Siretta

Enabling Industrial IoT

QUARTZ-GOLD-5G

Compact 5G NR Gigabit Ethernet Industrial Router Range

Software Manual

Rev 1.0

Table of Contents

Introduction

This manual is intended to describe how to configure the QUARTZ-GOLD-5G NR compact cellular router into a computer network so that it may be used as the gateway router either to a WAN or the 5G NR / 4G LTE cellular network, with the option of automatic fallback between the two. To complete network configuration, it is required to use the QUARTZ-GOLD-5G built-in web server.

Three modes of routing operation are possible:

1. 5G NR / 4G LTE cellular router where the WAN connection of the router is the cellular interface. In this mode both Ethernet interfaces are for LAN use. Internet connectivity comes from the internal cellular interface.

2. WAN router where one Ethernet port of the router is used as the WAN connection and the other LAN. The WAN port in this case would normally be connected to a cable or ADSL modem to obtain Internet connectivity.

3. Backup router which combines the two above modes. The router can switch between the cellular and WAN connections automatically to maintain Internet connectivity if one path fails. The preferred route may be set to cellular or WAN.

About Siretta

Siretta is a wireless communications company located in Reading, United Kingdom manufacturing & supplying industrial IoT products since 1998.

Siretta's product portfolio is made up of:

- Antennas, plus their associated Cable Assemblies & Adapters,
- Cellular Network Analysers
- Industrial Modems
- Industrial Routers
- Associated Cloud Management

Siretta supplies products directly and via a worldwide network of distributors, into numerous markets and applications across the globe.

Siretta's distribution partners range from industrial IoT specialists through to global catalogue organisations.

Whether "off the shelf" or custom solutions are required, Siretta has a wide portfolio of products to fit many types of application.

Siretta's extensive knowledge and experience in the wireless market allows support of a wide range of customer applications, focusing on frequencies between 400 MHz to 6 GHz. These encompass modems, routers and antennas for:

- Cellular technologies: GSM / UMTS / LTE (including Cat M & NB) / 5G NR and other cellular technologies as they emerge.
- Global positioning: GPS/GNSS
- WLAN/Wi-Fi

Whilst providing the above products for the industrial cellular market, Siretta also has a number of antennas to cover applications for:

- Bluetooth, Zigbee, ISM band, LoRa and Sigfox

With a heavy emphasis on design, Siretta has a team of dedicated Engineers and Product Managers, who specialise in wireless applications.

Siretta continually makes significant investment in R&D endeavouring to provide customers with market leading, future-proofed, wireless solutions. Siretta works closely with many technology partners to stay at the forefront of industrial IOT.

Features

Operating System

- Linux based Operating System

Network Protocols

- IPv4
- IPv6 (Cellular WAN only)
- PPPoE
- PPP
- UDP/TCP/ICMP/NTP/DHCP
- UPnP/NAT-PMP
- HTTP/HTTPS
- SNMPv3

VPN

- GRE (up to 8 tunnels)
- OpenVPN Client (up to 2 clients)
- PPTP/L2TP Client (up to 10 clients with backup/failover scheduling)
- L2TP V3 (up to 5 tunnels and 10 sessions)
- IPSec (up to 2 clients with backup/failover scheduling)

Router Management

- Local/Remote GUI
- Whitelist of allowed remote management IP addresses
- Telnet/SSH
- TR-069 Zero Touch configuration
- Cloud based M2M management platform
- Scheduled reboot
- Activity logging internally and to external SysLog server
- Factory default and user default reset settings

WiFi Modes

- 2.4 GHz IEEE 802.11b/g/n
- 5 GHz IEEE 802.11a/ac
- Up to 8 SSIDs
- Wireless Site Survey

WLAN Modes

- Access Point
- Wireless Client
- Wireless Ethernet Bridge

WiFi Security
- WPA Personal
- WPA2 Personal
- WPA/WPA2 Personal

Cellular
- Network steering
- Cellular operator steering
- SMS control of router
- Cellular connection failure monitoring
- Support for fixed IP address SIM
- View incoming SMS messages

Firewall
- IP filter
- MAC filter
- Port filter
- Key Word filter
- URL filter
- Domain name filter whitelist/blacklist
- Ingress and egress filtering

Network Monitoring
- ICMP Check with programmable packet sizes
- Traffic statistics
- Traceroute
- Packet Capture compatible with Wireshark
- Real Time interface bandwidth measurement and graphing
- Real time data traffic graphing by IP address

Network Features
- DHCP Server with static DHCP addresses
- Support for up to 4 Subnets
- Cellular/WAN Failover
- Up to 16 VLANs
- Dynamic DNS (2 services allowed)
- Bandwidth Management by limiting and priority
- Static NAT/DMZ with access whitelist and remote configuration bypass options
- IP Passthrough
- Port Forwarding / Port Redirection
- Triggered Port Forwarding
- Static / Dynamic routing (OSPF/RIP)
- Policy-based routing
- UPnP & NAT-PMP
- VRRP

Network Features

- NTP with user programmable servers
- SNMPv3 with option for remote access by whitelisted IP addresses
- Spanning Tree
- Wake-on-LAN
- Captive Portal
- Serial (and optionally Modbus, as an order option) to TCP/IP with optional heartbeat and caching
- AT Commands over IP to control the cellular engine

Ordering Information

Compact Industrial 5G Quad Gigabit Ethernet Router

QUARTZ-GOLD-21-5G (GL) - Stock Code 61901
QUARTZ-GOLD-21-5G (GL) + ACCESSORIES - Stock Code 61902

Dual WiFi Compact Industrial 5G Quad Gigabit Ethernet Router

QUARTZ-GOLD-W21-5G (GL) – Stock code 61867
QUARTZ-GOLD-W21-5G (GL) + ACCESSORIES - Stock Code 61896

All routers may be ordered with RS485/Modbus serial interface. This is an optional feature. Please contact Siretta sales for details.

The accessories kit contains all the other components required to be able to use the router:

- 2 swivel joint WLAN antennas (Wi-Fi models only)
- 4 swivel joint Cellular antennas supplied with detachable magnetic mount bases with 3m of cable
- RJ45 Ethernet cable
- Multi-region 2A, 12V power supply

Configuration

Router Setup

The QUARTZ-GOLD-5G must be configured either using a web-based GUI or by a CLI (Command Line Interface) before being used. As received, this will need to be done with a local connection between a LAN port of the QUARTZ-GOLD-5G and a PC using an Ethernet cable. However, the router may be configured for remote access subsequently (see Administration > Admin Access).

IMPORTANT: For use as a cellular router, a functioning SIM card must be used (See QUARTZ-GOLD-5G hardware manual for details of fitting). Additionally, the APN and any user name and password required to be able to use the SIM needs to be entered (see Basic Network > Cellular).

Connecting to the QUARTZ-GOLD-5G NR router

Basic Settings

To configure the QUARTZ-GOLD-5G, access the webserver integrated into the router. Do this with a wired Ethernet connection to the router (using one of the two LAN ports). When connecting to the QUARTZ-GOLD-5G for the first time, the computer used should be assigned an IP address from the routers built in DHCP server. Note that Windows PCs can be reluctant to change IP address sometimes. Windows reboot in this case is the easiest way to clear this problem if it occurs.

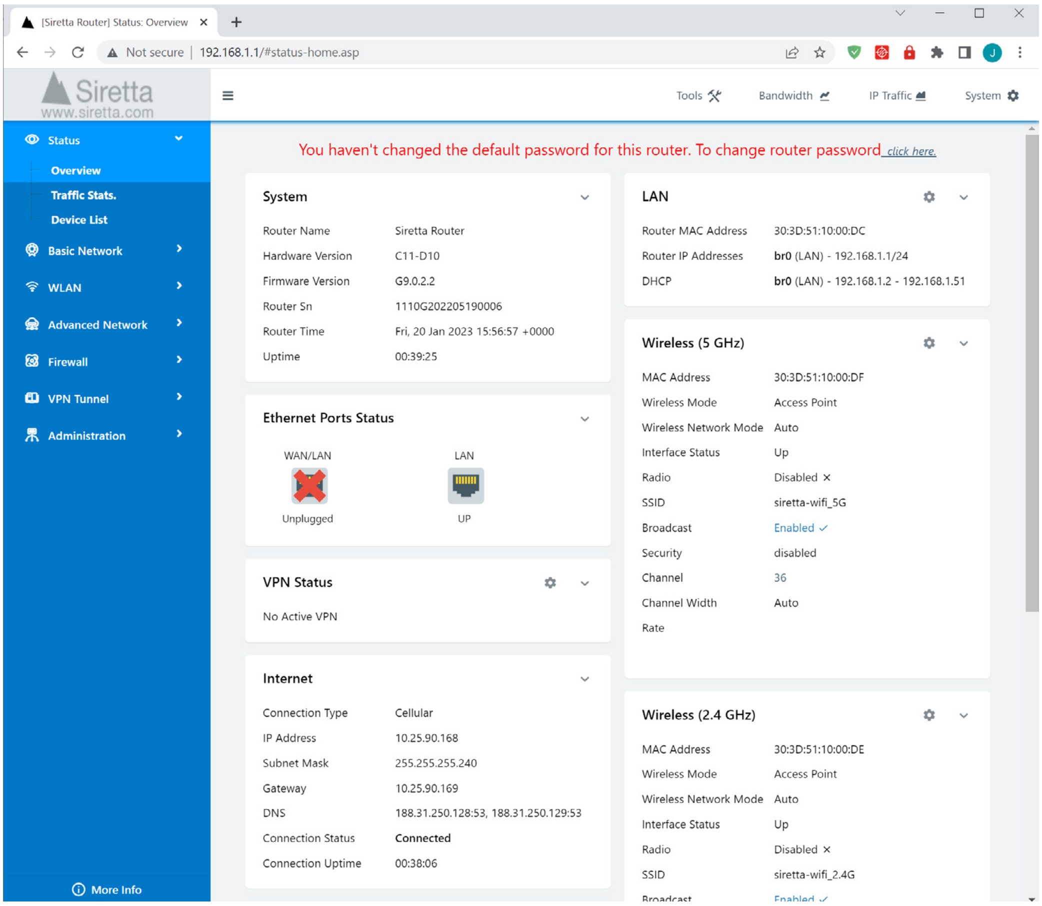
When connecting to the router by LAN, turn off the computers WiFi, and make sure that the PC is connected to the QUARTZ-GOLD-5G and no other gateway device.

By following the above instructions, the PC used for configuring the QUARTZ-GOLD-5G will only be networked with the QUARTZ-GOLD-5G and will therefore obtain an IP address from the QUARTZ-GOLD-5G's internal DHCP server. It is now possible to connect to the internal web server using a web browser and browsing the QUARTZ-GOLD-5Gs gateway address. The settings that are required are:

Gateway address	192.168.1.1
Username	admin
Password	admin

Web Interface

This will display the root webpage (Status > Overview page) of the routers webserver:



You haven't changed the default password for this router. To change router password click here.

System

Router Name Siretta Router
Hardware Version C11-D10
Firmware Version G9.0.2.2
Router Sn 1110G202205190006
Router Time Fri, 20 Jan 2023 15:56:57 +0000
Uptime 00:39:25

Ethernet Ports Status

WAN/LAN: Unplugged
LAN: UP

VPN Status

No Active VPN

Internet

Connection Type Cellular
IP Address 10.25.90.168
Subnet Mask 255.255.255.240
Gateway 10.25.90.169
DNS 188.31.250.128:53, 188.31.250.129:53
Connection Status **Connected**
Connection Uptime 00:38:06

LAN

Router MAC Address 30:3D:51:10:00:DC
Router IP Addresses **br0** (LAN) - 192.168.1.1/24
DHCP **br0** (LAN) - 192.168.1.2 - 192.168.1.51

Wireless (5 GHz)

MAC Address 30:3D:51:10:00:DF
Wireless Mode Access Point
Wireless Network Mode Auto
Interface Status Up
Radio Disabled ✕
SSID siretta-wifi_5G
Broadcast Enabled ✓
Security disabled
Channel 36
Channel Width Auto
Rate

Wireless (2.4 GHz)

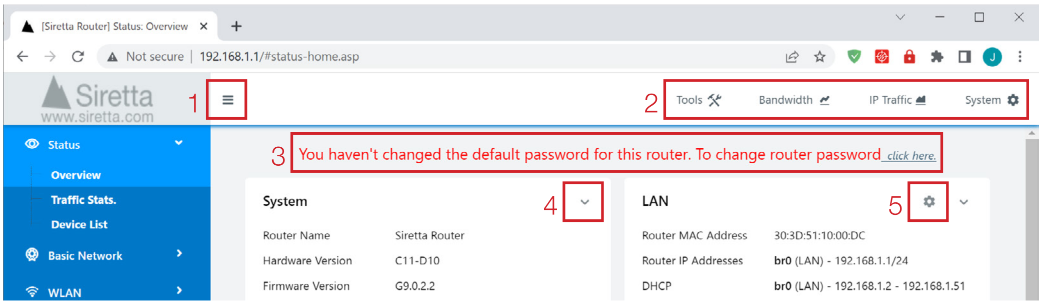
MAC Address 30:3D:51:10:00:DE
Wireless Mode Access Point
Wireless Network Mode Auto
Interface Status Up
Radio Disabled ✕
SSID siretta-wifi_2.4G
Broadcast Enabled ✓

IMPORTANT: When first connecting to the QUARTZ-GOLD-5G, all settings will be at factory default. This is so that it is easy to access the router for configuration. But this also means that others could access the router just as easily. To prevent the QUARTZ-GOLD-5G and it's network from being compromised, it is recommended to immediately do the following:

1. Change the login username/password. This may be done by accessing the Administration > Admin Access page (that is also accessible from the password warning at the top of the page)

When browsing to the routers IP address (= the gateway address) the initial view will always be the Status > Overview page which gives a summary of the QUARTZ-GOLD-5G configuration and operational status.

No matter where in the web interface that is navigated to, there will always be special status areas and tools shown:



You haven't changed the default password for this router. To change router password click here.

System

Router Name Siretta Router
Hardware Version C11-D10
Firmware Version G9.0.2.2

LAN

Router MAC Address 30:3D:51:10:00:DC
Router IP Addresses br0 (LAN) - 192.168.1.1/24
DHCP br0 (LAN) - 192.168.1.2 - 192.168.1.51

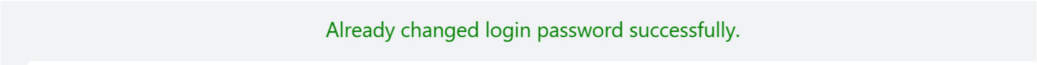
1. Navigation pane expand/collapse (expanded shown).
2. Measurement and debugging tools.
3. Important system messages.
4. Expand/collapse window button (expanded shown).
5. Fast navigation to the configuration menu for the features shown in this window.

Important System Messages

When first used, the system will prompt the user to change the admin password:

You haven't changed the default password for this router. To change router password click here.

While the admin password remains set to ‘admin’ this message will be displayed. Once the password has been changed, the message will change to:



Already changed login password successfully.

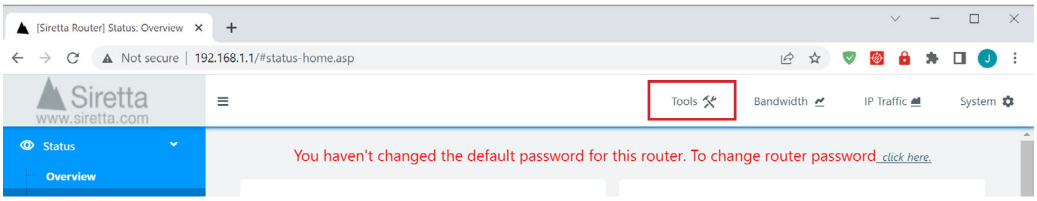
When the QUARTZ-GOLD-5G needs to be rebooted after a configuration change it will show:

The settings changed, some settings will take effect after the router reboots. Reboot Now

Setting up the router will usually involve changes on many pages. It is usually only necessary to reboot the router after all changes have been made so that they are applied.

