Contents

Router Login

To log into your router, connect your desktop computer or laptop via ethernet cable to the router's LAN port (or use Wi-Fi connection). To access and configure the router, open a web browser such as Google Chrome, Microsoft Edge, Mozilla Firefox, Opera or any similar application. Type **192.168.1.1** in the address bar of the browser. Image 1 illustrates the window that will appear on screen. In the Username field, type "**admin"**. In the Password field, type the password as it appears on the back of your router. Once all fields are populated, click **Login** button**.**

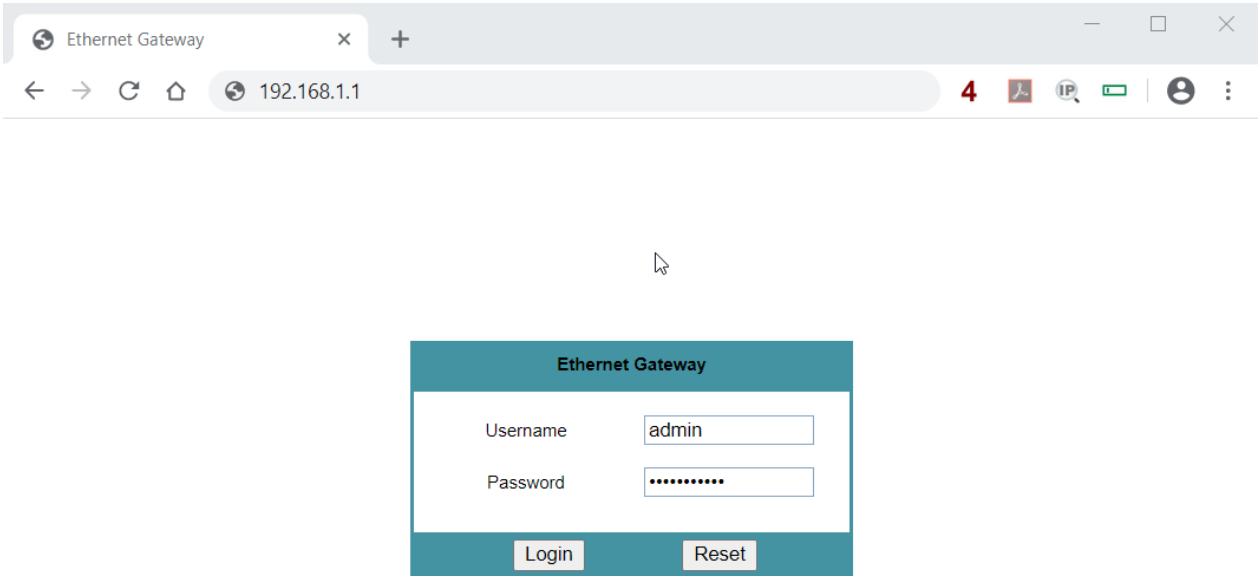


Image 1. Router HA-140W-B Login screen

Change of DNS (admin account)

To change your DNS properties for local LAN clients, log into your router (page 2) and go to **Network > LAN** (see image 2). By default, the router uses two Hyperoptic DNS servers. These servers communicate directly with the WAN ethernet router port and provide means for swift browsing. To define specific DNS, use fields **Primary DNS** and **Secondary DNS**. In these fields, enter the IPv4 address of your desired server (e.g. 8.8.8.8 or 8.8.4.4) and click **Save**. Click **OK** in the pop-up window to confirm router reboot and settings change.

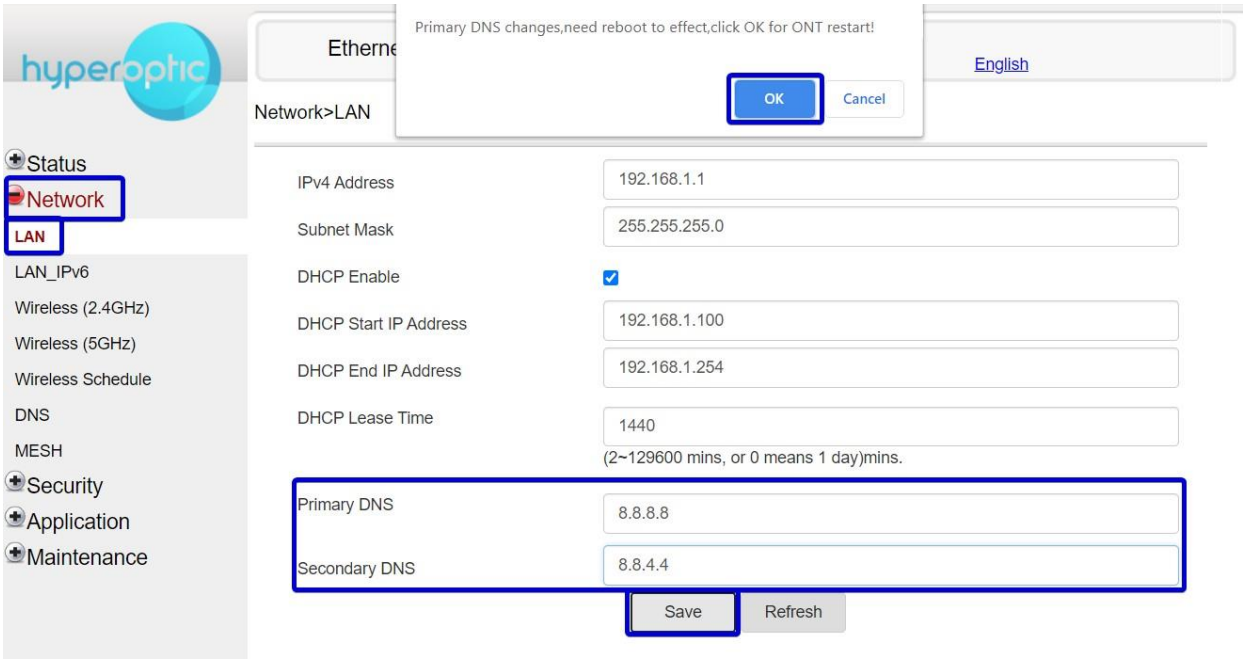


Image 2. Specifying DNS servers for LAN clients

UPnP router configuration (admin account)

To configure your router via UPnP LAN, log into your router (page 2). Go to **Application > UPNP and DLNA**. Tick **Enable UPnP/DLNA**. Click **Save/Apply (see image 3)**. UPnP can be used for easier and more convenient router configuration from an LAN client app. *PortMapper* Windows application is one example of such an app. If no UPnP application is used, UPnP should be unticked. The default UPnP setting is unticked. Please bear in mind that after a router reboot or factory reset, any changes made via UPnP will be removed from router configuration.

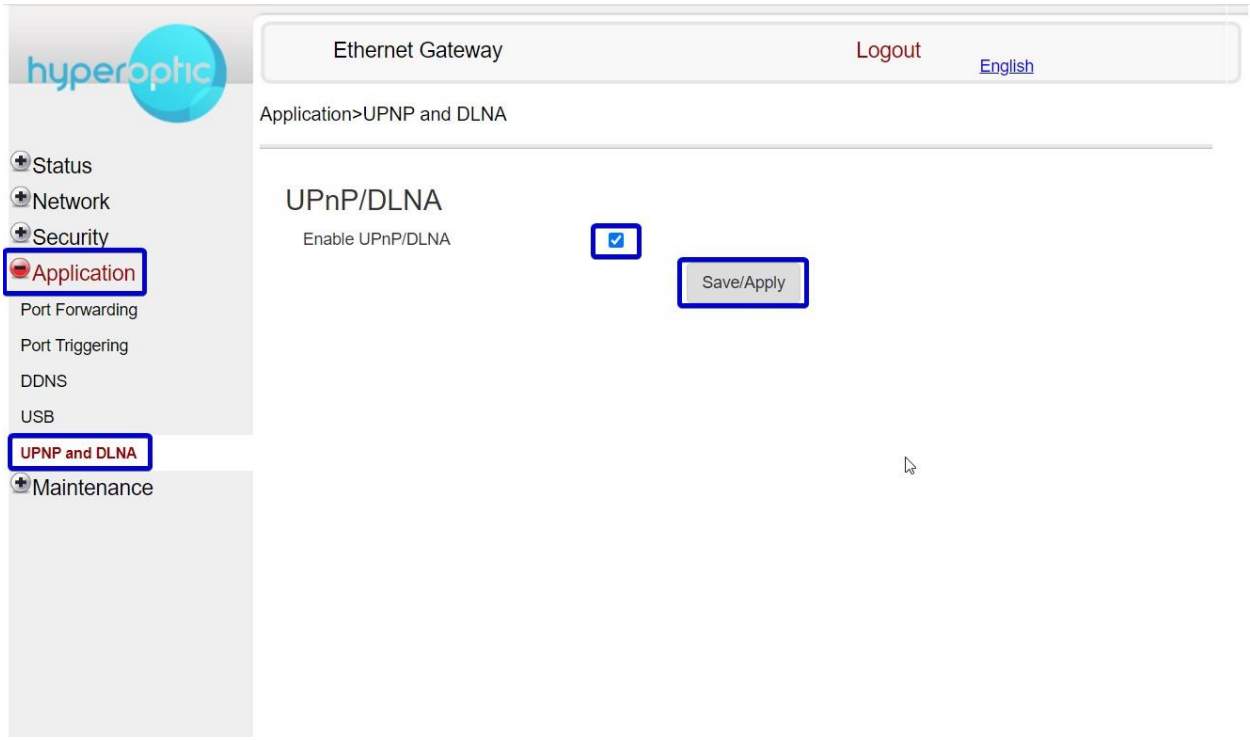


Image 3. Enabling UPnP

LAN clients (admin account)

To check the number of LAN clients connected, log into your router (page 2). To check leased IPv4 addresses and to check which clients are connected via ethernet or via Wi-Fi, navigate to section **Status > Home Networking** (see image 4). The **Local Devices** section will show all connected devices (i.e. all devices using the router's Wi-Fi and/or Ethernet network). The list of connected devices is refreshed every 60 seconds.

