloaded and click on “**Upgrade And Reboot**”

This will take approx. 1 minute to complete the upgrading process. During this process please do not power off your router.



10.0 Frequently Asked Questions and other related information

The latest Frequently asked questions for your product can be found on the support page of your product. Eminent will update these pages frequently to assure you have the most recent information. Visit www.eminent-online.com for more information about your product.

11.0 Service and support

This user manual has been carefully written by Eminent's technical experts. If you have problems installing or using the product, please fill out the support form at the website www.eminent-online.com/support.

You can also contact us by phone. Please check www.eminent-online.com/support for the helpdesk phone number and opening hours.

12.0 Warning and points of attention



Due to laws, directives and regulations set out by the European parliament, some (wireless) devices could be subject to limitations concerning its use in certain European member states. In certain European member states the use of such devices could be prohibited. Contact your (local) government for more information about this limitations.

Always follow up the instructions in the manual*, especially where it concerns devices which need to be assembled.

Warning: In most cases this concerns an electronic device. Wrong/improper use may lead to (severe) injuries!

When you connect the device to the mains, make sure it will not be damaged or subject to (high) pressure.

A power socket is needed which should be close and easy accessible from the device.

Repairing of the device should be done by qualified Eminent staff. Never try to repair the device yourself. The warranty immediately voids when products have undergone self-repair and/or by misuse. For extended warranty conditions, please visit our website at www.eminent-online.com/warranty.

Dispose of the device appropriately. Please follow your countries regulation for the disposal of electronic goods.

Please check below safety points carefully:

- Do not apply external force on the cables
- Do not unplug the device by pulling the power cable
- Do not place the device near heating elements
- Do not let the device come in contact with water or other liquids
- If there is any strange sound, smoke or odor, remove the device immediately from the power outlet.
- Do not put any sharp objects into the venting hole of a product
- Do not use any damaged cables (risk of electric shock)
- Keep the product out of reach of children
- Wipe off the product with soft fabric, not water mop.
- Keep the power plug and outlet clean
- Do not unplug the device from the power outlet with wet hands
- Unplug the device when you don't use it for a long time
- Use the device at a well ventilated place

**Tip: Eminent manuals are written with great care. However, due to new technological developments it can happen that a printed manual does not longer contain the most recent information. If you are experiencing any problems with the printed manual or you cannot find what you are looking for, please always check our website www.eminent-online.com first for the newest updated manual.*

Also, you will find frequently asked questions in the FAQ section. It is highly recommended to consult the FAQ section. Very often the answer to your questions will be found here.

13.0 Warranty conditions

The Eminent warranty applies to all Eminent products. After buying a second-hand Eminent product the remaining period of warranty is measured from the moment of purchase by the product's initial owner. Eminent warranty applies to all Eminent products and parts, indissolubly connected or mounted to the product it concerns. Power supply adapters, batteries, antennas and all other products not directly integrated in or connected to the main product or products of which, without reasonable doubt, can be assumed that wear and tear during use will show a different pattern than the main product, are not covered by the Eminent warranty. Products are not covered by the Eminent warranty when exposed to incorrect/improper use, external influences or when opening the service parts of the product by parties other than Eminent. Eminent may use refurbished materials for repair or replacement of your defective product. Eminent cannot be held responsible for changes in network settings by internet providers. We cannot guarantee that the Eminent networking product will keep working when settings are changed by the internet providers. Eminent cannot guarantee the working of web services, apps and other third party content that is available through Eminent products.

When my product gets defective

Should you encounter a product rendered defective for reasons other than described above: Please contact your point of purchase for taking care of your defective product.



Trademarks: all brand names are trademarks and/or registered trademarks of their respective holders. The information contained in this document has been created with the utmost care. No legal rights can be derived from these contents. Eminent cannot be held responsible, nor liable for the information contained in this document.



Eminent is a member of the Intronics Group