Measurement and debugging

Tools

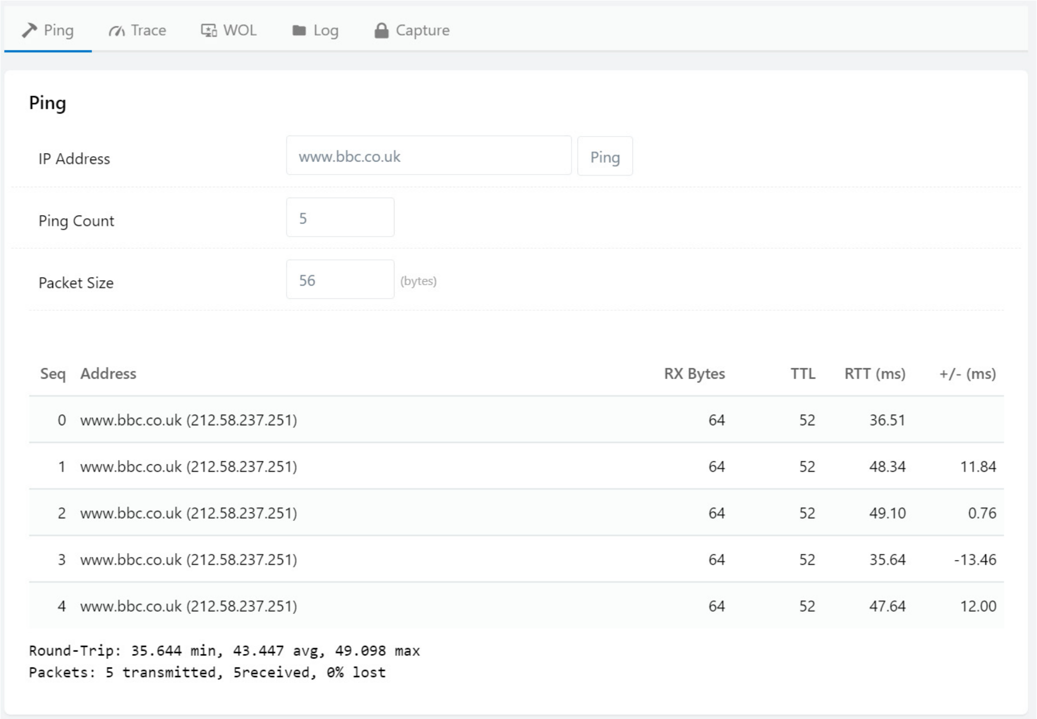

[Siretta Router] Status: Overview
Not secure | 192.168.1.1/#status-home.asp
Siretta
www.siretta.com
Tools
Bandwidth
IP Traffic
System
Status
Overview

You haven't changed the default password for this router. To change router password click here.

Clicking the Tools icon will offer several tools:

Ping

The Ping test tool is used to send ICMP echo request packets to a target IP address to check for errors such as packet loss and to estimate the latency.



Ping

IP Address: www.bbc.co.uk [Ping]

Ping Count: 5

Packet Size: 56 (bytes)

Seq	Address	RX Bytes	TTL	RTT (ms)	+/- (ms)
0	www.bbc.co.uk (212.58.237.251)	64	52	36.51	
1	www.bbc.co.uk (212.58.237.251)	64	52	48.34	11.84
2	www.bbc.co.uk (212.58.237.251)	64	52	49.10	0.76
3	www.bbc.co.uk (212.58.237.251)	64	52	35.64	-13.46
4	www.bbc.co.uk (212.58.237.251)	64	52	47.64	12.00

```
Round-Trip: 35.644 min, 43.447 avg, 49.098 max
Packets: 5 transmitted, 5received, 0% lost
```

IP address: Enter the URL or IPv4 address of the target to be checked (DNS lookup supported).

Ping Count: Enter the number of ICMP packets to be sent.

Packet Size: Number of bytes of data payload that the ICMP packet must carry.
Click 'Ping' to start the test. Note that not all IP addresses support ICMP ping. It can often be disabled to make the IP address being pinged appear inactive.

RX bytes is the number of received bytes returned. Normally this is 8 bytes greater than the packet sent as the return message normally contains the first 8 bytes of the message sent so that the sending process can identify it.

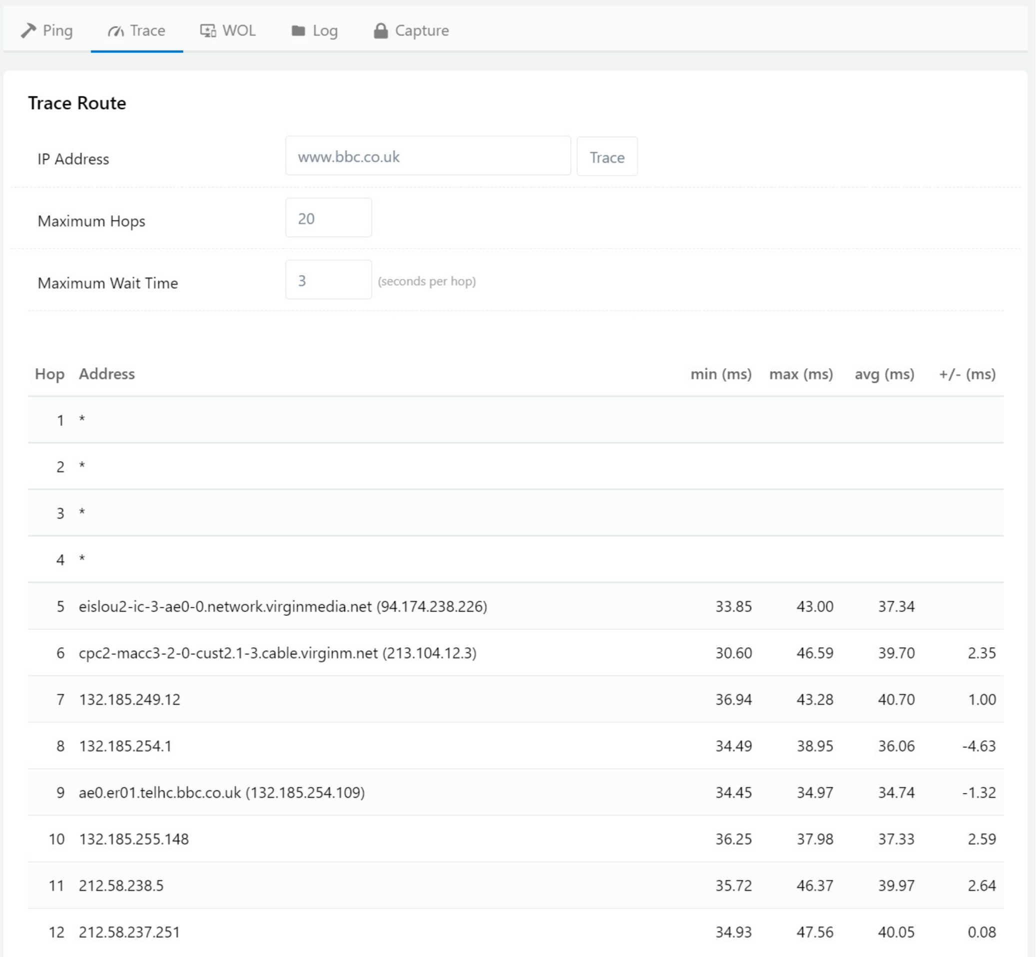
TTL is the Time to Live. This value is set by target IP address when it responds to the ICMP packet (outgoing ICMP packets are sent with a TTL=64). TTL refers to the number of hops along a network path that is allowed, not a time in seconds. The TTL is decremented by one each hop, so returned results with different TTL can be assumed to have taken different network paths.

RTT is the Round Trip Time in mS (to the destinate address and back again)

+/- is the difference in RTT time from the previous ICMP packet.

Trace

The Trace tool is used to determine the path and timings of the connection to an IP address.



Trace Route

IP Address: www.bbc.co.uk [Trace]

Maximum Hops: 20

Maximum Wait Time: 3 (seconds per hop)

Hop	Address	min (ms)	max (ms)	avg (ms)	+/- (ms)
1	*				
2	*				
3	*				
4	*				
5	eislou2-ic-3-ae0-0.network.virginmedia.net (94.174.238.226)	33.85	43.00	37.34	
6	cpc2-macc3-2-0-cust2.1-3.cable.virginm.net (213.104.12.3)	30.60	46.59	39.70	2.35
7	132.185.249.12	36.94	43.28	40.70	1.00
8	132.185.254.1	34.49	38.95	36.06	-4.63
9	ae0.er01.telhc.bbc.co.uk (132.185.254.109)	34.45	34.97	34.74	-1.32
10	132.185.255.148	36.25	37.98	37.33	2.59
11	212.58.238.5	35.72	46.37	39.97	2.64
12	212.58.237.251	34.93	47.56	40.05	0.08

IP address: Enter the URL or IPv4 address of the target to be checked (DNS lookup supported).

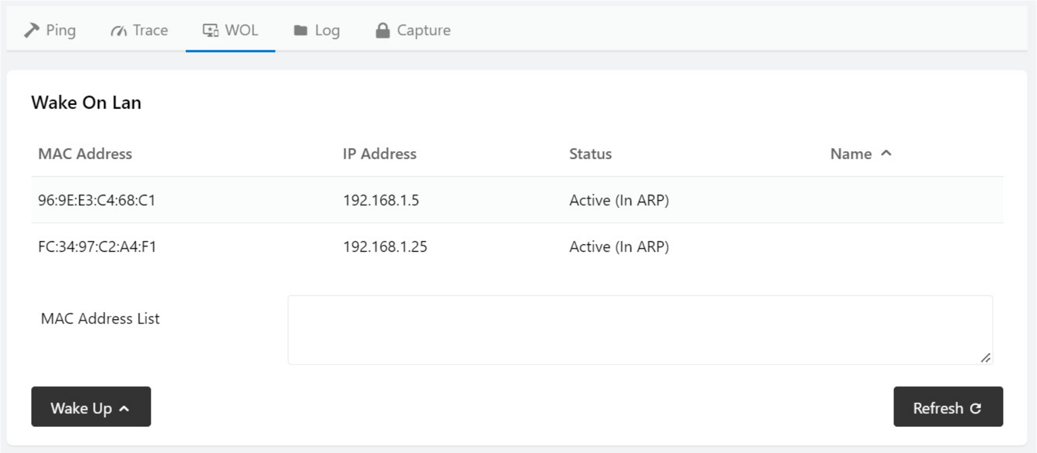
Maximum Hops: Enter the maximum number of hops to be tested.

Maximum Wait Time: Enter the maximum wait time allowed per hop.

Click 'Trace' to run the test. Note that not all points on the path are likely to respond, those that don't will be indicated by a '*'.

WOL

Wake on LAN. This allows a magic packet to be sent to wake up a networking device on the local subnet.



Wake On Lan

MAC Address	IP Address	Status	Name ^
96:9E:E3:C4:68:C1	192.168.1.5	Active (In ARP)	
FC:34:97:C2:A4:F1	192.168.1.25	Active (In ARP)	

MAC Address List

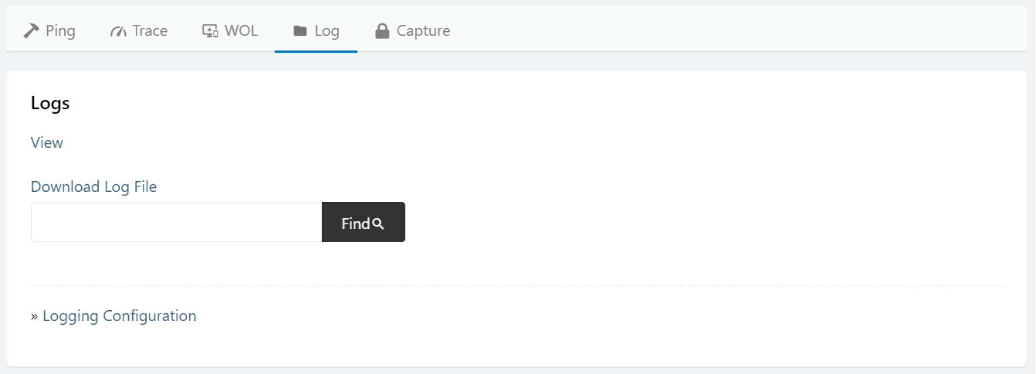
The interface shows the current ARP list of the router. Clicking any entry in the ARP list will send a magic packet to that MAC address.

It is also possible to enter one or more MAC addresses in the MAC Address List field. Separate multiple MAC addresses with a space or new line. Click 'Wake Up' to send the Magic Packet to all MAC addresses in the list. If the list is large, re-size the field by dragging the marker at the bottom right of the box. 'Wake Up' also saves the MAC Address List – the list will persist through reboots.

Use hint: If a device is turned off, it will not appear in the ARP list. To use WOL effectively, plan ahead. The ARP list is only refreshed when the page is browsed or the refresh button clicked. Use the ARP list to identify the MAC addresses of the devices to be controlled while they are on the network, and copy these MAC addresses to the MAC Address List to be able to use them later.

Log

This allows the user to look at and download the router logs. The log is a rolling buffer of the last few minutes of activity of the router. Additionally, the log file can be sent to an external Syslog server.



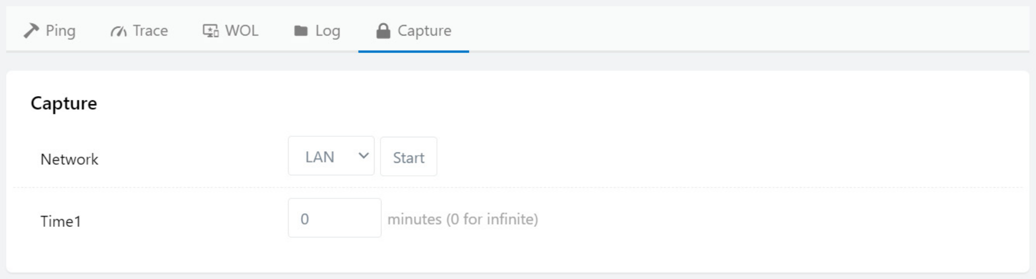
Click ‘View’ to open the log as a web page, or ‘Download Log File’ to download the log as a syslog.txt file.

Typing in a word and clicking ‘Find’ will open a filtered view in the web browser showing only lines in the log containing the word searched for.

Click on ‘Logging Configuration’ show further options including to enable logging to an external server (which may be done as well as or instead of the internal log) and capping the rate of log file size increase.

Capture

The capture tool allows for a complete capture of all network traffic in a .pcap file format that can be viewed and analysed in Wireshark and other packet analyser software tools.

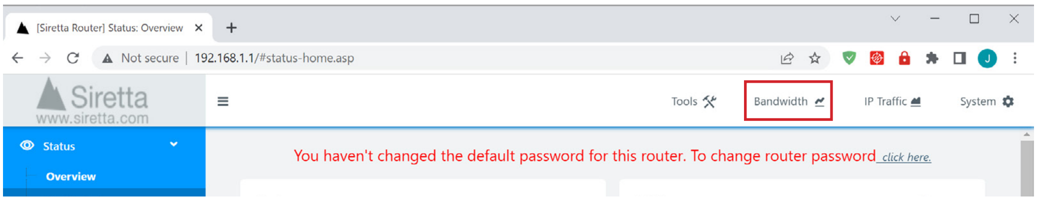


Network: LAN

Time1: 0 minutes (0 for infinite)

Select either LAN or WAN from the dropdown menu to choose the interface whose traffic will be captured, the log duration, and the click ‘Start’. A dump.pcap file is created as a file download and added to for the time requested, or until ‘Stop’ is clicked.