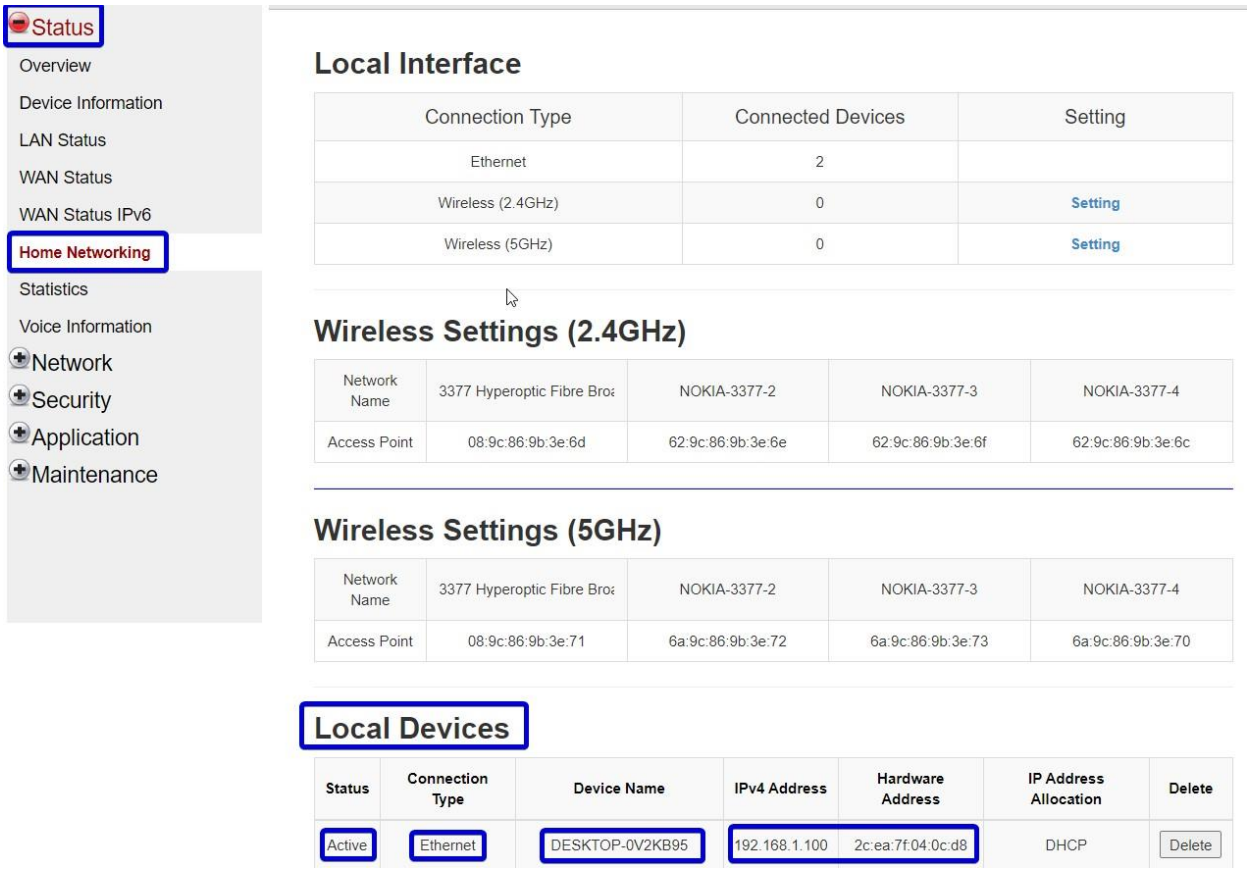


Image 4. List of WLAN and Ethernet LAN clients

Wi-Fi password and SSID change (admin account)

To change your SSID (i.e. the name of your Wi-Fi network) and/or Wi-Fi password, log into your router (page 2) and go to **Network > Wireless (2.4GHz) (see image 5) or Network > Wireless (5GHz) (see image 6).**

SSID name and **WPA Key** can be changed as desired. Don't forget to click **Save**.

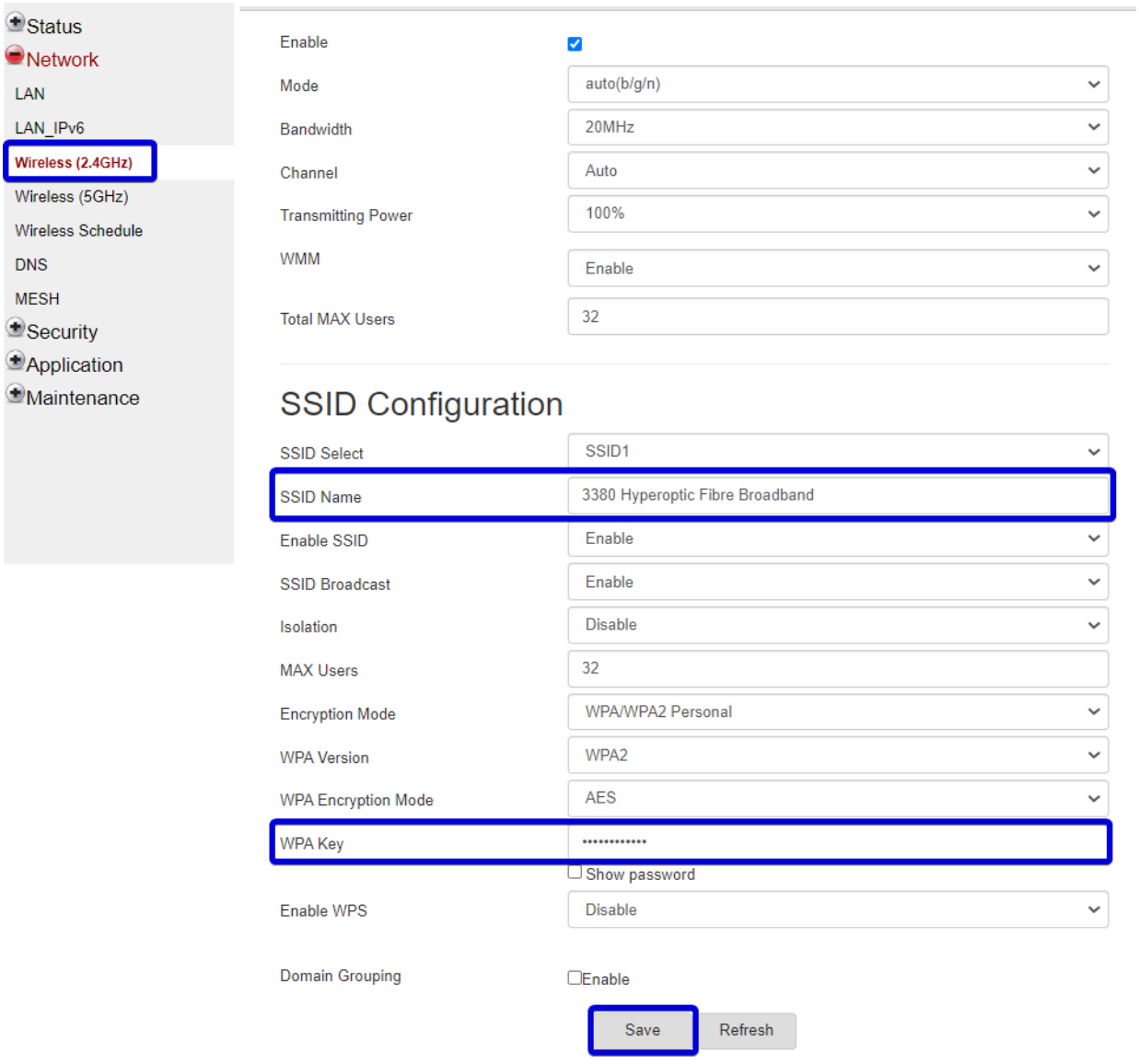


Image 5. Configuration of 2.4GHz Wi-Fi parameters

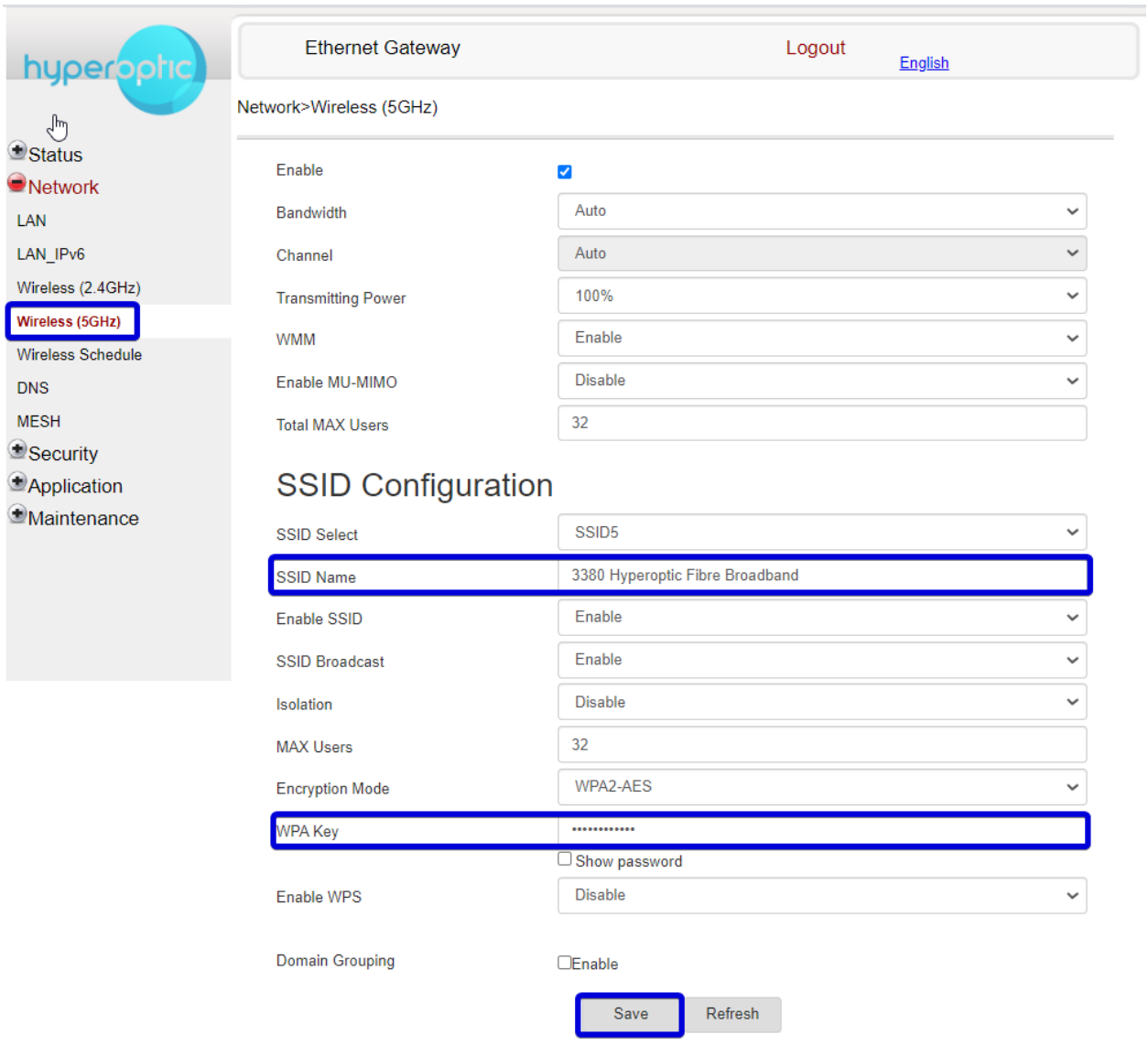


Image 6. Configuration of 5GHz Wi-Fi parameters

Creating, disabling and changing settings for SSIDs (admin account)

To create a new 2.4GHz SSID, log into your router (page 2) and go to **Network > Wireless (2.4GHz)**. Select **SSID2**, **SSID3** or **SSID4** from the dropdown menu of field **SSID Select**. Once new SSID is selected, you can change the name in the **SSID Name** field. You can set the password for that specific SSID in the **WPA Key** field. The SSID needs to be enabled by selecting the **Enable** option from the **Enable SSID** dropdown menu. If the SSID needs to be disabled, select **Disable** from the **Enable SSID** dropdown menu. Don't forget to click **Save**. See image 7.

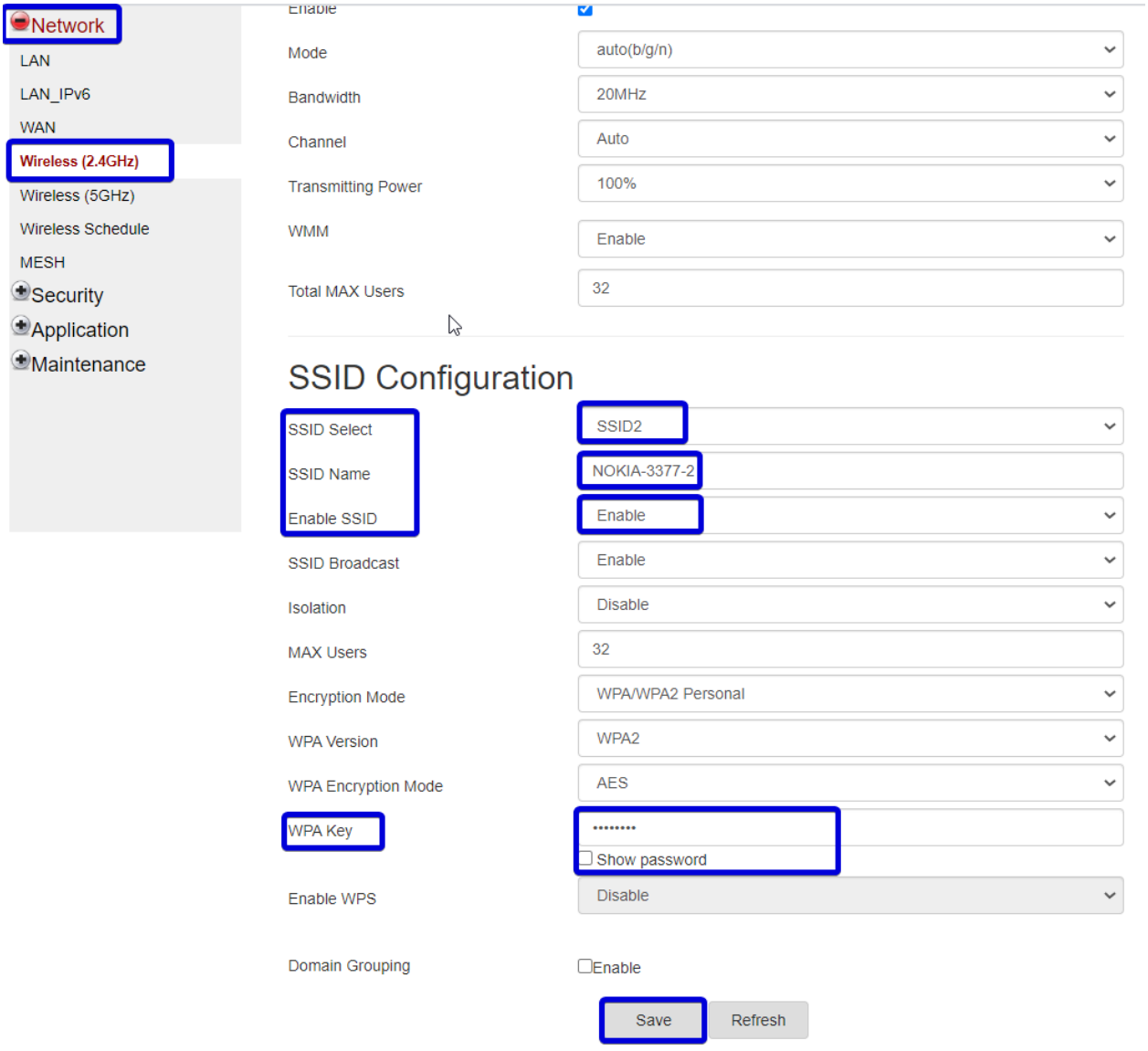


Image 7. Creation and modification of new 2.4GHz SSID

To create a new 5GHz SSID, log into your router (page 2) and go to **Network > Wireless (5GHz)**. Select **SSID6**, **SSID7** or **SSID8** from the dropdown menu of field **SSID Select**. Once new SSID is selected, you can change the name in the **SSID Name** field. You can set the password for that specific SSID in the **WPA Key** field. The SSID needs to be enabled by selecting the **Enable** option from the **Enable SSID** dropdown menu. If the SSID needs to be disabled, select **Disable** from the **Enable SSID** dropdown menu. Don't forget to click **Save**. See image 8.

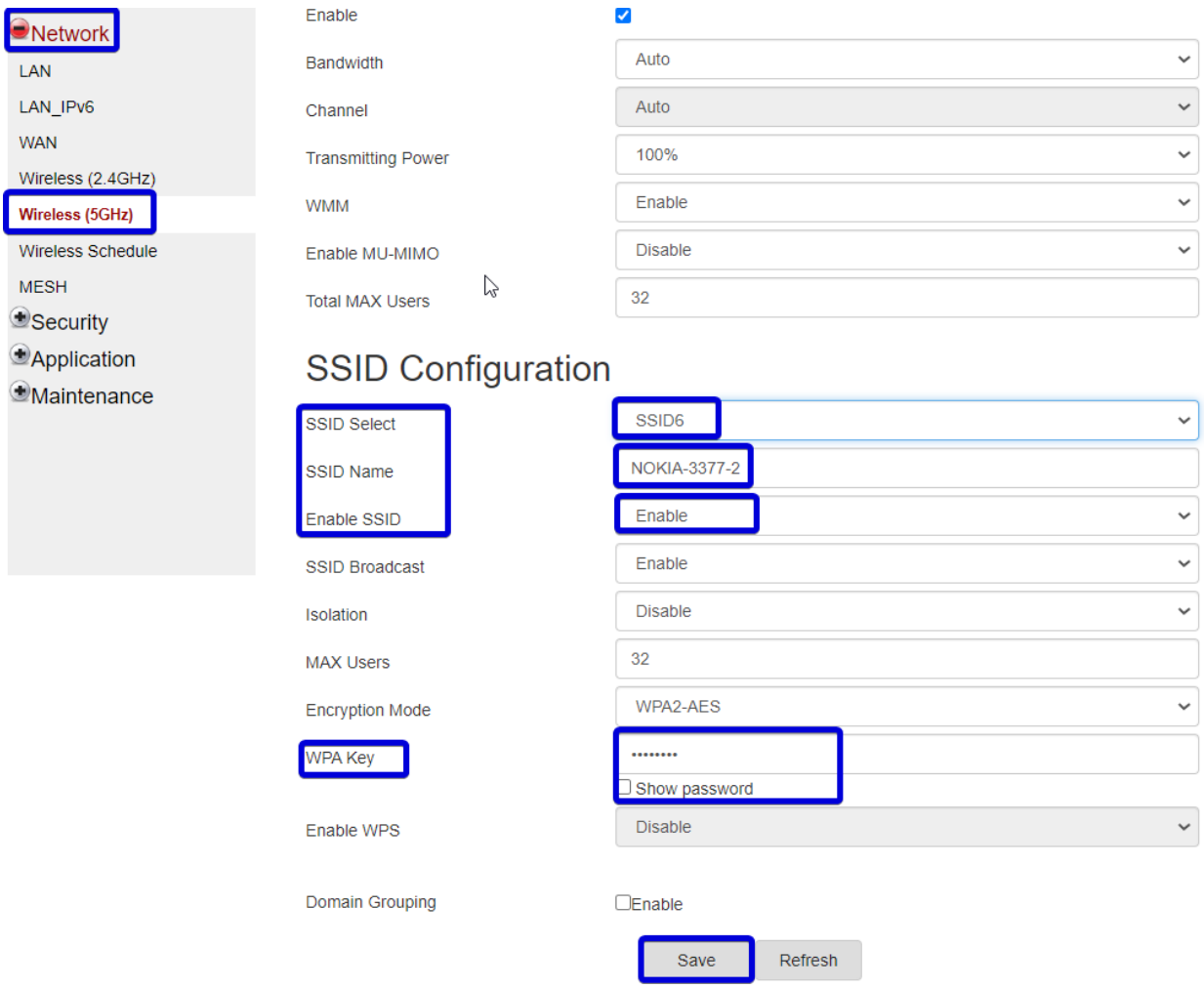


Image 8. Creation and modification of new 5GHz SSID

Wi-Fi channel change (admin account)

Your router continually and automatically changes Wi-Fi channel to minimise the level of interference to your connection. We strongly recommend keeping the automatic channel selection as is, but should you wish to change it manually, you can.

To change the operating channel of the 2.4GHz Wi-Fi network, log into your router (page 2) and go to **Network > Wireless (2.4GHz)**. In the **Channel** field, select your chosen channel from the dropdown menu (e.g. 11). Don't forget to click save. See image 9.

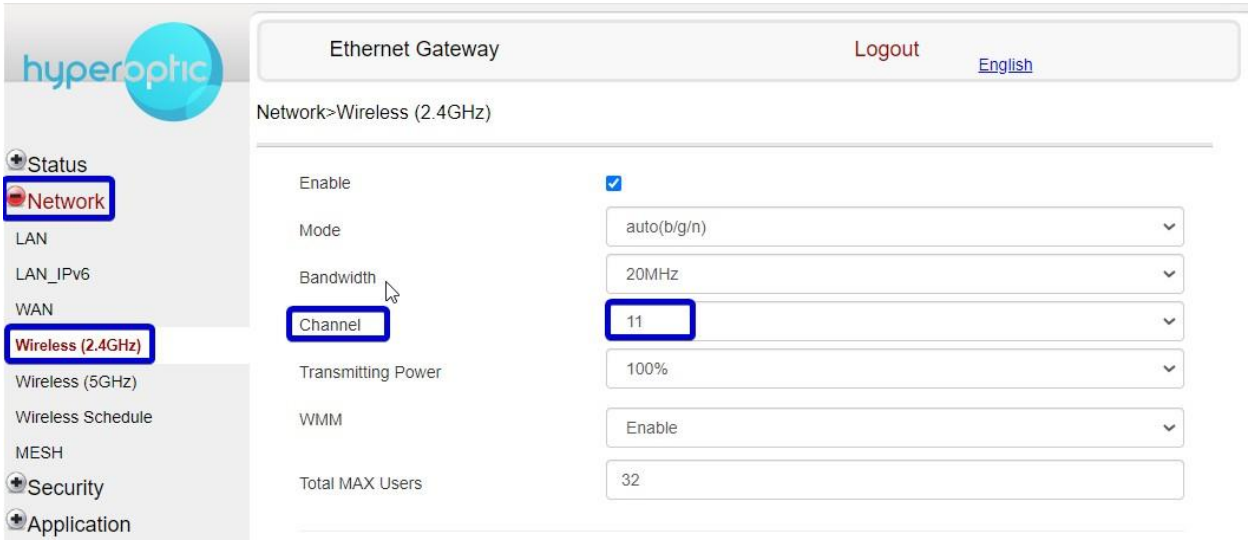


Image 9. Channel change in 2.4GHz Wi-Fi band

For the best performance on the 5GHz Wi-Fi network, select 80MHz in the **Bandwidth** field. After **Bandwidth** parameter is chosen from the dropdown menu, select channel from the section **Channel** (e.g. 36). See image 10. Click **Save** to apply changes.