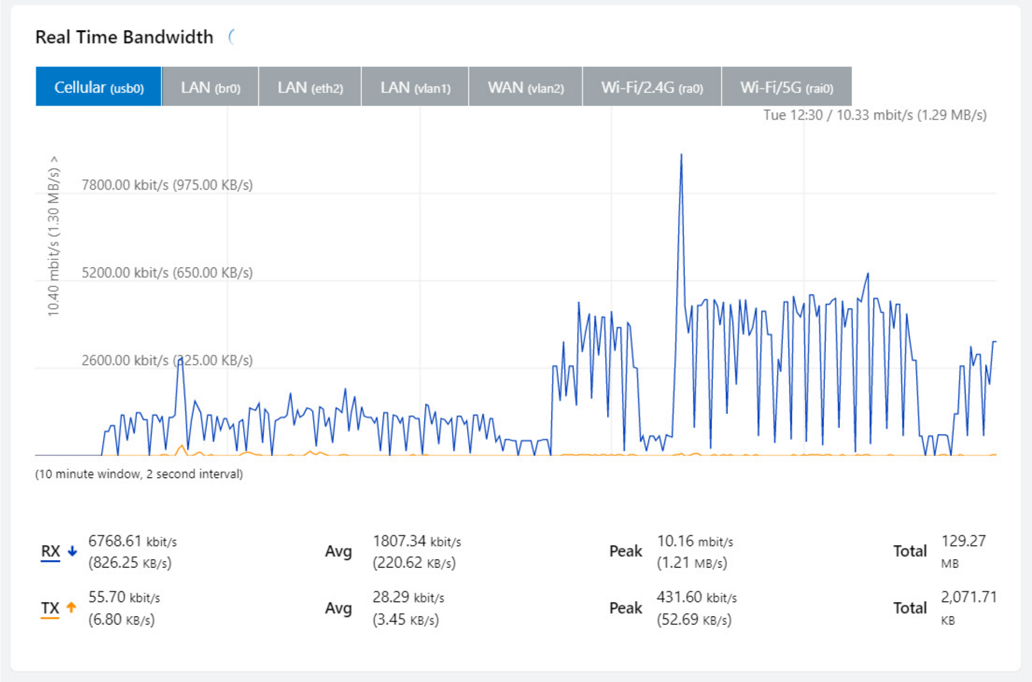
Bandwidth


[Siretta Router] Status: Overview
Not secure | 192.168.1.1/#status-home.asp
Siretta
www.siretta.com
Tools
Bandwidth
IP Traffic
System
Status
Overview

You haven't changed the default password for this router. To change router password click here.

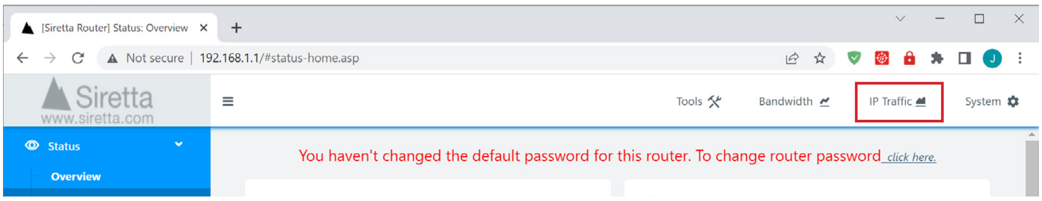
Real-Time

This reports the traffic on the different interfaces of the QUARTZ-GOLD-5G. This is shown both graphically and numerically.


Real Time Bandwidth
Cellular (usb0)
LAN (br0)
LAN (eth2)
LAN (vlan1)
WAN (vlan2)
Wi-Fi/2.4G (ra0)
Wi-Fi/5G (rai0)
Tue 12:30 / 10.33 mbit/s (1.29 MB/s)
10.40 mbit/s (1.30 MB/s) >
7800.00 kbit/s (975.00 KB/s)
5200.00 kbit/s (650.00 KB/s)
2600.00 kbit/s (325.00 KB/s)
(10 minute window, 2 second interval)

RX ↓	6768.61 kbit/s (826.25 KB/s)	Avg	1807.34 kbit/s (220.62 KB/s)	Peak	10.16 mbit/s (1.21 MB/s)	Total	129.27 MB
TX ↑	55.70 kbit/s (6.80 KB/s)	Avg	28.29 kbit/s (3.45 KB/s)	Peak	431.60 kbit/s (52.69 KB/s)	Total	2,071.71 KB

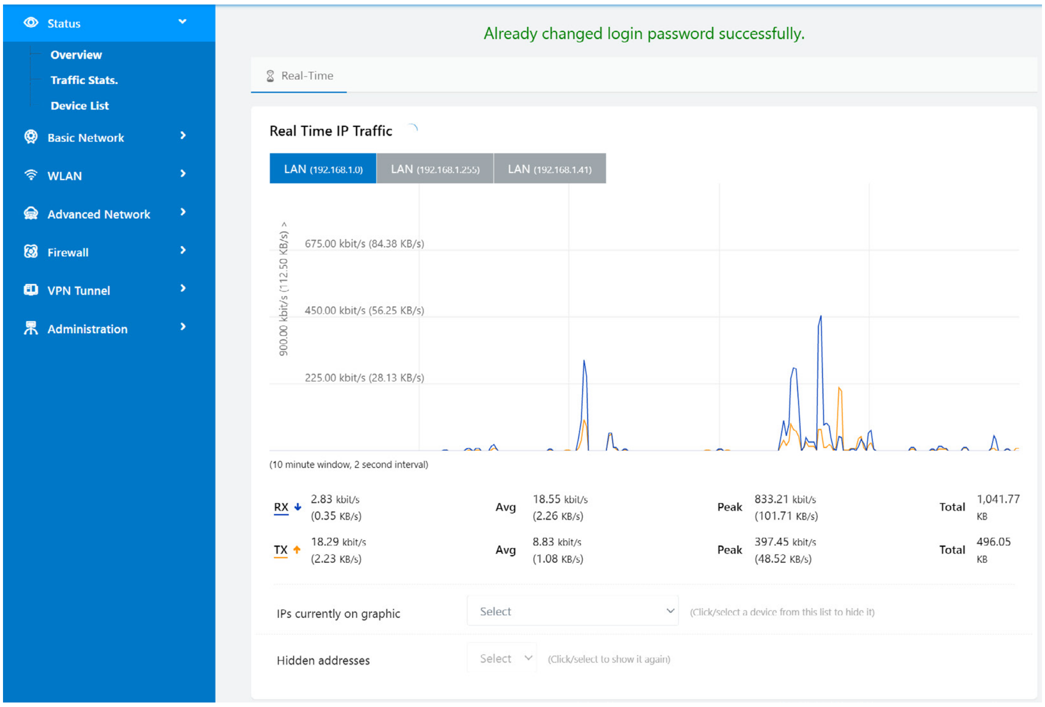
IP Traffic


[Siretta Router] Status: Overview
Not secure | 192.168.1.1/#status-home.asp
Siretta
www.siretta.com
Tools
Bandwidth
IP Traffic
System
Status
Overview

You haven't changed the default password for this router. To change router password click here.

Real-Time IP Traffic

This reports the traffic by IP address in the QUARTZ-GOLD-5G. This is shown both graphically and numerically. Select and hide IP addresses using the drop-down boxes at the bottom of the page.



Already changed login password successfully.

Real Time IP Traffic

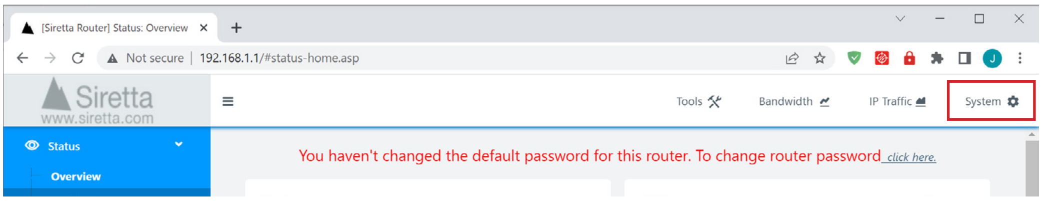
(10 minute window, 2 second interval)

RX	2.83 kbit/s (0.35 KB/s)	Avg	18.55 kbit/s (2.26 KB/s)	Peak	833.21 kbit/s (101.71 KB/s)	Total	1,041.77 KB
TX	18.29 kbit/s (2.23 KB/s)	Avg	8.83 kbit/s (1.08 KB/s)	Peak	397.45 kbit/s (48.52 KB/s)	Total	496.05 KB

IPs currently on graphic: Select (Click/select a device from this list to hide it)

Hidden addresses: Select (Click/select to show it again)

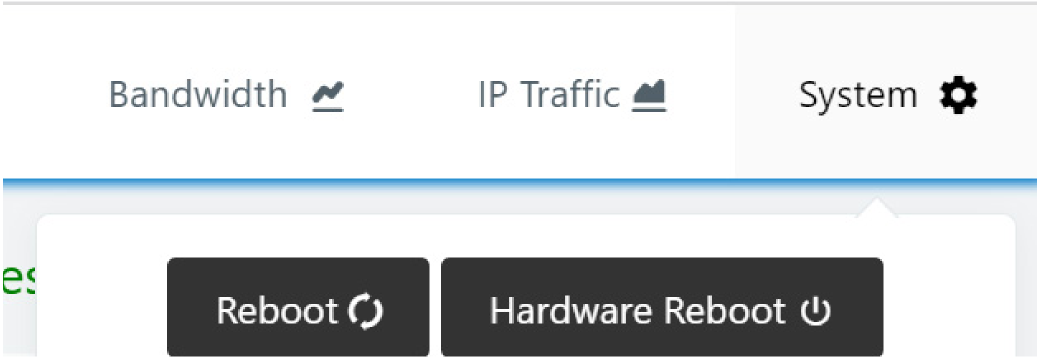
System



[Siretta Router] Status: Overview
Not secure | 192.168.1.1/#status-home.asp
Siretta
www.siretta.com
Tools
Bandwidth
IP Traffic
System
Status
Overview

You haven't changed the default password for this router. To change router password click here.

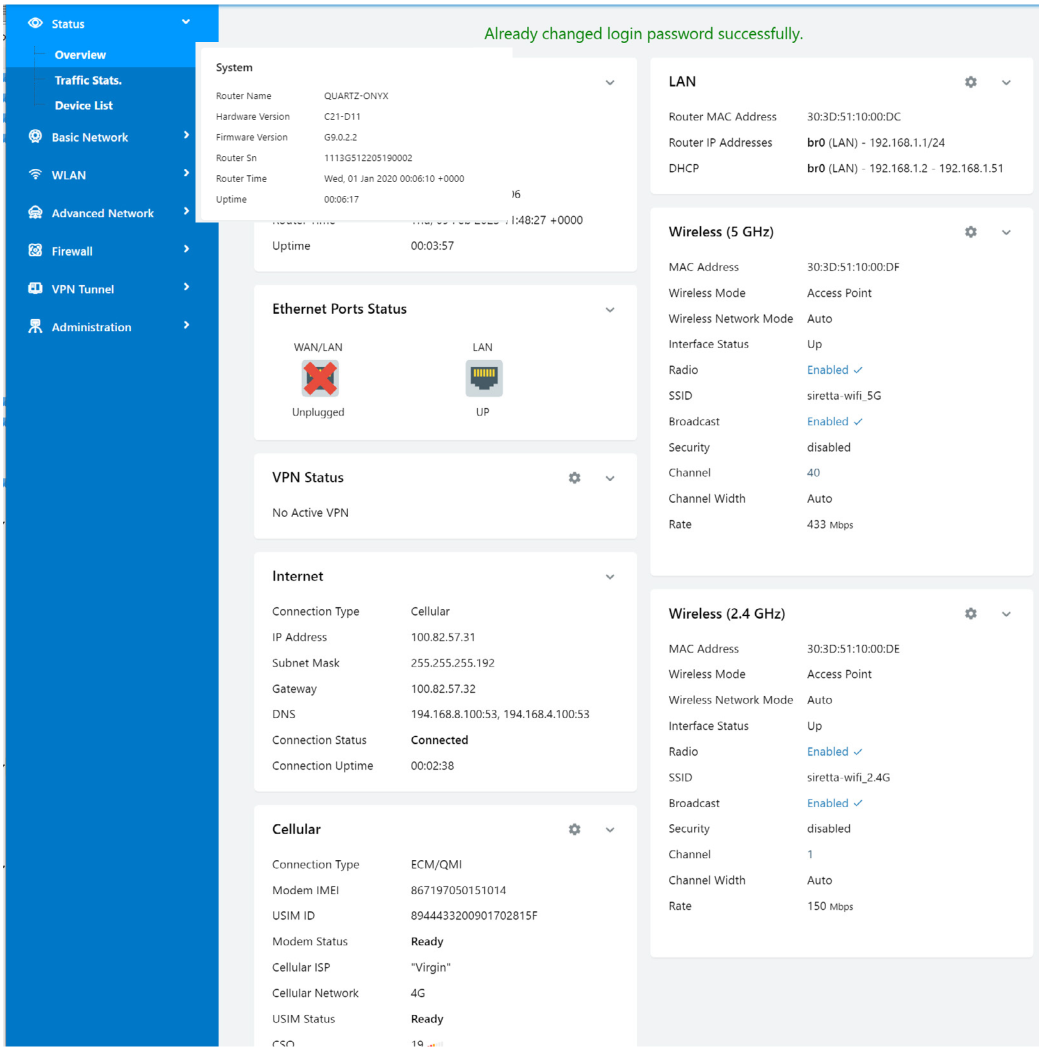
The system menu allows for reboot and logging out from the QUARTZ-GOLD-5G. Reboot is a software reboot. Hardware Reboot is a software initiated power cycle of the router.



Status

Overview

This displays the state of the interfaces of the QUARTZ-GOLD-5G and shows the running operating configuration.



Already changed login password successfully.

System

Router Name	QUARTZ-ONYX
Hardware Version	C21-D11
Firmware Version	G9.0.2.2
Router Sn	1113G512205190002
Router Time	Wed, 01 Jan 2020 00:06:10 +0000
Uptime	00:06:17

Uptime 00:03:57

Ethernet Ports Status

WAN/LAN	LAN
Unplugged	UP

VPN Status

No Active VPN

Internet

Connection Type	Cellular
IP Address	100.82.57.31
Subnet Mask	255.255.255.192
Gateway	100.82.57.32
DNS	194.168.8.100:53, 194.168.4.100:53
Connection Status	Connected
Connection Uptime	00:02:38

Cellular

Connection Type	ECM/QMI
Modem IMEI	867197050151014
USIM ID	8944433200901702815F
Modem Status	Ready
Cellular ISP	"Virgin"
Cellular Network	4G
USIM Status	Ready
CSQ	19

LAN

Router MAC Address	30:3D:51:10:00:DC
Router IP Addresses	br0 (LAN) - 192.168.1.1/24
DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51

Wireless (5 GHz)

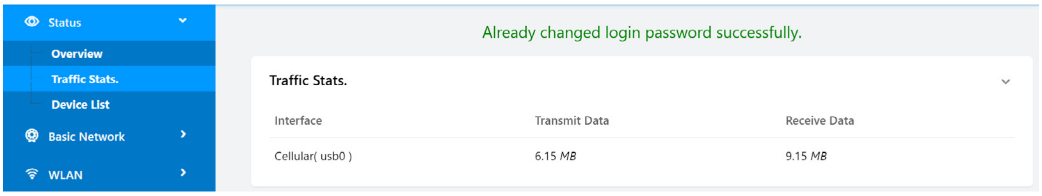
MAC Address	30:3D:51:10:00:DF
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up
Radio	Enabled ✓
SSID	siretta-wifi_5G
Broadcast	Enabled ✓
Security	disabled
Channel	40
Channel Width	Auto
Rate	433 Mbps

Wireless (2.4 GHz)

MAC Address	30:3D:51:10:00:DE
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up
Radio	Enabled ✓
SSID	siretta-wifi_2.4G
Broadcast	Enabled ✓
Security	disabled
Channel	1
Channel Width	Auto
Rate	150 Mbps

Traffic Stats

This shows the total data uploaded and downloaded by the QUARTZ-GOLD-5G since it was last rebooted (software or hardware reboot).