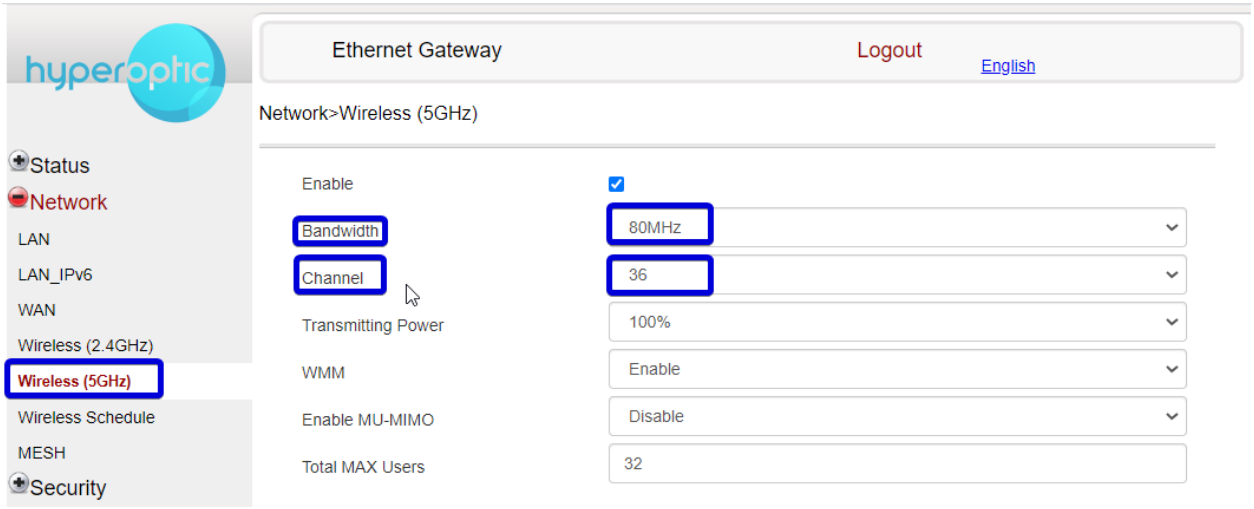


Image 10. Channel change in 5GHz Wi-Fi band

Wi-Fi security (admin account)

You can change the Wi-Fi security settings for each SSID. To do this, log into your router (page 2) and go to **Network > Wireless (2.4GHz).** Types of encryption parameters are seen in image 11. After selecting an **Encryption Mode** from the drop-down menu, click **Save**. By default, an advanced encryption algorithm is used. Similar settings exist in **Network > Wireless (5GHz)** section of router web UI. **We strongly recommend using only WPA2-AES for 2.4GHz and 5GHz.**

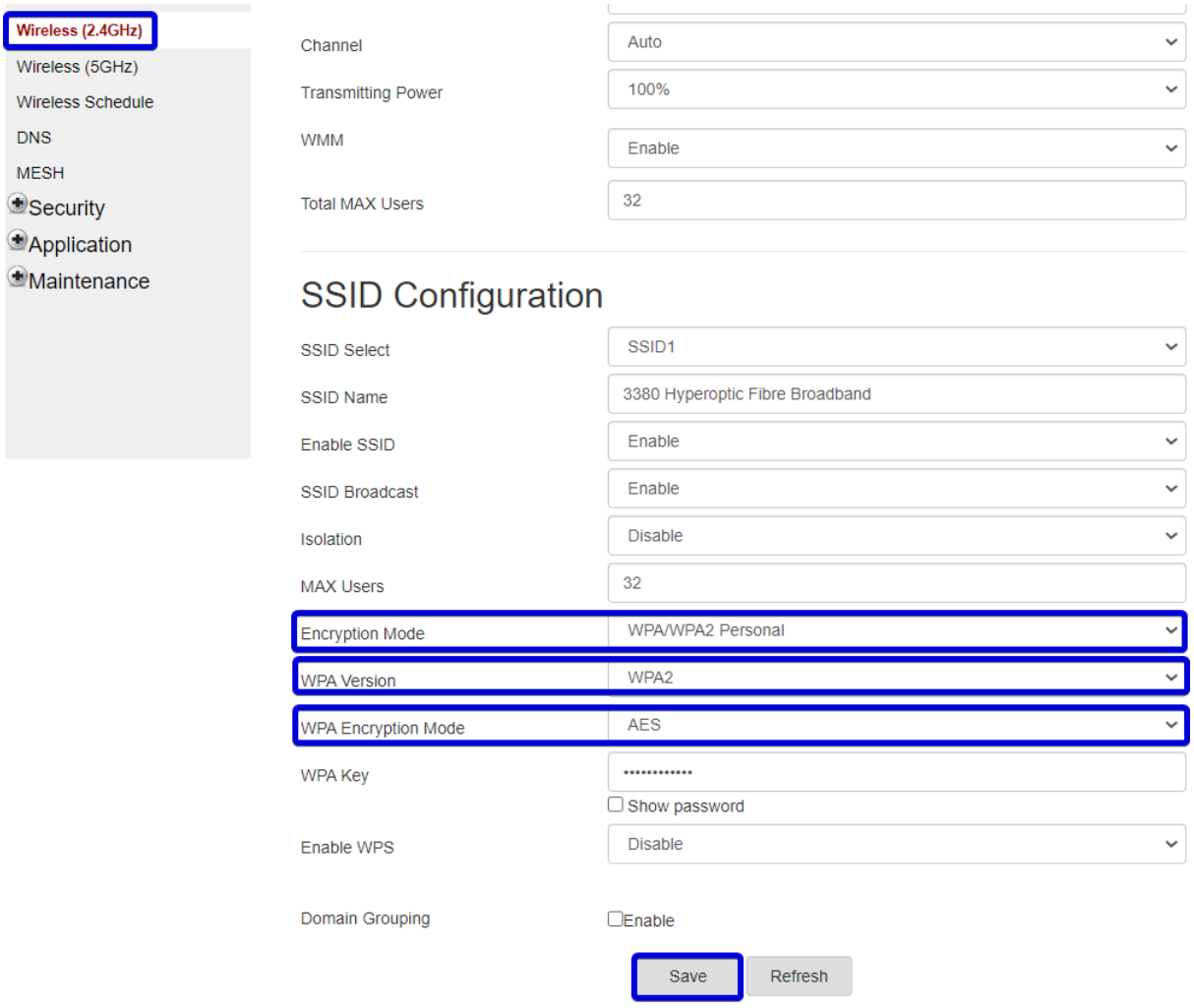


Image 11. Encryption types per SSID

WPS connection (admin account)

To allow LAN clients to connect to your Wi-Fi network without a password, log into your router (page 2) and go to **Wireless (2.4GHz)** or **Wireless (5GHz). Enable** WPS. See image 12. For WPS Mode, select **PBC** and click **WPS Connect** button. After few seconds press the WPS button on the LAN device and they'll connect.

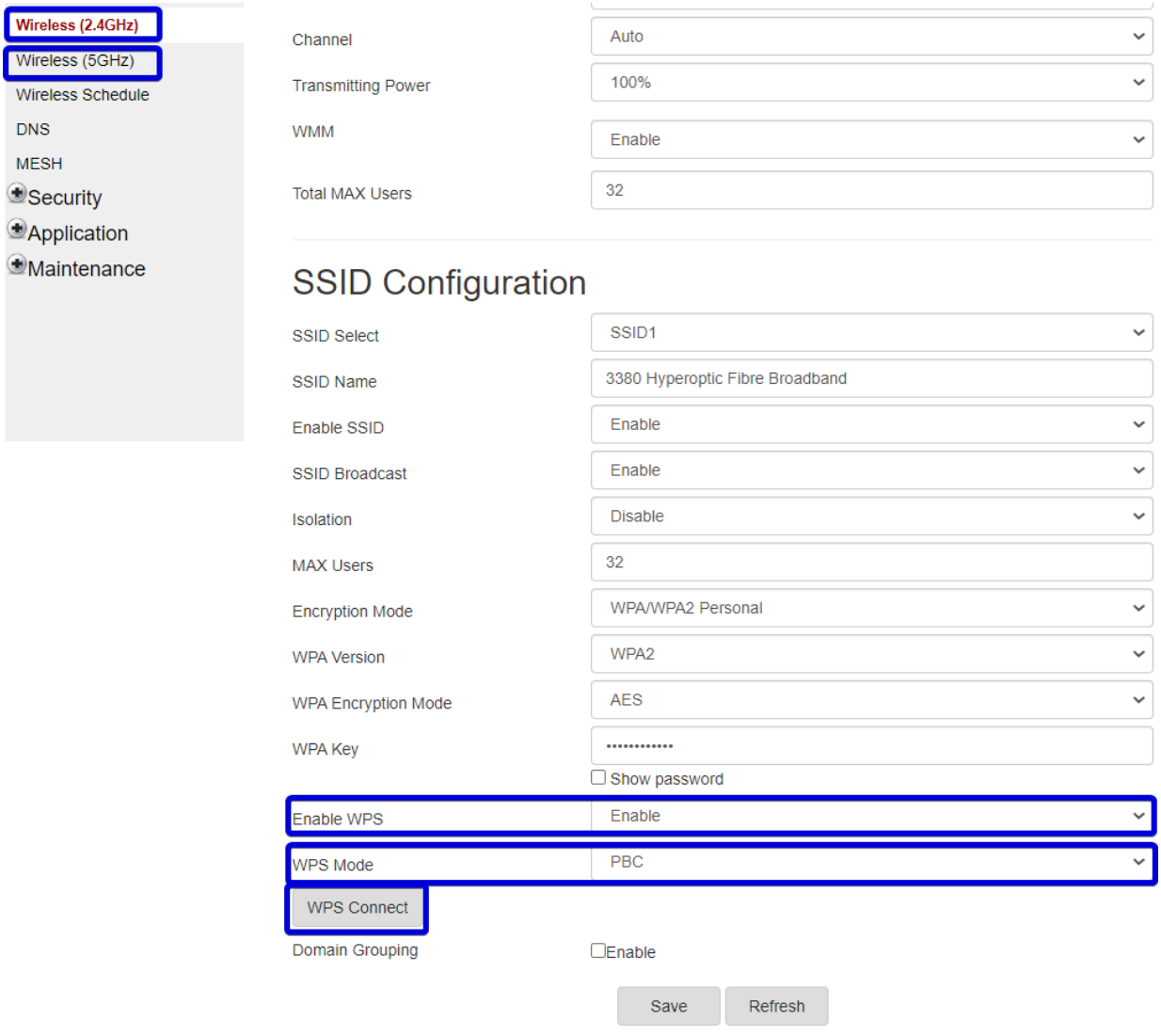


Image 12. Connecting LAN clients via WPS

Change of admin credentials (admin account)

To change the router admin login password, log into your router (page 2) and go to **Maintenance > Password.** See image 13. You can find the original password on the router itself. After entering and re-entering the new password, click **Save**.

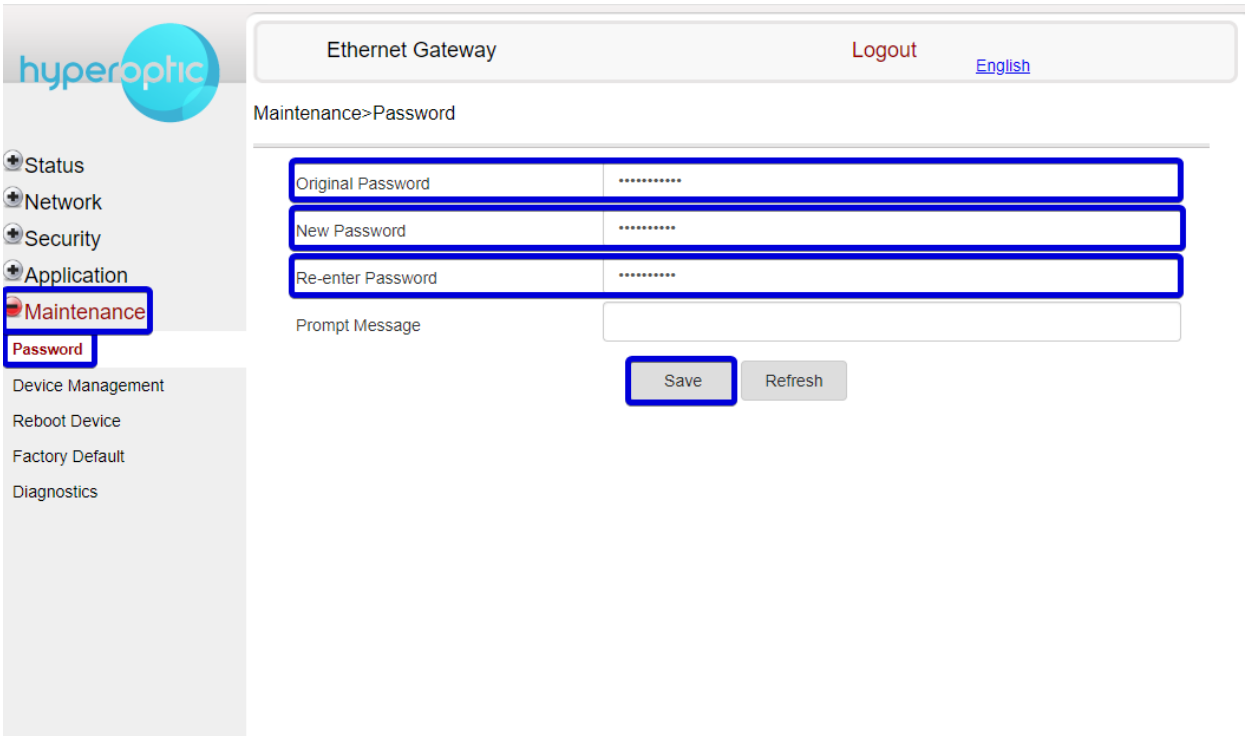


Image 13. Changing admin password

After the password's been changed, you'll see a confirmation screen (see image 14).

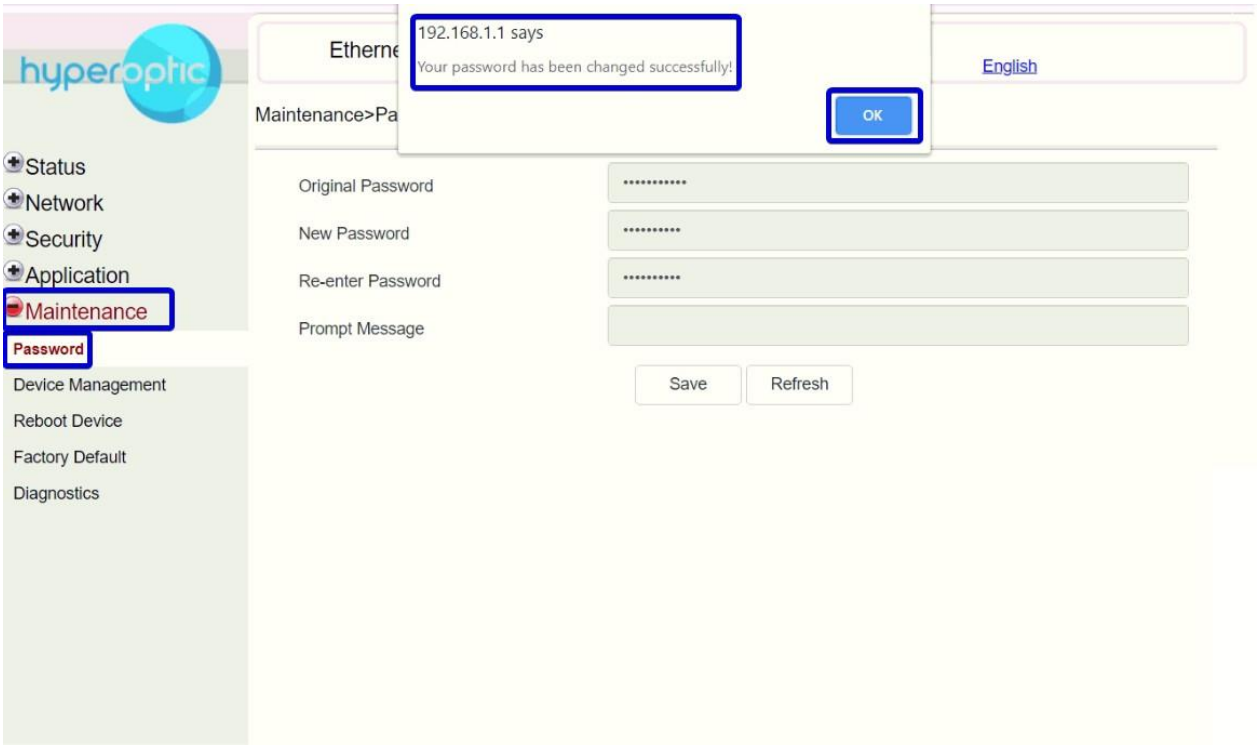


Image 14. Confirmation that password is changed successfully

Reboot and Factory Reset (admin account)

To reboot your router, log in (page 2) and go to **Maintenance > Reboot Device**. Click on **Reboot** (see image 15).

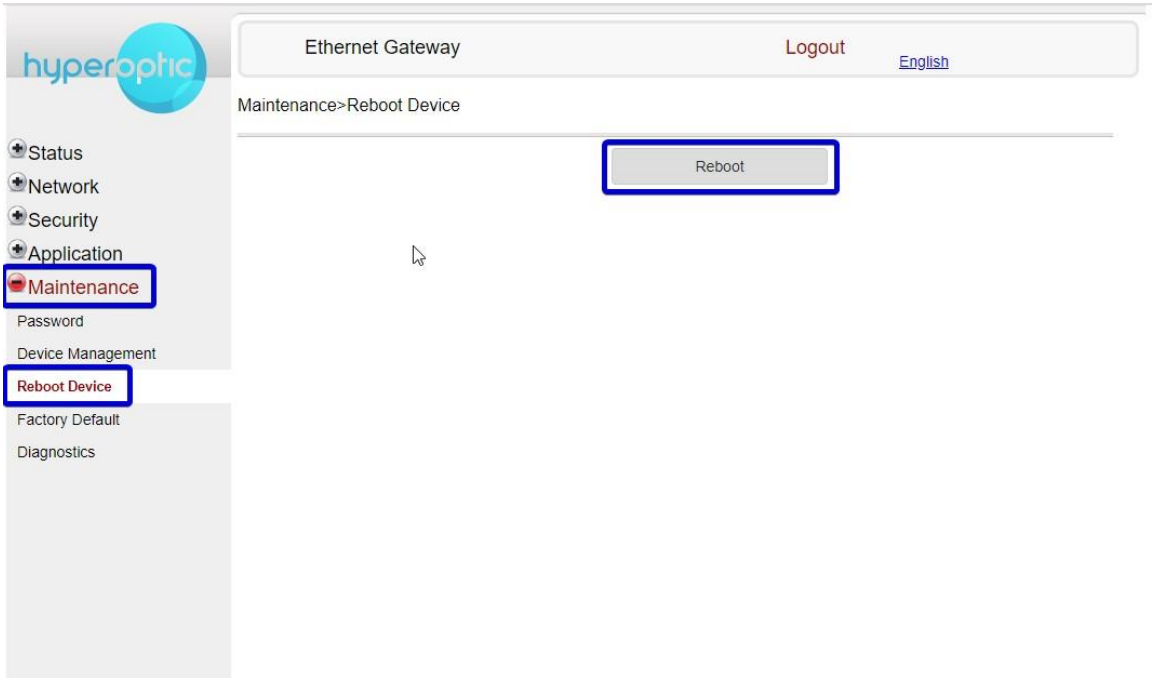


Image 15. Reboot and Factory reset buttons

Confirm the reboot by clicking **OK** (see image 16).

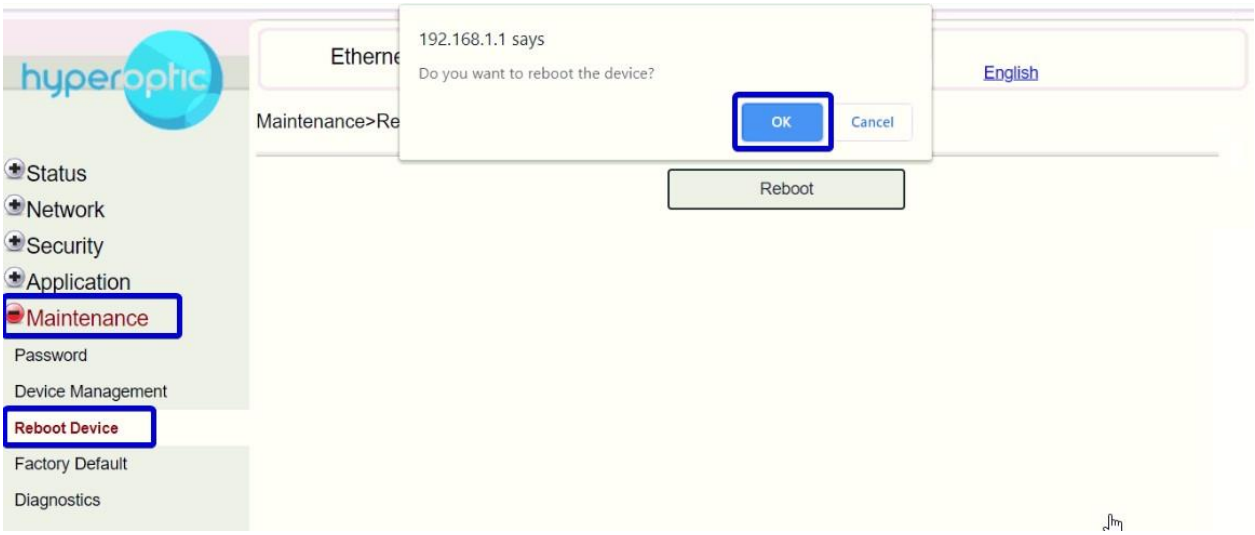


Image 16. Confirmation of rebooting

To perform a factory reset on your router, log in (page 2) and go to **Maintenance > Factory Default**. Click on **Factory Default** (see image 17). Please avoid using factory reset often as it can shorten the life of a router. Please also bear in mind that factory reset will override any of your personalised or previously saved settings.