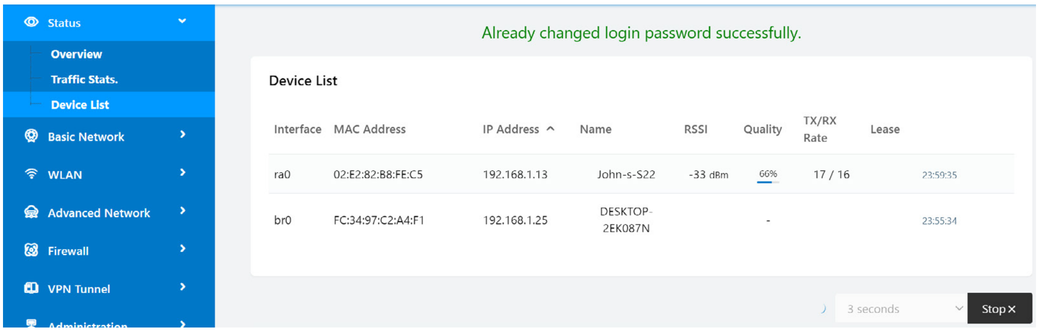
Already changed login password successfully.

Traffic Stats.

Interface	Transmit Data	Receive Data
Cellular(usb0)	6.15 *MB*	9.15 *MB*

Device list

This shows a list of the devices attached to the network and information about their connection.



Already changed login password successfully.

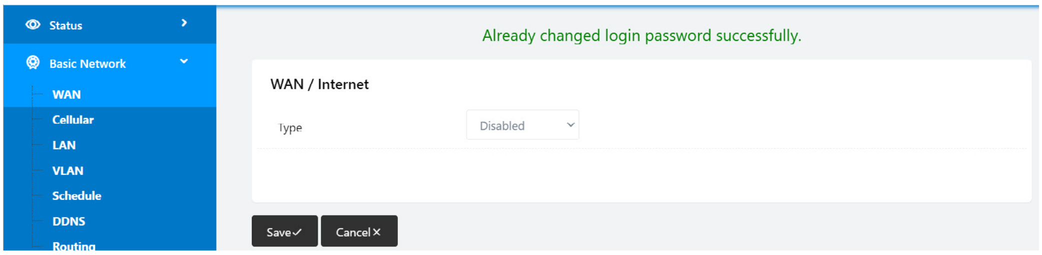
Device List

Interface	MAC Address	IP Address ^	Name	RSSI	Quality	TX/RX Rate	Lease
ra0	02:E2:82:B8:FE:C5	192.168.1.13	John-s-S22	-33 dBm	66%	17 / 16	23:59:35
br0	FC:34:97:C2:A4:F1	192.168.1.25	DESKTOP-2EK087N		-		23:55:34

Basic Network

WAN

This defines how the WAN port works. If WAN is disabled (the factory default state), the port will work as a LAN port.



Already changed login password successfully.

WAN / Internet

Type: Disabled

WAN Setting	Options
Type	Disabled / DHCP / PPPoE / Static Address
MTU	Default / Custom

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

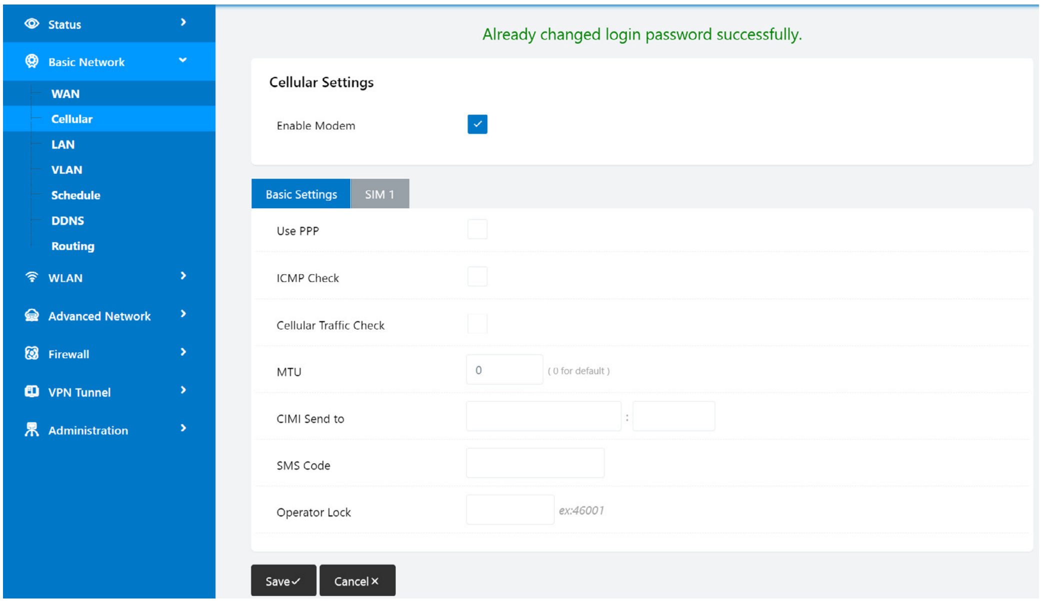
If the WAN is not set to disabled, then further context relevant configuration settings are shown.

Cellular

The cellular settings allow the 5G NR / 4G LTE cellular connection to be enabled/ disabled, and contains the settings necessary for the 5G NR / 4G LTE router to be configured correctly for the cellular network used.

In order to be able to successfully use the cellular WAN connection, an activated SIM card needs to be inserted into one of the SIM card slots (see Hardware User’s Manual) and the slot in which the SIM card inserted correctly configured with the correct APN/ Username and password. The Basic Settings configuration tab must also be completed.

Basic Settings



Already changed login password successfully.

Cellular Settings

Enable Modem	☑

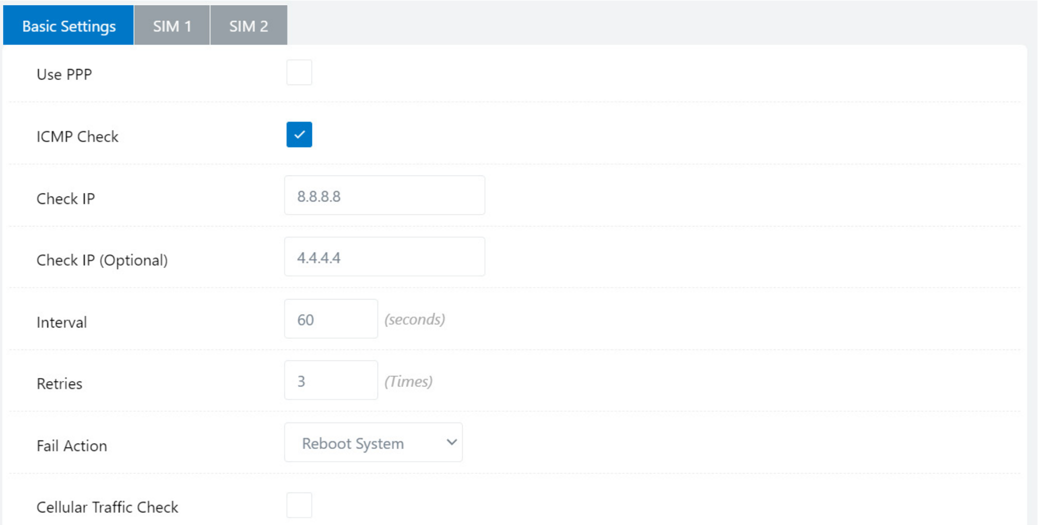
Use PPP	□
ICMP Check	□
Cellular Traffic Check	□
MTU	0 (0 for default)
CIMI Send to	:
SMS Code	
Operator Lock	ex:46001

Basic Setting	Options
Enable Modem	Enable / Disable 5G NR / 4G LTE modem
Use PPP	IP is used as default. PPP may be enabled if required
ICMP Check	When enabled, the cellular interface attempts to send an ICMP ping to a user specified address at a user specified interval to check for connectivity. If the test fails, the router may be rebooted or cellular reconnect attempted. See next page
Cellular Traffic Check	Router checks for cellular Tx/Rx data transmission over a user specified interval. If the test fails because no traffic is detected, the router may be rebooted or cellular reconnect attempted. See below
MTU	Entered desired MTU size for the cellular interface
CIMI Send to	Send CIMI to user defined IP and port using TCP protocol
SMS Code	Password to enable remote control of the router by SMS
Operator Lock	Only allows the network specified by the PLMN entered to be used

ICMP Check and Cellular Traffic Check are intended to be used mutually exclusively. They are two different approaches to monitoring for the failure of the cellular link and the recovery from this should it occur.

ICMP Check

This checks for network connectivity using ICMP ping. The router will send a ICMP ping to the check IP address at the interval specified. If there is no response to the ICMP ping, then the router will retry every 3 seconds until the number of retries specified is met. If there is still no response, the fail action will be taken and the process will start again.

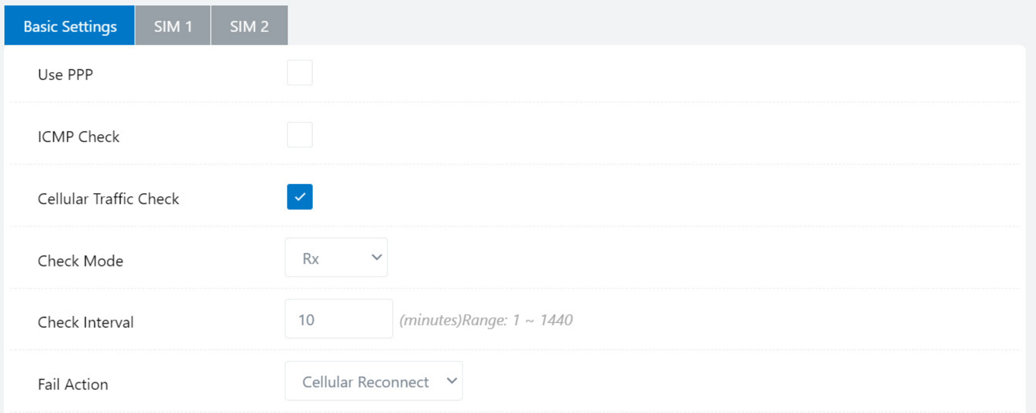


Use PPP	□
ICMP Check	☑
Check IP	8.8.8.8
Check IP (Optional)	4.4.4.4
Interval	60 (seconds)
Retries	3 (Times)
Fail Action	Reboot System
Cellular Traffic Check	□

ICMP Setting	Options
Check IP	IP address that should respond to ICMP ping
Check IP (optional)	Optional alternative IP address that should respond to ICMP ping
Interval	Interval in seconds after which connectivity is to be checked
Retries	Number of times to attempt to reach check IP address
Fail Action	Cellular Reconnect / Reboot System

Cellular Traffic Check

This checks for cellular network connectivity by looking for cellular network traffic. If there is no cellular network traffic occurring during the user set Check Interval, the cellular network will be judged as failed. When the cellular network has failed, the fail action will be taken and the process will start again.



Use PPP □

ICMP Check □

Cellular Traffic Check ☑

Check Mode: Rx

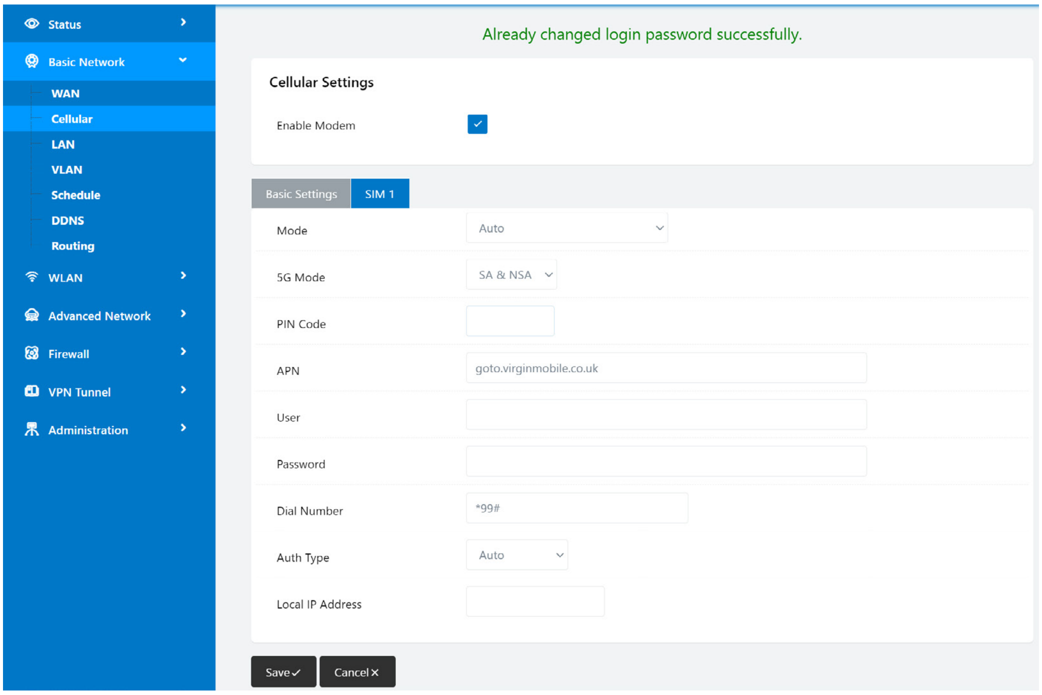
Check Interval: 10 (minutes)Range: 1 ~ 1440

Fail Action: Cellular Reconnect

Traffic Setting	Options
Check Mode	Rx / Tx / Rx & Tx
Check Interval	Enter time in minutes. 1440 minutes = 24 hours.
Fail Action	Cellular Reconnect / Reboot System

SIM

Enter the settings required for the SIM card here



Already changed login password successfully.

Cellular Settings

Enable Modem ☑

Mode: Auto

5G Mode: SA & NSA

PIN Code:

APN: goto.virginmobile.co.uk

User

Password:

Dial Number: *99#

Auth Type: Auto

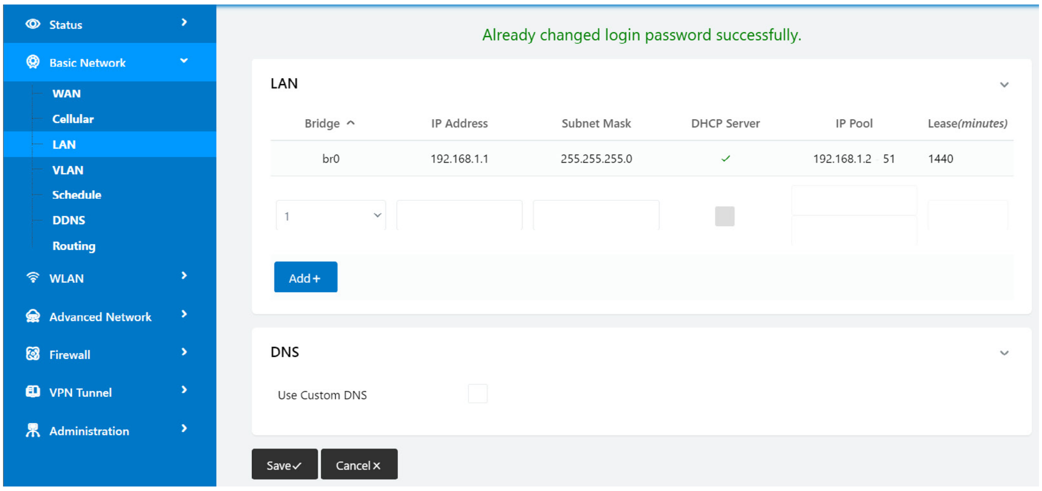
Local IP Address:

SIM Setting	Options
Enable Modem	Enable / Disable LTE modem
SIM Mode	Auto / LTE(FDD/TDD) / 3G(WCDMA/TD-SCDMA/HSPA) / 3G(CDMA 2000/CDMA 1x) Using Auto will connect to the best network available, usually 5G NR if available
SIM 5G Mode	SA & NSA / NSA / SA
SIM PIN Code	Enter the PIN number assigned to the SIM Card if required
SIM APN	Enter the APN provided by the cellular provider (always required)
SIM User	Enter User Name if provided by the cellular provider
SIM Password	Enter Password if provided by the cellular provider
SIM Dial number	Defaults to ‘*99#’. Only change if cellular provider requires this.
SIM Auth type	Auto / PAP / CHAP / MS-CHAP / MS-CHAPv2
SIM Local IP address	From cellular provider if they have provided a fixed IP address

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

LAN

The LAN settings define the LAN subnets, DHCP server and DNS settings. Up to 4 subnets may be configured and used.