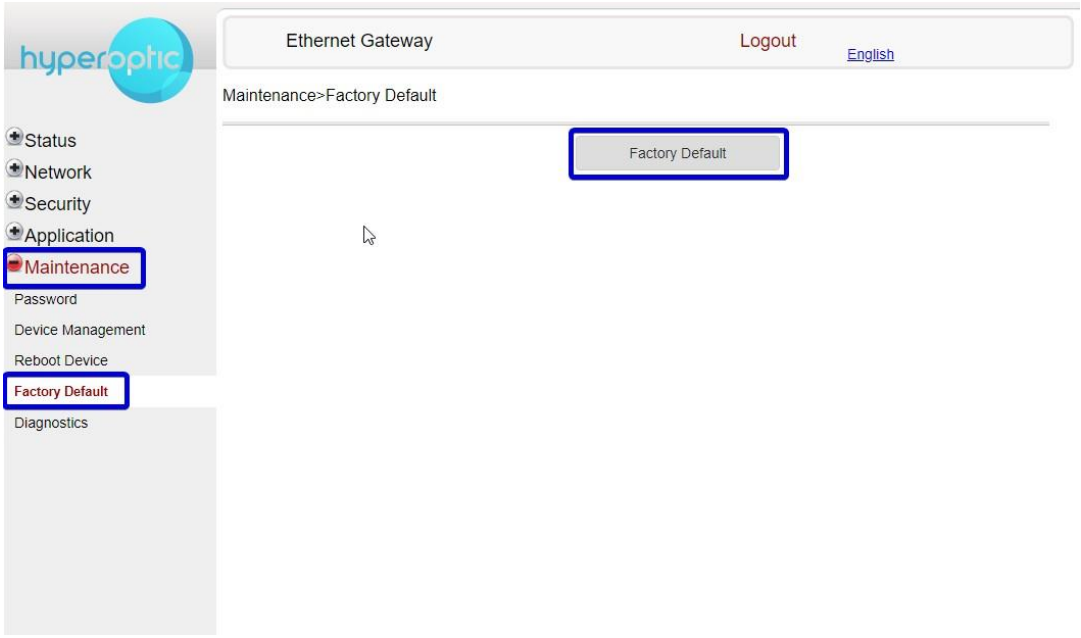


Image 17. Factory Default button

Confirm the factory reset by clicking **OK** (see image 18).

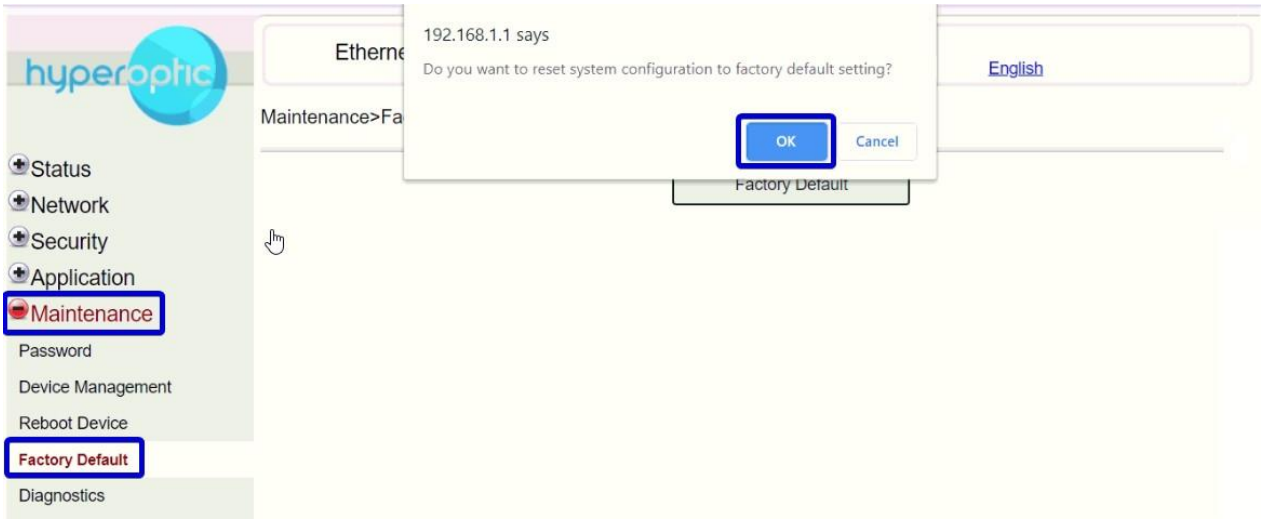


Image 18. Confirmation of factory reset

USB storage (admin account)

You can access USB flash storage from a LAN client and from the internet side (through WAN interface). To grant access to a USB flash drive, log into your router (page 2) and go to **Application > USB**. Tick **Enable FTP Server** to allow access from LAN clients. Set FTP password and username in appropriate fields. To allow access from the internet side, tick **Enable SFTP Server** and **Enable SFTP for Remote Access**. Set appropriate password and username for SFTP service. Click **Save** (see image 19).

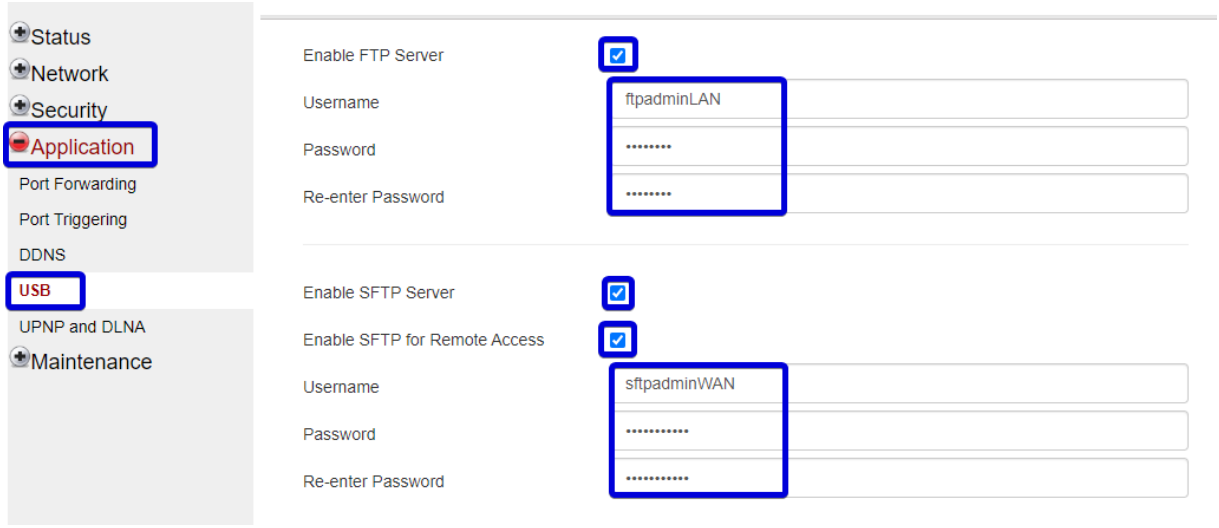


Image 19. Enabling FTP access to USB flash

Access to USB flash drive from LAN can be seen in image 20. FTP communicates over **TCP port 21**.

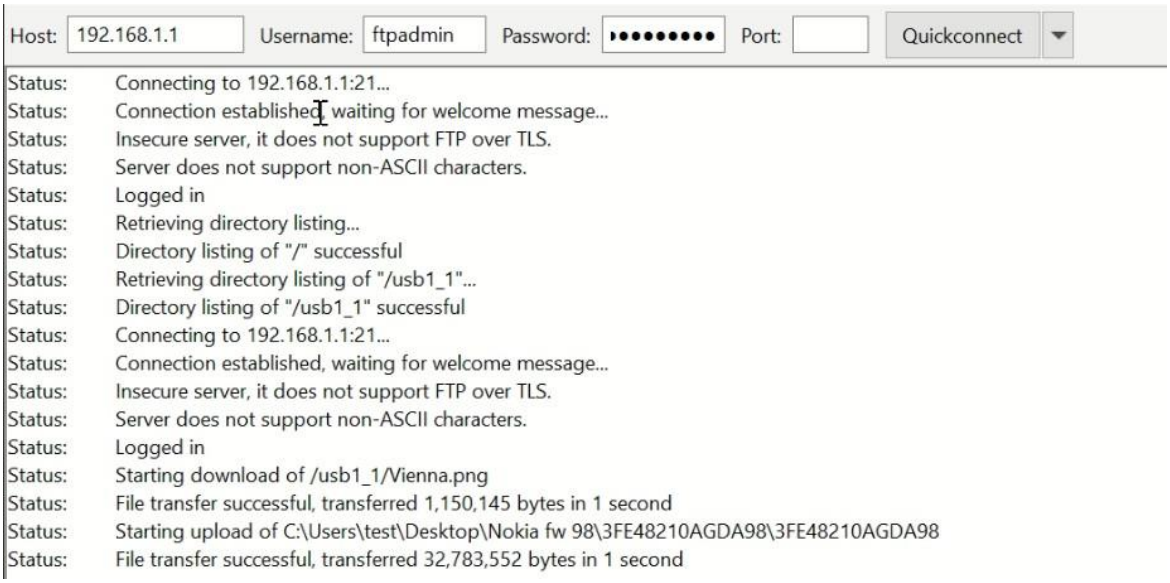


Image 20. Access to USB flash drive via FileZilla client app (from LAN)

Access to USB flash drive from WAN can be seen image 21. SFTP communicates over **TCP port 2122**.

Image 21. Access to USB flash drive via FileZilla client app (from WAN)

Port forwarding (admin account)

Port forwarding can be used to establish a home-based FTP server, web server or similar kind of a server. The server is located on the LAN client (e.g. desktop computer or laptop). To set Port forwarding, log into your router (page 2) and go to **Application > Port Forwarding**. See image 22.

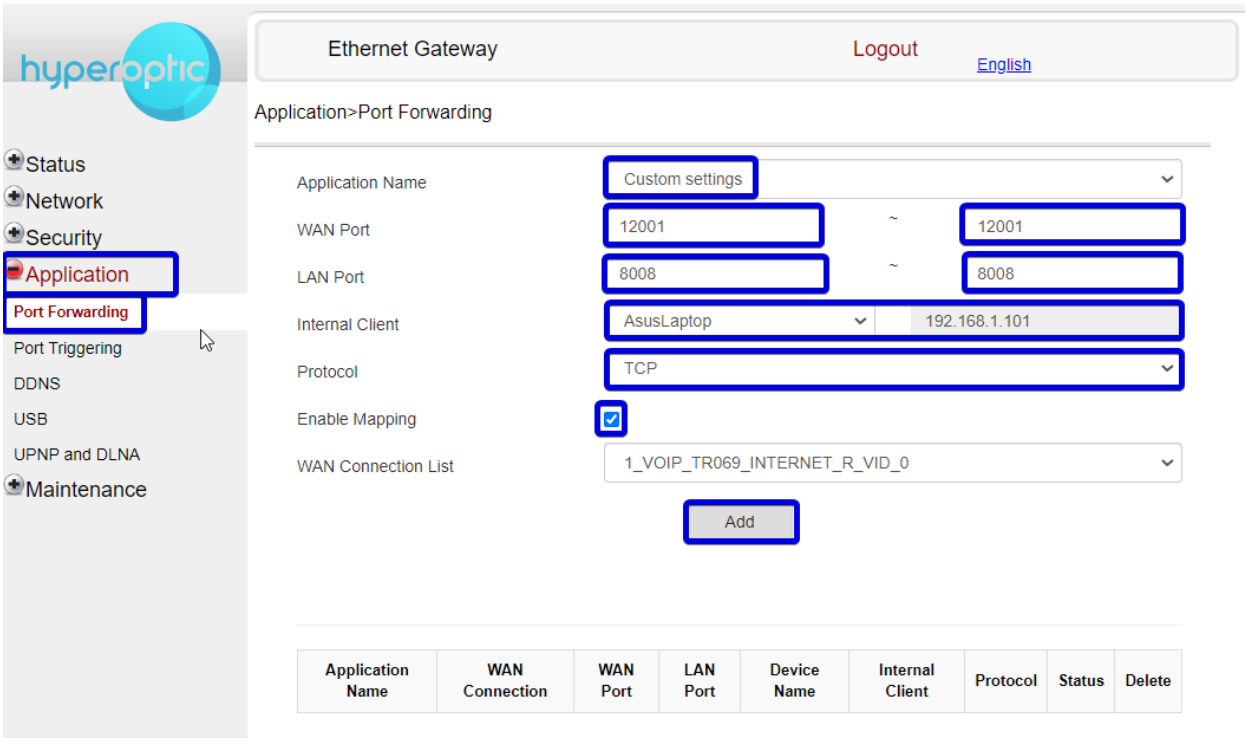
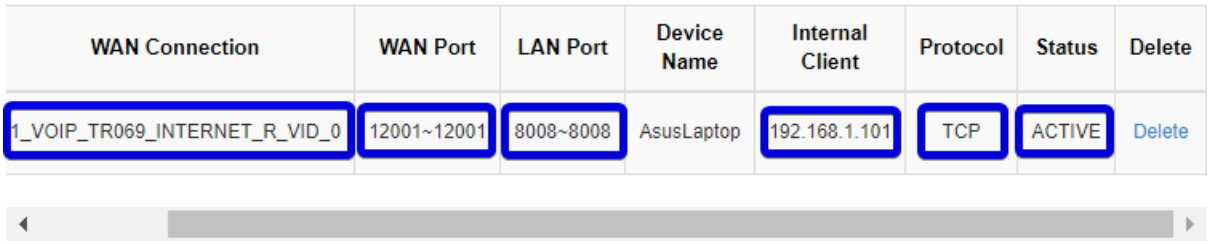


Image 22. Port forwarding configured with port mapping (WAN port maps to LAN port)

To set a specific port forwarding rule, select **Custom settings** for **Application Name** line. In the WAN Port field, set an arbitrary port on WAN interface of a router (e.g. TCP port 12001). All requests coming to the server from the internet side will have a destination IP address of the router itself, and a destination port as listed in **WAN Port** fields. For **LAN port** fields, list the port on which the LAN client server app is running (in this case TCP port 8008). Select the appropriate LAN client (server machine) from the dropdown menu on **Internal Client**. **Protocol** is determined by the type of server application (in this case **TCP**). Tick **Enable Mapping** and click **Add** to save the rule. Once rule is saved, you'll see the confirmation (see image 23).



WAN Connection	WAN Port	LAN Port	Device Name	Internal Client	Protocol	Status	Delete
1_VOIP_TR069_INTERNET_R_VID_0	12001~12001	8008~8008	AsusLaptop	192.168.1.101	TCP	ACTIVE	Delete

Image 23. Port forwarding rule confirmation

Similarly, ports on WAN and LAN side can be kept the same (see image 24). Image 24 shows the second way things can be configured. It's up to you whether you prefer to use the methods in image 22 or image 24.

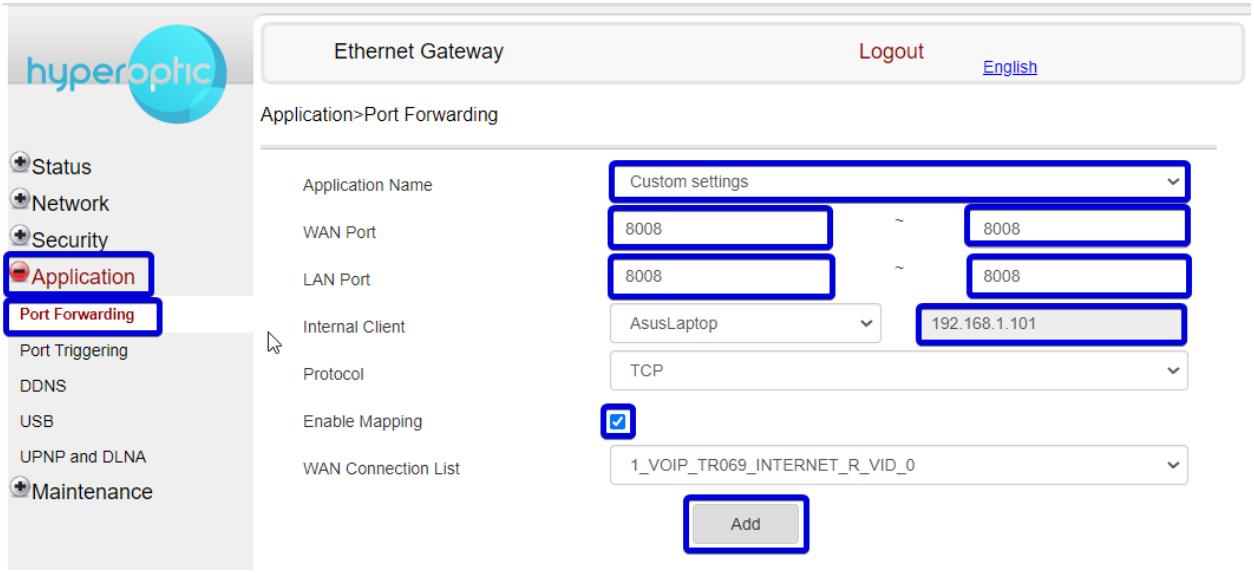


Image 24. Alternative approach of configuring port forwarding (LAN and WAN ports are the same)

Please also note that ports TCP 8080 and 443 **should never be used on WAN**, as these ports are reserved for Hyperoptic Ltd. remote management. If you'd like to use these ports on your server in a LAN, then you can use different ports on WAN as shown in Image 22 (e.g. you can use ports on WAN 12000, 12001 and map them to LAN ports 8080, 443 respectively).

A list of commonly used ports can be seen in image 25. For additional information on TCP/UDP port numbers, please refer to https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Port Number(s)	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
514	UDP	Syslog
16,384 – 32,767	UDP	RTP (voice, video)

Image 25. List of commonly used ports

DMZ (admin account)

Please be aware that devices placed in DMZ will not be affected by a router's firewall. Placing LAN devices in DMZ can therefore pose an IT security risk and this action should be taken with caution.

If a LAN device needs to be placed in a demilitarized zone, log into your router (page 2) and go to **Security > Firewall as seen in image 26**. Select **Advanced** option for **Security Level.** Click **Save** to apply settings.

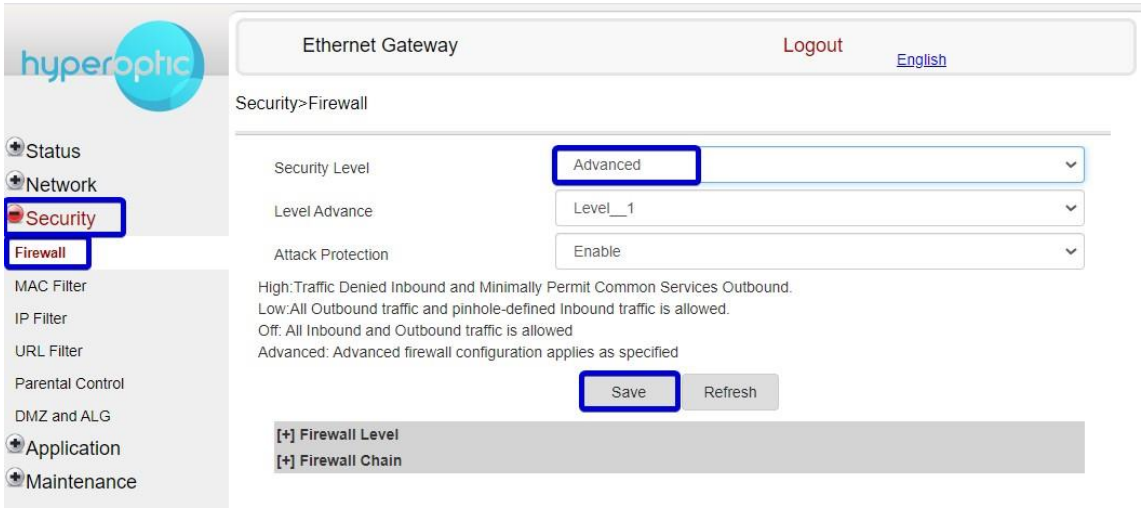


Image 26. Setting Firewall level to Advanced

Now, go to **Security > DMZ and ALG** (see image 27). Select LAN client from the **DMZ IP Address** dropdown menu. Tick **Enable DMZ** and click **Save DMZ**.