Already changed login password successfully.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 51	1440
1			□		

DNS

Use Custom DNS □

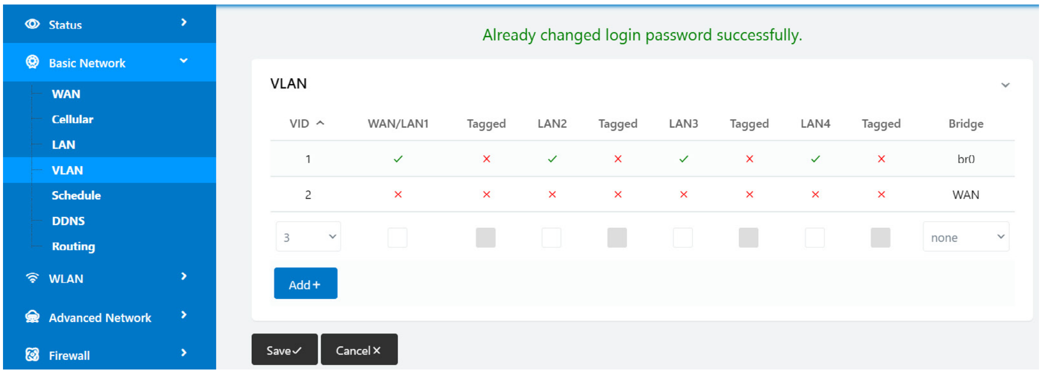
LAN Setting	Options
Bridge	br0 / br1 / br2 / br3
IP Address	First IP address for the subnet
Subnet Mask	Size of the subnet
DHCP Server	DHCP server enabled on subnet?
IP Pool	Range of IP addresses provided by DHCP server
Lease	DHCP lease time

DNS Setting	Options
Use Custom DNS	Enable to set custom DNS, otherwise DNS from the active WAN is used
Primary DNS	Custom primary DNS
Secondary DNS	Custom secondary DNS

IMPORTANT: After creating a new LAN, click Add+ to add it. After making all required changes, click ‘Save’ to apply them.

VLAN

VLANs may be set up and used in the QUARTZ-GOLD-5G. When using a backup mode from WAN to Cellular or vice versa, configuring a VLAN is required.



Already changed login password successfully.

VLAN

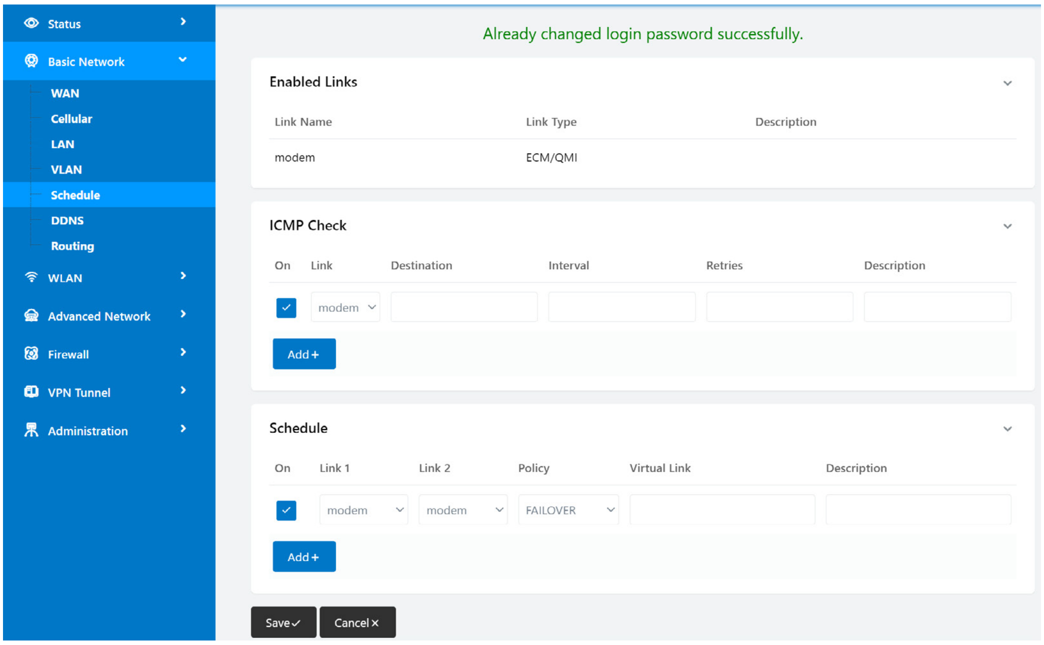
VID	WAN/LAN1	Tagged	LAN2	Tagged	LAN3	Tagged	LAN4	Tagged	Bridge
1	✓	✗	✓	✗	✓	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	WAN
3	□	□	□	□	□	□	□	□	none

VLAN Setting	Options
VID	VLAN ID. Number between 1 and 16
WAN/LAN, LAN	Define the Ethernet jack
Tagged	Enable to add VLAN tag to the traffic
Bridge	None / WAN / Br0 / Br1 / Br2 / Br3

IMPORTANT: After creating a new VLAN, click Add+ to add it. After making all required changes, click ‘Save’ to apply them.

Schedule

Enter scheduled events that change the gateway in the router. The enabled links show the broadband connections that have been configured and their names. These are used in the ICMP Check and Schedule Fields. Enabled links could be Ethernet WAN, Cellular modem or Wireless Client



Already changed login password successfully.

Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

On	Link	Destination	Interval	Retries	Description
☑	modem				

Schedule

On	Link 1	Link 2	Policy	Virtual Link	Description
☑	modem	modem	FAILOVER		

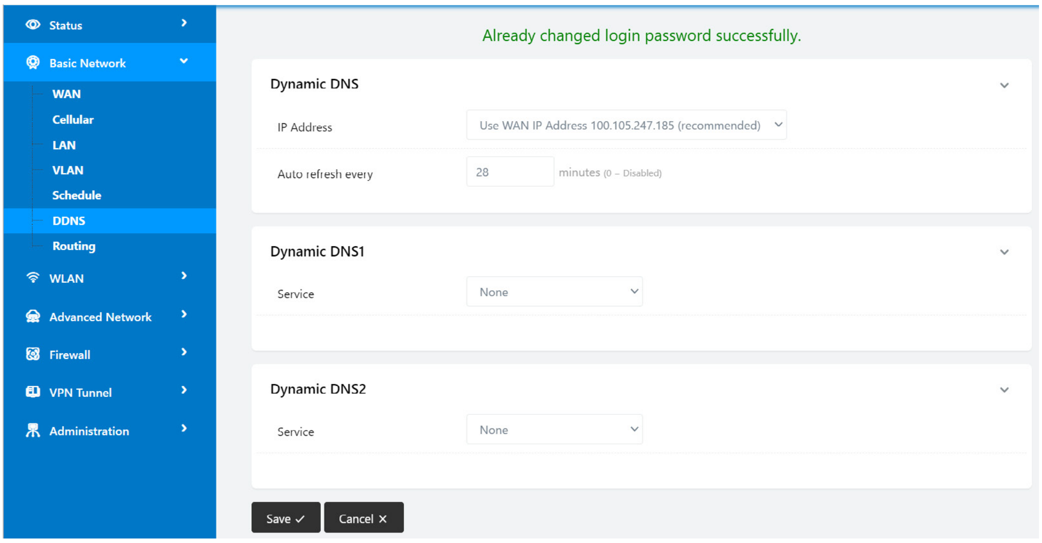
ICMP Setting	Options
On	Check to enable line
Link	Select interface to check from pull down menu
Destination	IP address that should respond to ICMP ping
Interval	Interval in seconds after which connectivity is to be checked
Retries	Number of times to attempt to reach check IP address
Description	User description for the rule

Schedule Setting	Options
On	Check to enable line
Link 1	Select primary interface from drop down. This is used until the ICMP check on it fails
Link 2	Select secondary interface from drop down
Policy	Select Failover or Backup. Fail Over switches links when the active link ICMP check fails. Backup uses Link 1 as the primary link and only switches to Link 2 while the Link 1 ICMP check fails.
Description	User description for the rule

IMPORTANT: After creating a new ICMP Check or Schedule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

DDNS

Enter Dynamic DNS settings here. Please check carefully that the IP address used is a public IP address. For a cellular connection, the address reported will be the IP address assigned by the cell which is probably a private rather than public address, and therefore not directly accessible from the Internet. If the cellular provider has supplied a fixed IP address, it should be entered as a Custom IP address.



Already changed login password successfully.

Dynamic DNS

IP Address: Use WAN IP Address 100.105.247.185 (recommended)

Auto refresh every: 28 minutes (0 – Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None

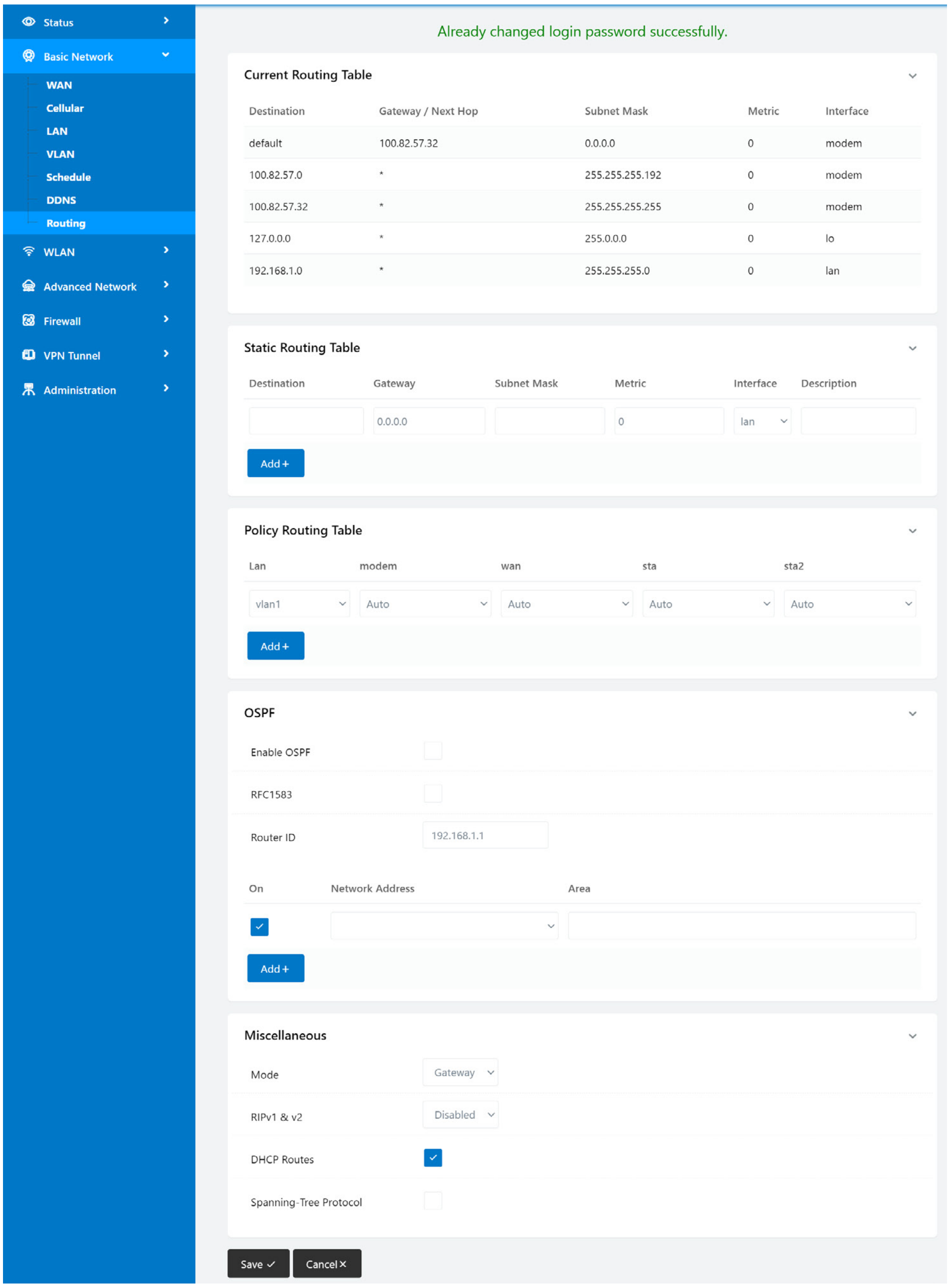
Dynamic DNS Setting	Options
IP Address	Select WAN address or custom IP address
Custom IP Address	Enter IP address to report to DDNS server
Auto refresh every	Time interval for DDNS refresh

Dynamic DNS1/2 Setting	Options
Service	Select DDNS provider or custom address of DDNS provider.

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Routing

This shows the current routing table and allows for routing options such as static / policy routes and OSPF to be set up and configured.



Already changed login password successfully.

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	100.82.57.32	0.0.0.0	0	modem
100.82.57.0	*	255.255.255.192	0	modem
100.82.57.32	*	255.255.255.255	0	modem
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
	0.0.0.0		0	lan	

Add +

Policy Routing Table

Lan	modem	wan	sta	sta2
vlan1	Auto	Auto	Auto	Auto

Add +

OSPF

Enable OSPF □

RFC1583 □

Router ID 192.168.1.1

On	Network Address	Area
☑		

Add +

Miscellaneous

Mode Gateway

RIPv1 & v2 Disabled

DHCP Routes ☑

Spanning-Tree Protocol □

Save ✓ Cancel ✕

Static Route Setting	Options
Destination	Enter the destination IP address
Gateway	Enter first IP address on route to destination IP address
Subnet Mask	Enter the subnet mask for the destination IP address
Metric	Enter routing metric for this route. Metrics determine a routes priority
Interface	Select the interface to be used to reach the Gateway
Description	User description for the rule

Policy Routing Setting	Options
LAN	Select vlan or ap
modem	Auto / Only / Primary / Secondary
wan	Auto / Only / Primary / Secondary
sta	Auto / Only / Primary / Secondary
Sta2	Auto / Only / Primary / Secondary

Modem is the cellular modem interface, wan is the RJ45 Ethernet WAN port, sta and sta2 are WiFi routes (if WiFi is configured as a client).

OSPF Setting	Options
Enable OSPF	Check to enable OSPF
RFC1583	Check to enable compatibility with RFC1583
Router ID	Enter IP address or number for OSPF Router ID
On	Check to enable
Network Address	Enter interface from pulldown
Area	Enter IP address or number for OSPF area.

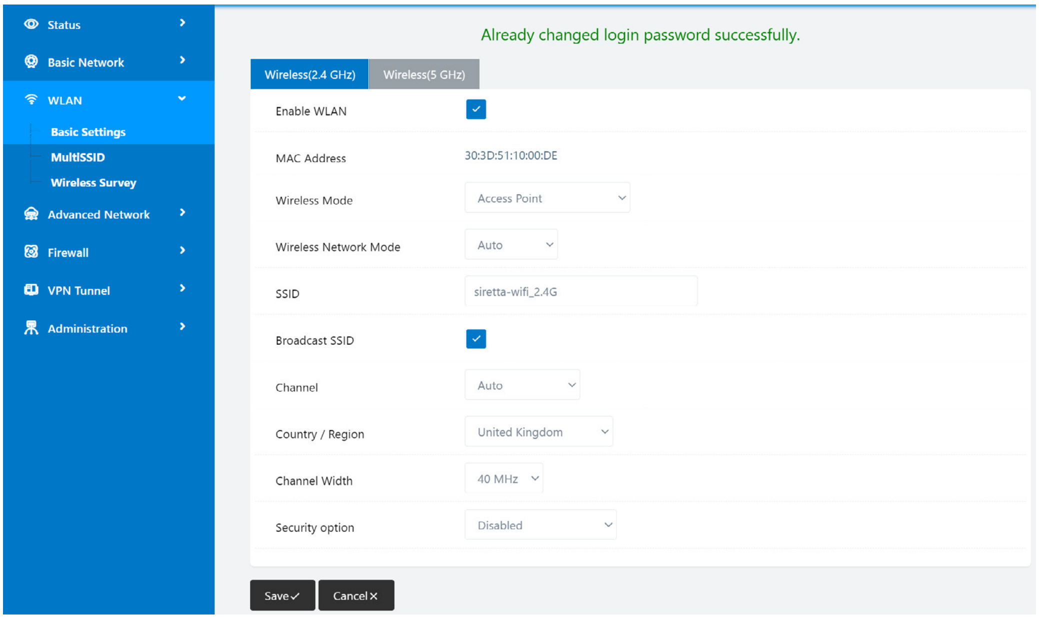
Miscellaneous Setting	Options
Mode	Choose Gateway or Router
RIPv1 & v2	Choose disabled, LAN, WAN or Both
DHCP Routes	Check to enable DHCP Routes
Spanning-Tree Protocol	Check to enable Spanning-Tree Protocol

IMPORTANT: After creating a new Static Route or OSPF, click Add+ to add it. After making all required changes, click 'Save' to apply them.

WLAN

Basic Settings

Set up and configure the WiFi here. There are 2 radio channels, 2.4 GHz and 5 GHz that may be enabled and used independently. The mode of each wireless network may be configured to be used as an Access Point, a Wireless Client, or a Wireless Ethernet Bridge. Depending on the mode used, the configuration settings page will show the appropriate configuration options. Configuration options for use as an Access Point are shown, contact Siretta help for assistance if required for use as a Wireless Client or Ethernet Bridge.



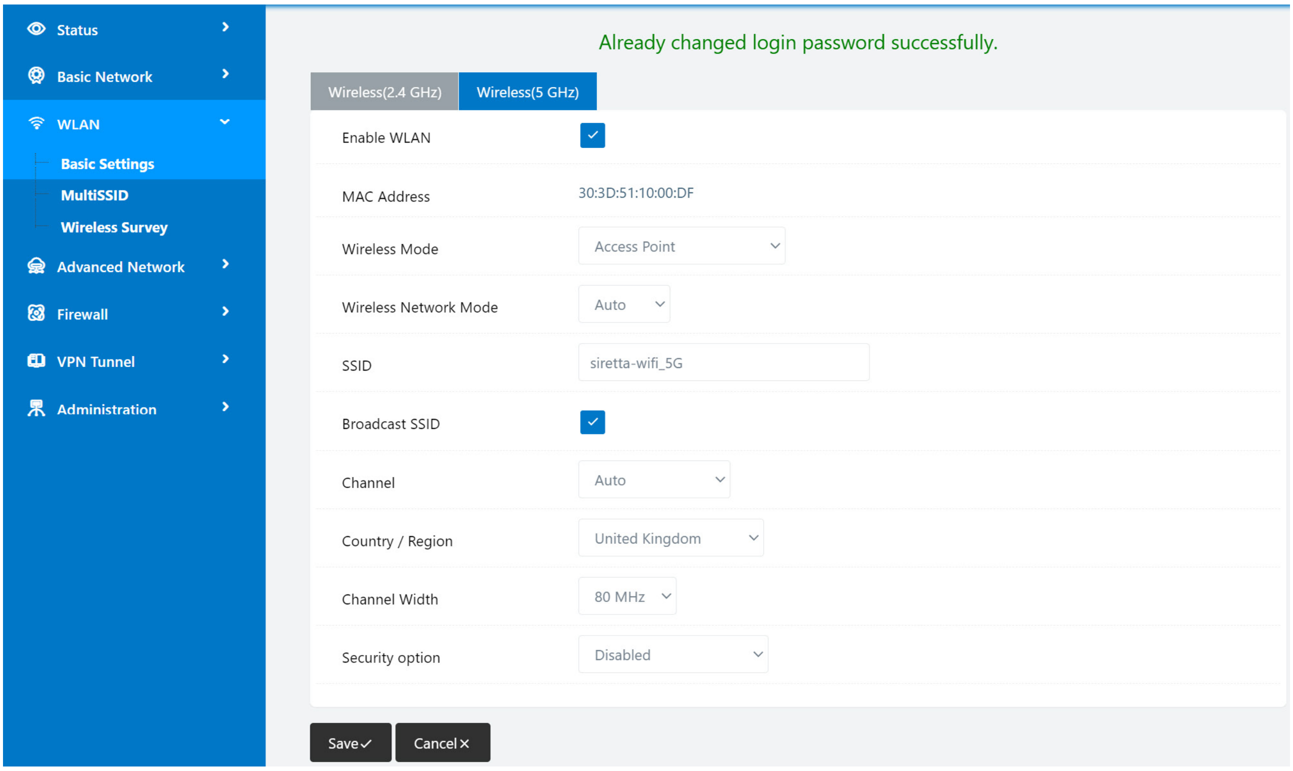
Already changed login password successfully.

Enable WLAN	☑
MAC Address	30:3D:51:10:00:DE
Wireless Mode	Access Point
Wireless Network Mode	Auto
SSID	siretta-wifi_2.4G
Broadcast SSID	☑
Channel	Auto
Country / Region	United Kingdom
Channel Width	40 MHz
Security option	Disabled

Wireless 2.4 GHz Settings	Options
Enable WLAN	Check to enable 2.4 GHz wireless
MAC Address	MAC address of 2.4 GHz wireless interface
Wireless Mode	Choose Access Point, Wireless Client or Wireless Ethernet Bridge
Wireless Network Mode	Chose Auto (b/g/n mode), B Only, G Only, B/G Mixed, or N only
SSID	Enter SSID (factory default = siretta-wifi_2.4G)
Broadcast SSID	Check to enable broadcast of the SSID
Channel	Auto or select channel number
Country/Region	Select the country in which the router is used to meet local radio regulations
Channel Width	Select 20 MHz, 40 MHz
Security Option	Chose Disabled, WPA personal, WPA2 Personal or WPA/WPA2 personal
Encryption	AES or TKIP
Shared Key	Set as required dependant on Security option selected

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

IMPORTANT: Always set the Country/Region to the country in which the QUARTZ-GOLD-5G is being used to meet all regulatory compliance requirements. Siretta is not responsible for any consequences resulting from this being set incorrectly.



Already changed login password successfully.

Enable WLAN	☑
MAC Address	30:3D:51:10:00:DF
Wireless Mode	Access Point
Wireless Network Mode	Auto
SSID	siretta-wifi_5G
Broadcast SSID	☑
Channel	Auto
Country / Region	United Kingdom
Channel Width	80 MHz
Security option	Disabled

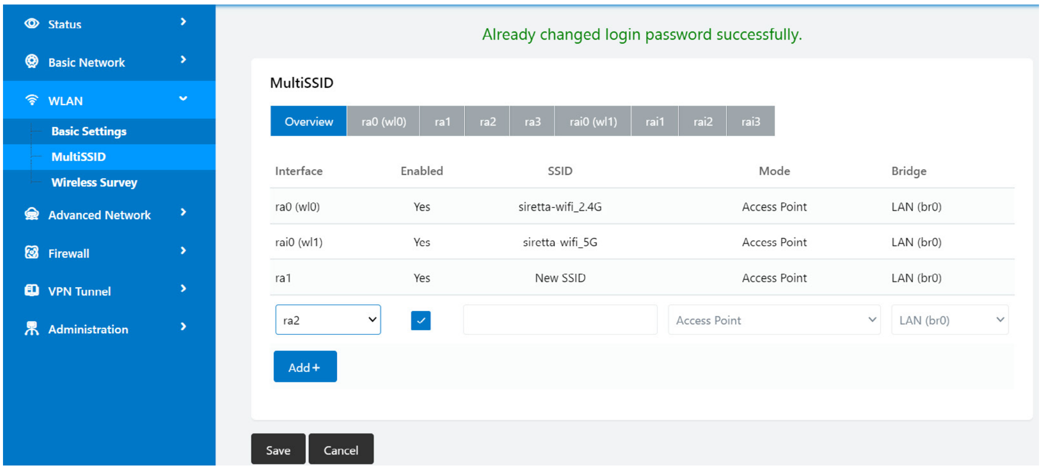
Wireless 5 GHz Settings	Options
Enable WLAN	Check to enable 5 GHz wireless
MAC Address	MAC address of 5 GHz wireless interface
Wireless Mode	Choose Access Point, Wireless Client or Wireless Ethernet Bridge
Wireless Network Mode	Chose Auto (a/n/ac), A Only
SSID	Enter SSID (factory default = siretta-wifi_5G)
Broadcast SSID	Check to enable broadcast of the SSID
Channel	Auto or select channel number
Country/Region	Select the country in which the router is used to meet local radio regulations
Channel Width	Select 20 MHz, 40 MHz or 80 MHz
Security Option	Chose Disabled, WPA personal, WPA2 Personal or WPA/ WPA2 personal
Encryption	AES or TKIP
Shared Key	Set as required dependant on Security option selected

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

IMPORTANT: Always set the Country/Region to the country in which the QUARTZ-GOLD-5G is being used to meet all regulatory compliance requirements. Siretta is not responsible for any consequences resulting from this being set incorrectly.

Multi-SSID

Set up Multi-SSID here. An additional 3 per radio may be configured, for a maximum of 8 SSIDs. Additional SSIDs may be set with their own unique wireless mode and security, and may be assigned their own VLAN (if multiple VLANs have been configured).



Already changed login password successfully.

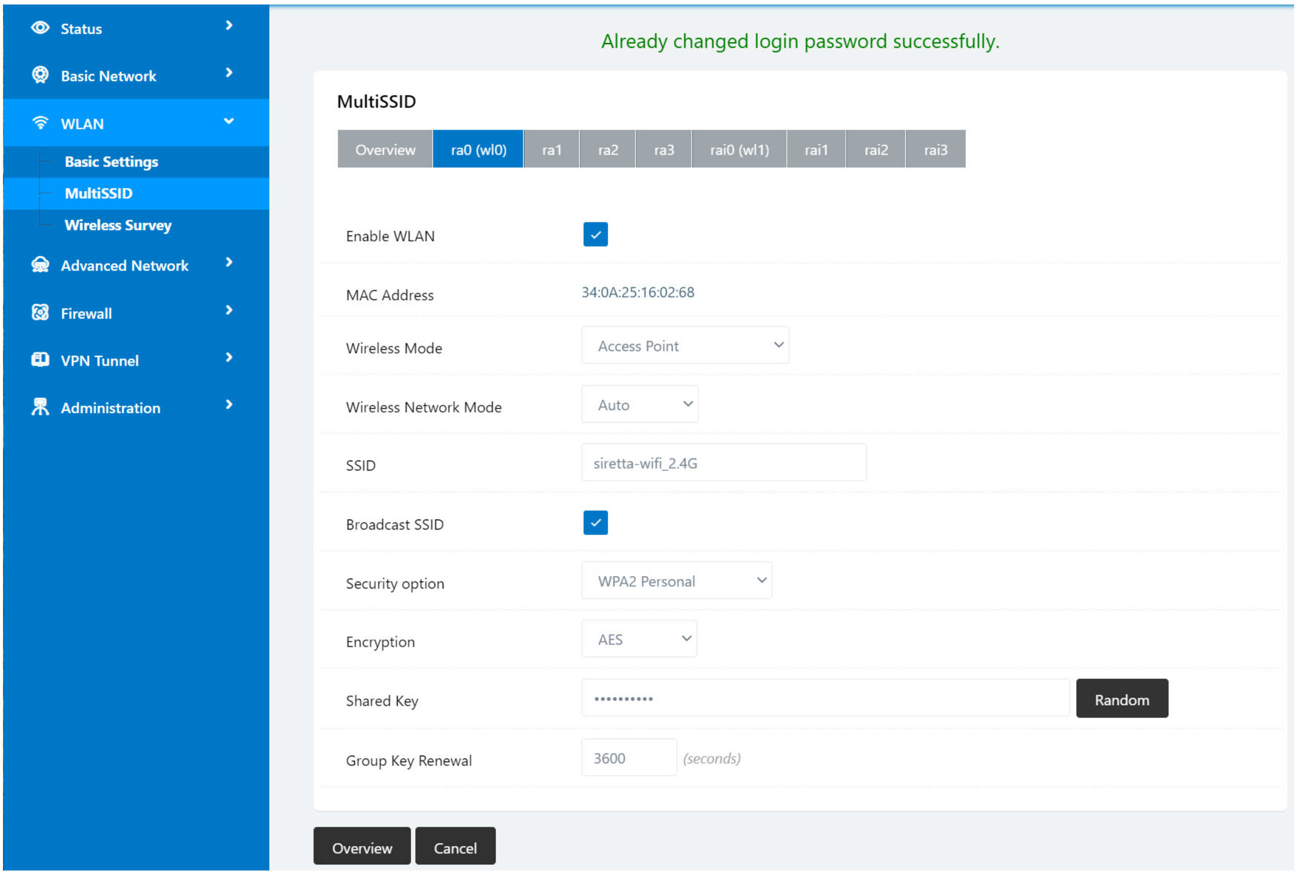
MultiSSID

Interface	Enabled	SSID	Mode	Bridge
ra0 (wl0)	Yes	siretta-wifi_2.4G	Access Point	LAN (br0)
rai0 (wl1)	Yes	siretta wifi_5G	Access Point	LAN (br0)
ra1	Yes	New SSID	Access Point	LAN (br0)
ra2	☑		Access Point	LAN (br0)

Multi-SSID Setting	Options
Interface	WiFi Interface used
Enabled?	Check to enable
Mode	Chosen Access Point, Wireless Client or Wireless Ethernet Bridge
Bridge	Chose an existing VLAN to connect to the SSID

IMPORTANT: After creating a new SSID, click Add+ to add it. After making all required changes, click ‘Save’ to apply them.

To set up security options, click on the tab at the top to reveal the security options for the SSID created, which may be set up in the same way as the primary SSIDs on the WiFi radio.



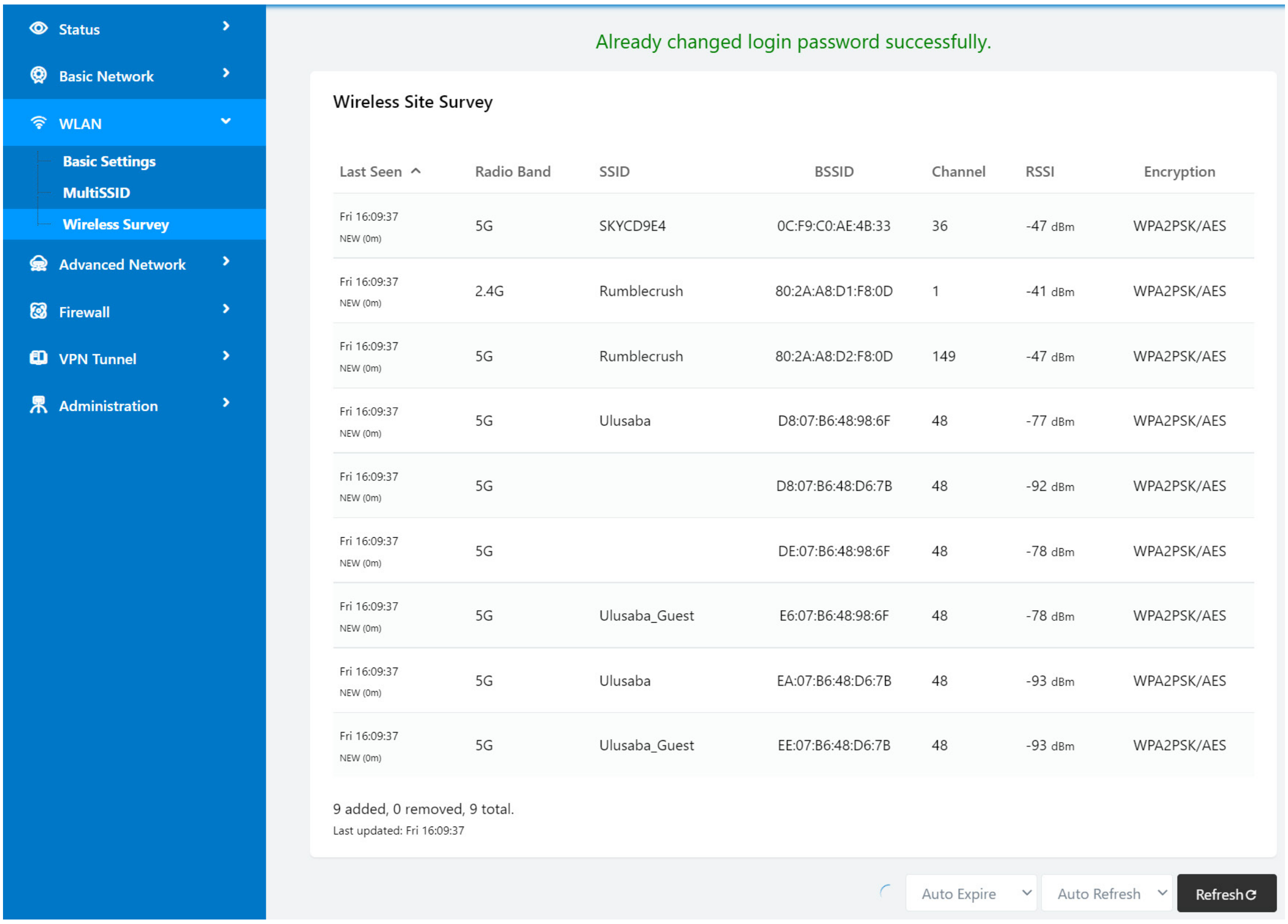
Already changed login password successfully.