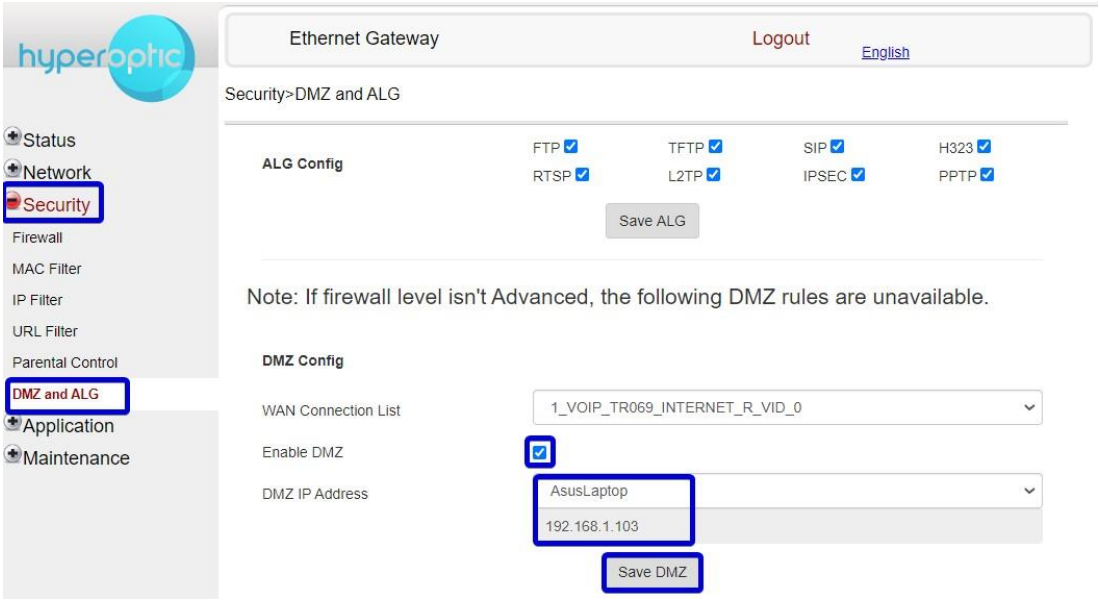


Image 27. Putting LAN client in DMZ

DHCP Binding (Admin account)

Specific LAN clients can have the same IPv4 address all the time. To define which LAN client will have which IPv4 address, DHCP binding must be completed. To do this, log into your router (page 2) and go to **Network > LAN**. Enter the MAC address of the LAN client and the desired IPv4 address. Click **Add** button to make changes. See image 28.

Image 28. Configuration of Static DHCP binding

Public IPv4 address block in LAN network

Navigate to section **Network > LAN**. Image 29 describes example of public block 137.220.108.0/29. Take first address from the IPv4 block and assign it to the router – **IPv4 Address** field. Rest of the available addresses define by setting **DHCP Start IP Address** and **DHCP End IP Address** values.

Table 1. Subnet mask values to be used in router config

Public IPv4 address block format	Subnet mask
x.x.x.x**/32**	255.255.255.**255**
x.x.x.x**/31**	255.255.255.**254**
x.x.x.x**/30**	255.255.255.**252**
x.x.x.x**/29**	255.255.255.**248**
x.x.x.x**/28**	255.255.255.**240**

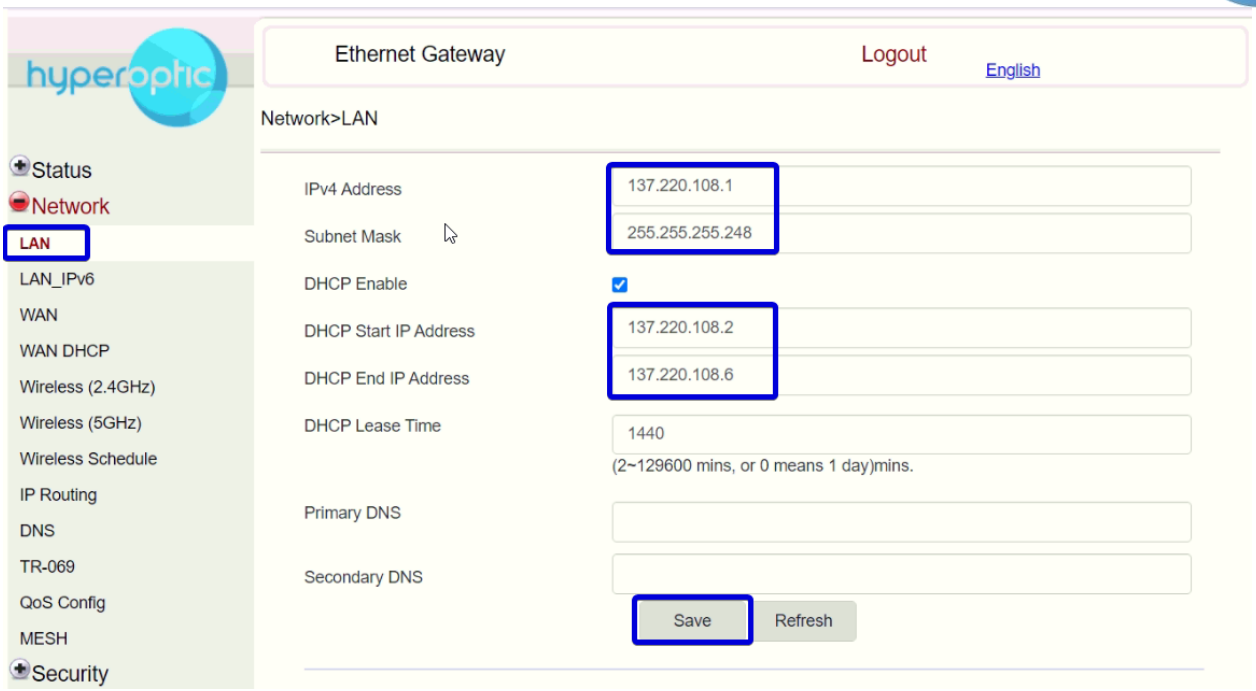


Image 29. Setting public IPv4 addresses for the LAN network

Once fields are populated click on the **Save** button. Router will notify that reboot is needed, click **OK** button to complete the setup, as per image 30.

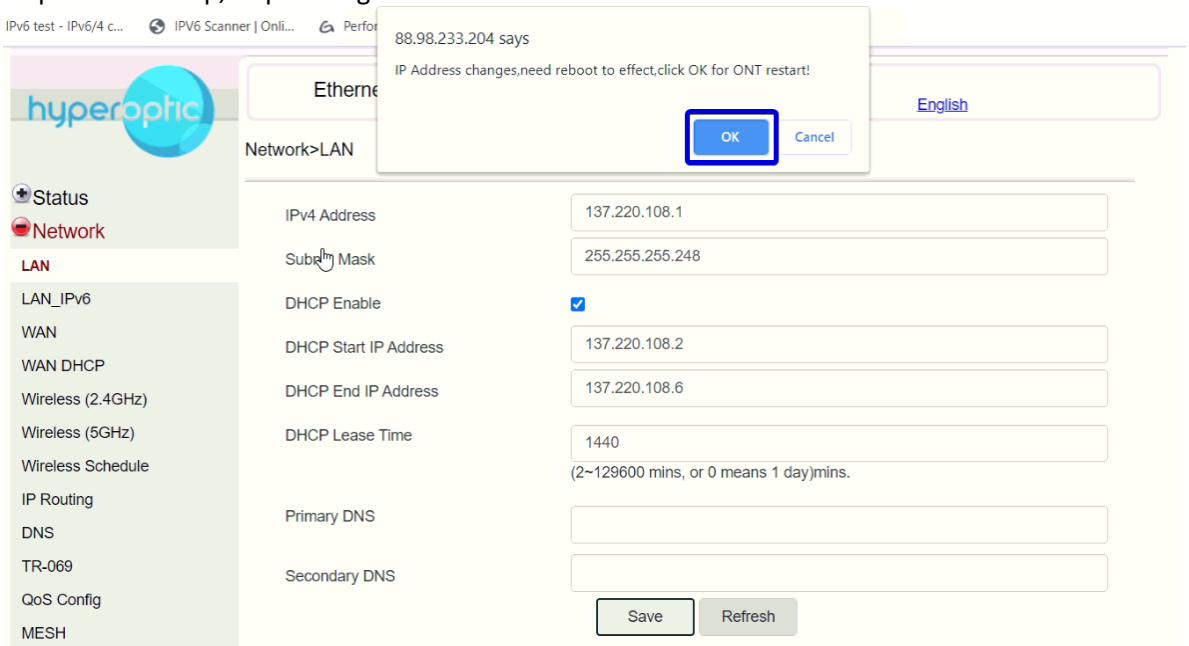


Image 30. Confirm reboot of the router

Last step is to disable NAT on the router (see image 31). To do this, navigate to section **Network > WAN** and uncheck **NAT** option. Click on the **Save** button at the bottom of the screen to save settings.

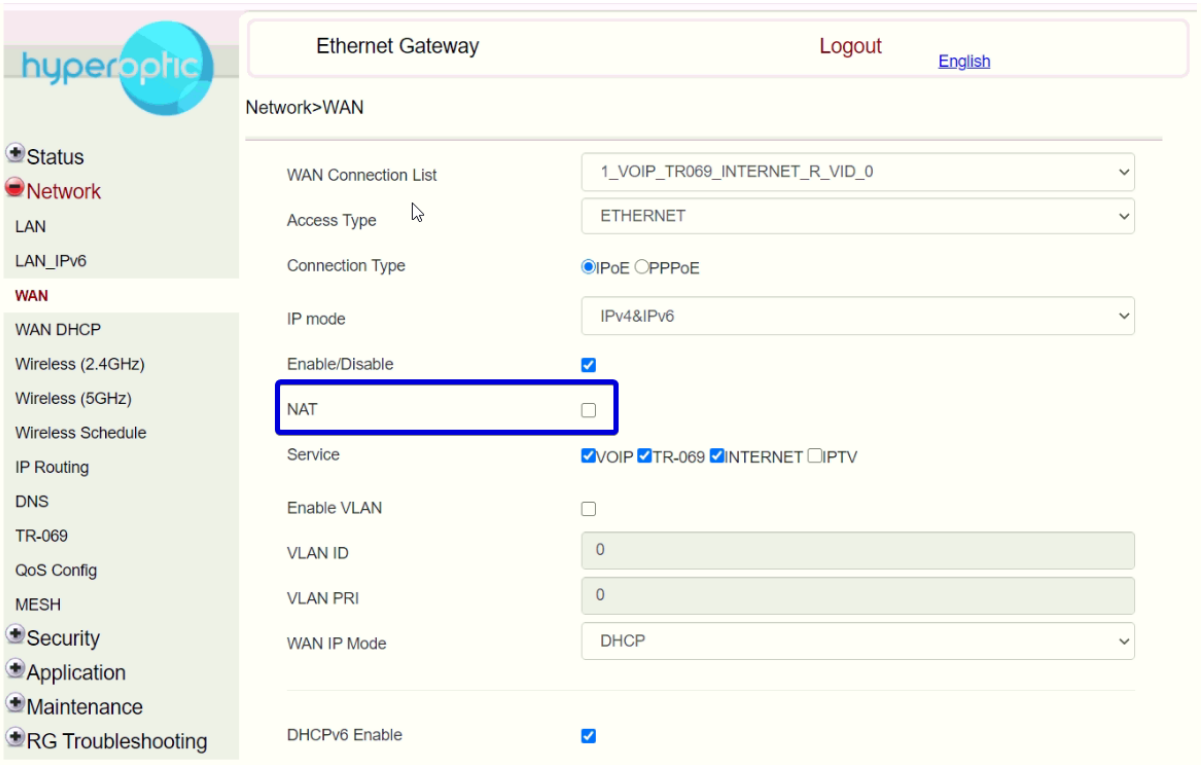


Image 31. Disabling NAT on the router