MultiSSID

Enable WLAN	☑
MAC Address	34:0A:25:16:02:68
Wireless Mode	Access Point
Wireless Network Mode	Auto
SSID	siretta-wifi_2.4G
Broadcast SSID	☑
Security option	WPA2 Personal
Encryption	AES
Shared Key	••••••••••
Group Key Renewal	3600 *(seconds)*

Wireless Survey

This shows details of the surrounding WiFi networks. This can be used to help decide the most suitable WiFi channel to use on the QUARTZ-GOLD-5G or find a network to connect to as a wireless client.



Already changed login password successfully.

Wireless Site Survey

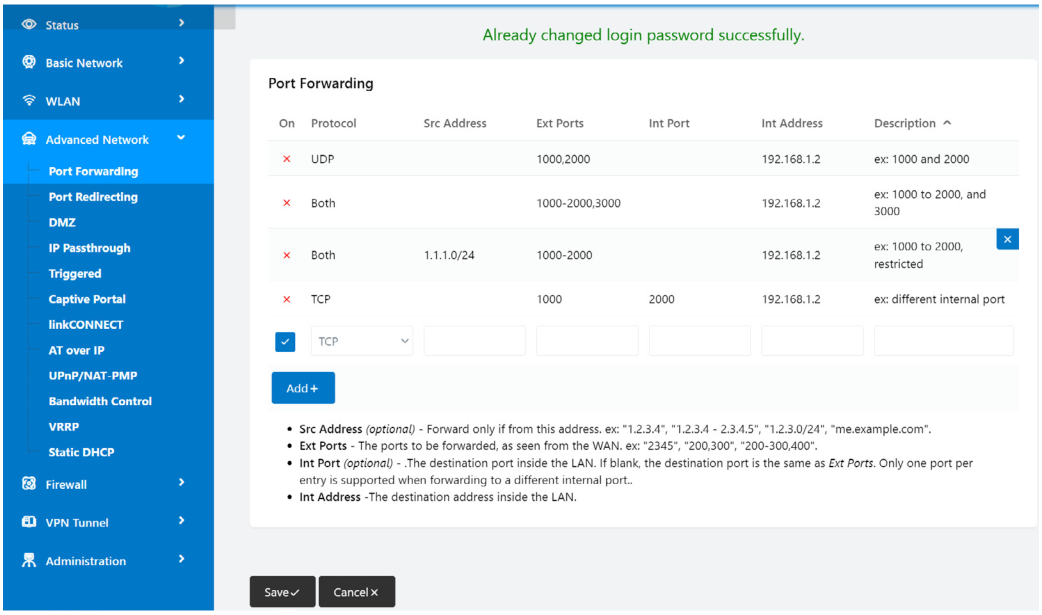
Last Seen	Radio Band	SSID	BSSID	Channel	RSSI	Encryption
Fri 16:09:37 NEW (0m)	5G	SKYCD9E4	0C:F9:C0:AE:4B:33	36	-47 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	2.4G	Rumblecrush	80:2A:A8:D1:F8:0D	1	-41 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G	Rumblecrush	80:2A:A8:D2:F8:0D	149	-47 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G	Ulusaba	D8:07:B6:48:98:6F	48	-77 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G		D8:07:B6:48:D6:7B	48	-92 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G		DE:07:B6:48:98:6F	48	-78 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G	Ulusaba_Guest	E6:07:B6:48:98:6F	48	-78 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G	Ulusaba	EA:07:B6:48:D6:7B	48	-93 dBm	WPA2PSK/AES
Fri 16:09:37 NEW (0m)	5G	Ulusaba_Guest	EE:07:B6:48:D6:7B	48	-93 dBm	WPA2PSK/AES

9 added, 0 removed, 9 total.
Last updated: Fri 16:09:37

Advanced Network

Port Fowarding

Set up port forwarding rules here. These rules allow the routing of packets arriving on specific ports from optionally specific IP addresses external to the WAN interface to be forwarded to specific internal IP addresses and optionally specific ports on the local LAN.



Already changed login password successfully.

Port Forwarding

On	Protocol	Src Address	Ext Ports	Int Port	Int Address	Description ^
×	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
×	Both		1000-2000,3000		192.168.1.2	ex: 1000 to 2000, and 3000
×	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
×	TCP		1000	2000	192.168.1.2	ex: different internal port
☑	TCP					

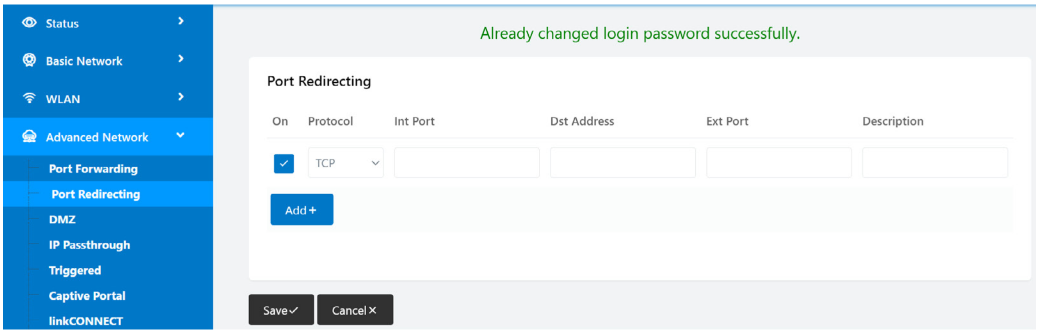
- **Src Address** *(optional)* - Forward only if from this address. ex: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.example.com".
- **Ext Ports** - The ports to be forwarded, as seen from the WAN. ex: "2345", "200,300", "200-300,400".
- **Int Port** *(optional)* - .The destination port inside the LAN. If blank, the destination port is the same as *Ext Ports*. Only one port per entry is supported when forwarding to a different internal port..
- **Int Address** -The destination address inside the LAN.

Port Forward Setting	Options
On	Check to enable the line
Protocol	Choose TCP, UDP or Both
Src Address	Optionally enter source address as IPv4 address or DNS resolvable name. Only traffic from this address may be passed by the rule.
Ext Ports	External ports. Enter ports separated by comma or a range or both.
Int Port	Optional internal port that matched packets will be forwarded to
Int Address	Internal IP address that matched packets will be forwarded to
Description	User description for the rule

IMPORTANT: After creating a new Port Forwarding rule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

Port Redirecting

Port redirecting redirects all traffic arriving on a user defined external WAN port to a specific IP address and port on the internal LAN.



Already changed login password successfully.

Port Redirecting

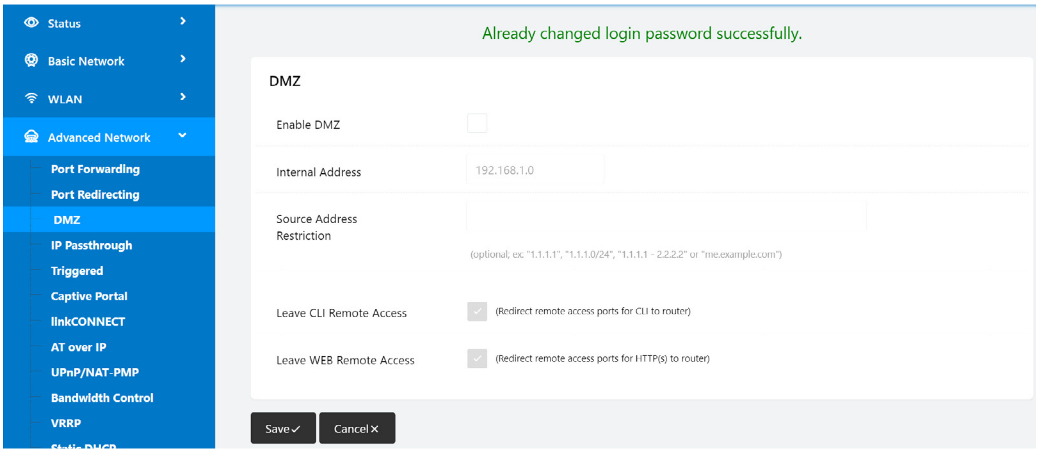
On	Protocol	Int Port	Dst Address	Ext Port	Description
☑	TCP				

Port Redirecting Setting	Options
On	Check to enable the line
Protocol	Choose TCP, UDP or TCP/UDP
Int Port	Internal port that matching packets will be forwarded to
Dst Address	Internal IP address that matching packets will be forwarded to
Ext Port	Enter port number external to the WAN whose traffic will be allowed entry through the firewall.
Description	User description for the rule

IMPORTANT: After creating a new Port Forwarding rule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

DMZ

Set up a DMZ here. The internal target address of the DMZ should be fixed by using Static DHCP.



Already changed login password successfully.

DMZ

Enable DMZ □

Internal Address 192.168.1.0

Source Address Restriction
(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")

Leave CLI Remote Access ☑ (Redirect remote access ports for CLI to router)

Leave WEB Remote Access ☑ (Redirect remote access ports for HTTP(s) to router)

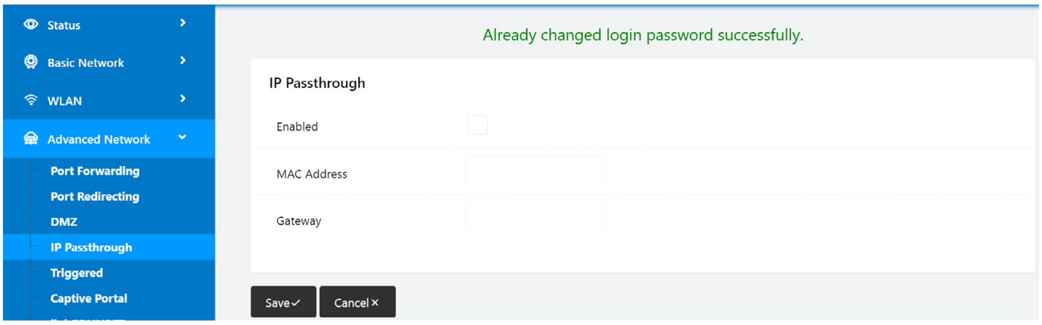
DMZ Setting	Options
Enable DMZ	Check to enable the DMZ
Internal Address	Internal IP address that packets on the WAN external interface will be forwarded to
Source Address Restriction	Limit the DMZ to pass only packets from specific IP addresses or domains
Leave CLI Remote Access	Do not redirect traffic to the Telnet port used for the router CLI interface when enabled
Leave WEB Remote Access	Do not redirect traffic to the port used for the router web interface when enabled

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

IMPORTANT: For this to work correctly with a cellular WAN connection, a fixed IP address SIM must be used

IP Passthrough

IP passthrough bridges all traffic on the external WAN interface to a single device attached to the routers LAN port. Therefore, this device connected to the LAN will be assigned the IP address that would otherwise have been used by the WAN and not an IP address from the routers DHCP server, i.e. NAT does not occur.



Already changed login password successfully.

IP Passthrough

Enabled	□
MAC Address	
Gateway	

Port Forward Setting	Options
Enabled	Check to enable IP Passthrough
MAC Address	Enter MAC address of device on LAN being bridged to. DHCP must still be used on the LAN, but in this case the assigned IP address will be public IP address.
Gateway	Enter an IP address that may be used by other devices on the LAN to access the router otherwise the router GUI will not be accessible.

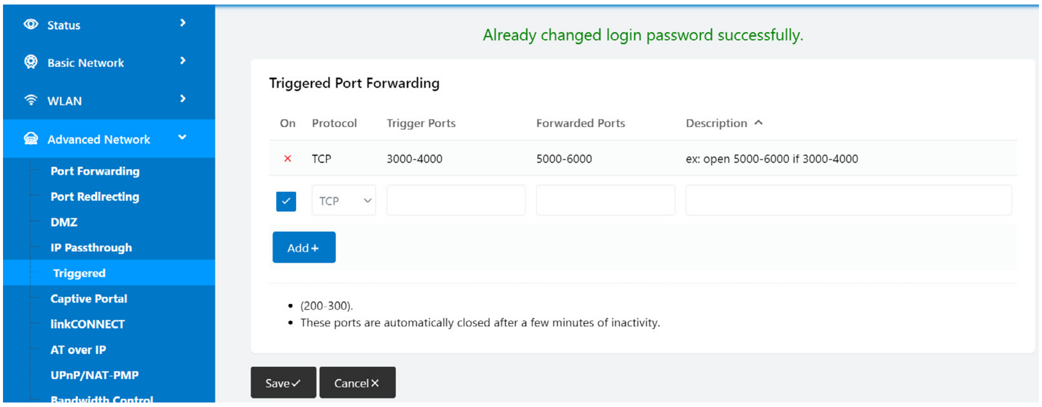
IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Triggered

Port trigger is a dynamic version of port forwarding. Outgoing traffic on a specific port will open an incoming port to the device on the LAN that originated the outgoing traffic. Incoming traffic on the opened port will be forwarded to all devices on the LAN that triggered the open port. The rule only applies while there is outgoing traffic.

Since the connection is not persistent and the connection dynamic, this is safer than port redirection which is always on. It also allows traffic on a port to be forwarded to multiple devices on the LAN.

See UPnP/NAT-PMP settings for details of how and when triggered ports are cleaned.



Already changed login password successfully.

Triggered Port Forwarding

On	Protocol	Trigger Ports	Forwarded Ports	Description ^
✕	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
☑	TCP			

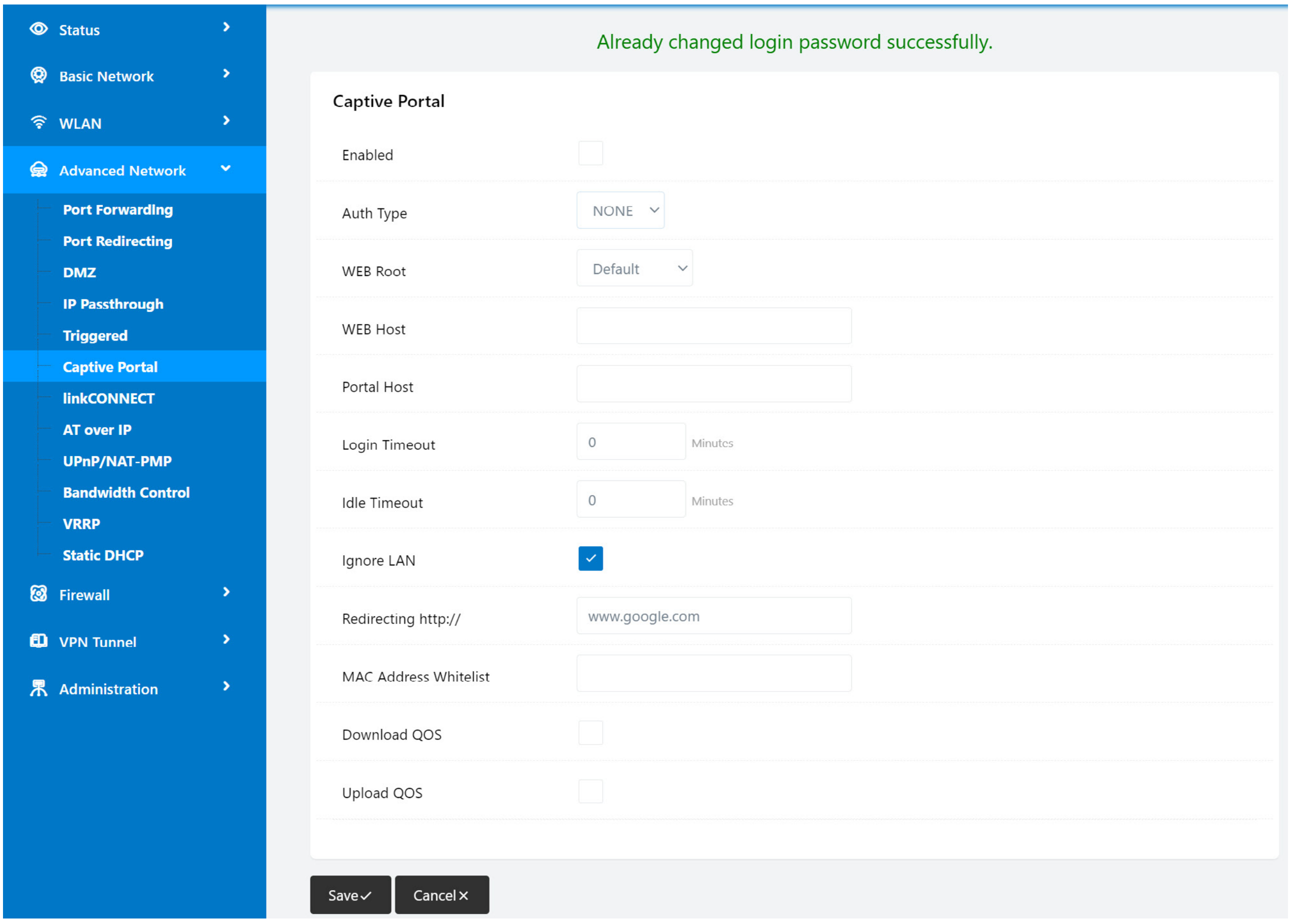
- (200-300).
- These ports are automatically closed after a few minutes of inactivity.

Triggered Setting	Options
On	Check to enable the line
Protocol	Choose TCP, UDP or Both
Trigger Ports	Chose port(s) to use as a trigger to open a port
Forwarded Ports	Chose the port(s) that will be forwarded from the WAN to the devices on the LAN that triggered the rule.
Description	User description for the rule

IMPORTANT: After creating a new Port Trigger rule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

Captive Portal

The Captive Portal is a web page that is accessed when first connecting to the router.



Already changed login password successfully.

Captive Portal

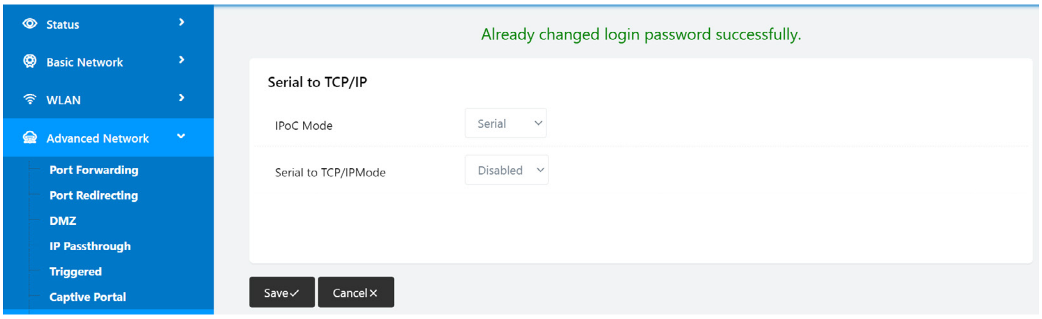
Enabled	□
Auth Type	NONE
WEB Root	Default
WEB Host	
Portal Host	
Login Timeout	0 Minutes
Idle Timeout	0 Minutes
Ignore LAN	☑
Redirecting http://	www.google.com
MAC Address Whitelist	
Download QOS	□
Upload QOS	□

Captive Portal Setting	Options
Enabled	Check to enable the Captive Portal
Auth Type	Reserved for future use
WEB Root	Select captive portal file storage: Default: Stored in router firmware In-Storage: Stored in internal flash memory Ex-Storage: Stored in extended internal flash memory.
WEB Host	Enter domain name for the captive portal access. LAN traffic for this domain is directed to the Captive Portal.
Portal Host	Reserved for future use
Login Timeout	Maximum user time allowed before forced to reconnect via the captive portal
Idle Timeout	Maximum user time allowed with no network activity before forced to reconnect via the captive portal
Ignore LAN	Enable to allow devices on the LAN to bypass the captive portal (so that the Captive Portal rules only apply to WiFi users)
Redirecting http://	Redirection page displayed once the terms and conditions on the captive portal have been accepted.
MAC Address Whitelist	Whitelist of MAC addresses that will bypass the captive portal
Download QOS	Enable to set download speeds for devices connected via the captive portal
Upload QOS	Enable to set upload speeds for devices connected via the captive portal

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

LinkCONNECT

This defines how the serial port on the connector shared with the power connection works. All versions of the QUARTZ-GOLD-5G come with a single RS232 port. As an option when purchasing the router, an RS485 Modbus port may be fitted in which case the user is able to select either the RS232 port or the RS485 port.



Already changed login password successfully.

Serial to TCP/IP

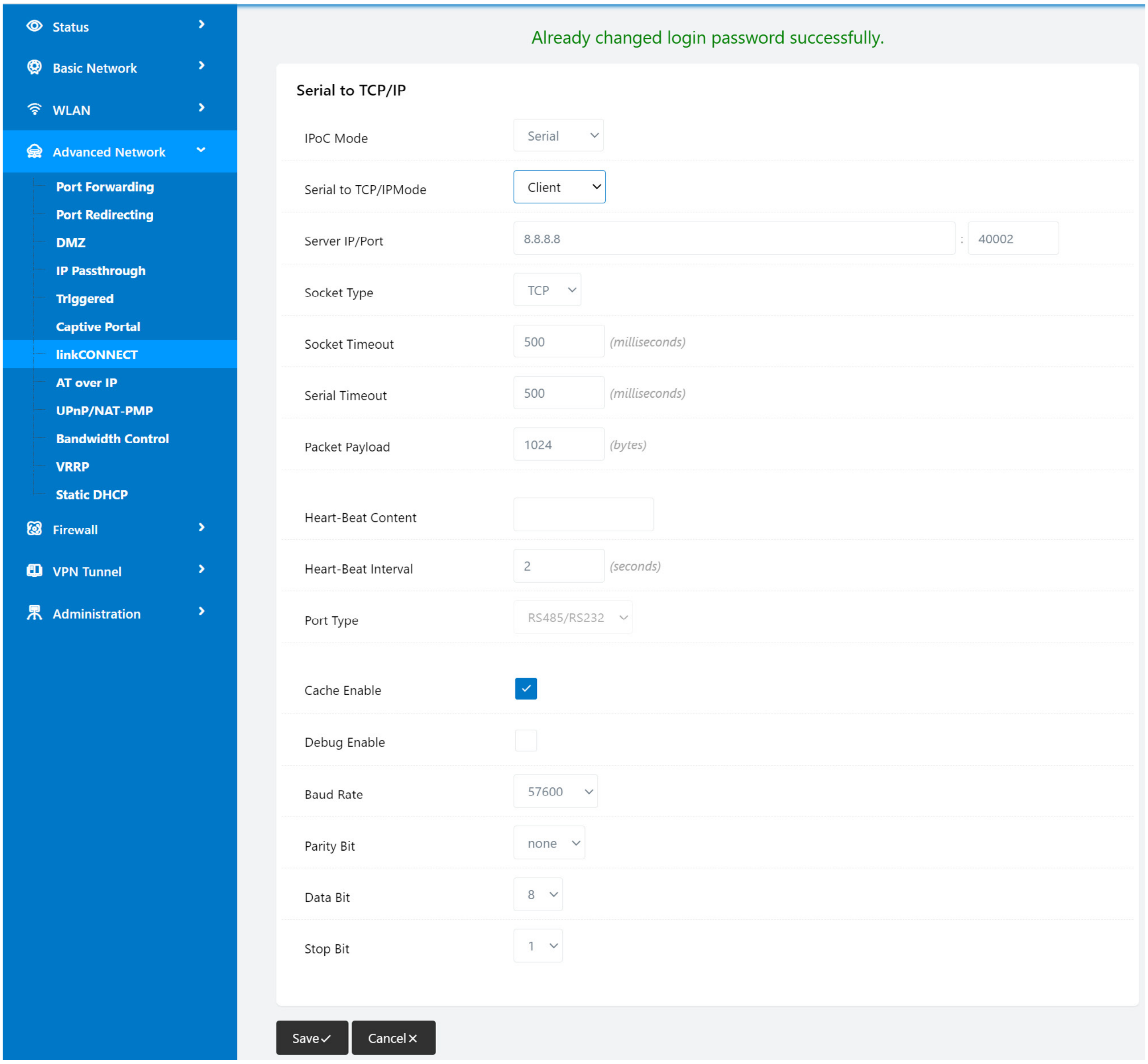
IPoC Mode: Serial

Serial to TCP/IPMode: Disabled

linkCONNECT Setting	Options
IPoC Mode	Choose Serial or Modbus. Selecting Modbus when the option is not fitted will disable the serial port.
Serial to TCP/IPMode	Choose Disabled, Server or Client (Serial) or Enable/Disable (Modbus)

IMPORTANT: After making these selections, further options pertinent to the mode of operation will be shown:

RS232 Client



Already changed login password successfully.

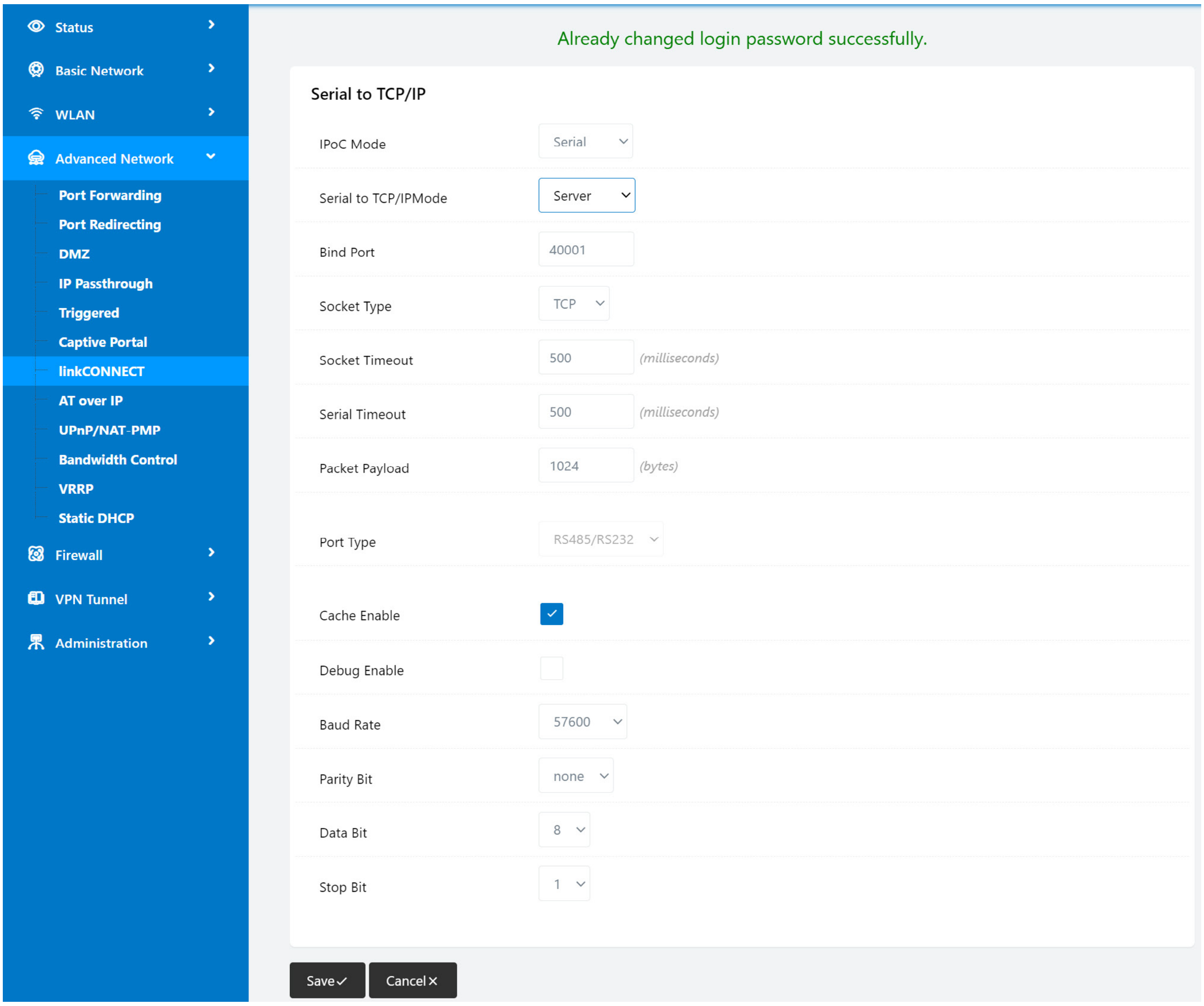
Serial to TCP/IP

IPoC Mode	Serial
Serial to TCP/IPMode	Client
Server IP/Port	8.8.8.8 : 40002
Socket Type	TCP
Socket Timeout	500 *(milliseconds)*
Serial Timeout	500 *(milliseconds)*
Packet Payload	1024 *(bytes)*
Heart-Beat Content	
Heart-Beat Interval	2 *(seconds)*
Port Type	RS485/RS232
Cache Enable	☑
Debug Enable	□
Baud Rate	57600
Parity Bit	none
Data Bit	8
Stop Bit	1

linkCONNECT Setting	Options
IPoC Mode	Choose Serial
Serial to TCP/IP Mode	Choose Client
Server IP/Port	Enter IP address / domain name and port of server
Socket type	Choose TCP or UDP
Socket Timeout	Choose socket timeout in mS. This the time that the router will wait if there is no more data before closing the socket.
Serial Timeout	Choose serial timeout in mS. This is the maximum waiting time for the serial data packet to reach its desired size. The serial data packet will be transmitted on the earlier of it reaching the desired size or this timeout setting.
Packet Payload	Desired size of the serial data packet. See Serial Timeout for explanation.
Heart-Beat Content	Add heart-beat content to serial data message to identify sender. Leave blank to disable heartbeat.
Heart-Beat Interval	Choose heartbeat send interval in seconds.
Port Type	Greyed out
Cache Enable	Check to enable data caching to reduce chances of data loss in poor reception areas
Debug Enable	Check to enable writing of debug information into the debug log
Baud Rate	Choose 300, 600, 1200, 2400, 9600, 19200, 38400, 57600 or 115200
Parity Bit	Choose none, odd or even
Data Bit	Choose 5, 6 7 or 8
Stop Bit	Choose 1 or 2

IMPORTANT: After making all required changes, click 'Save' to apply them.

RS232 Server



Already changed login password successfully.

Serial to TCP/IP

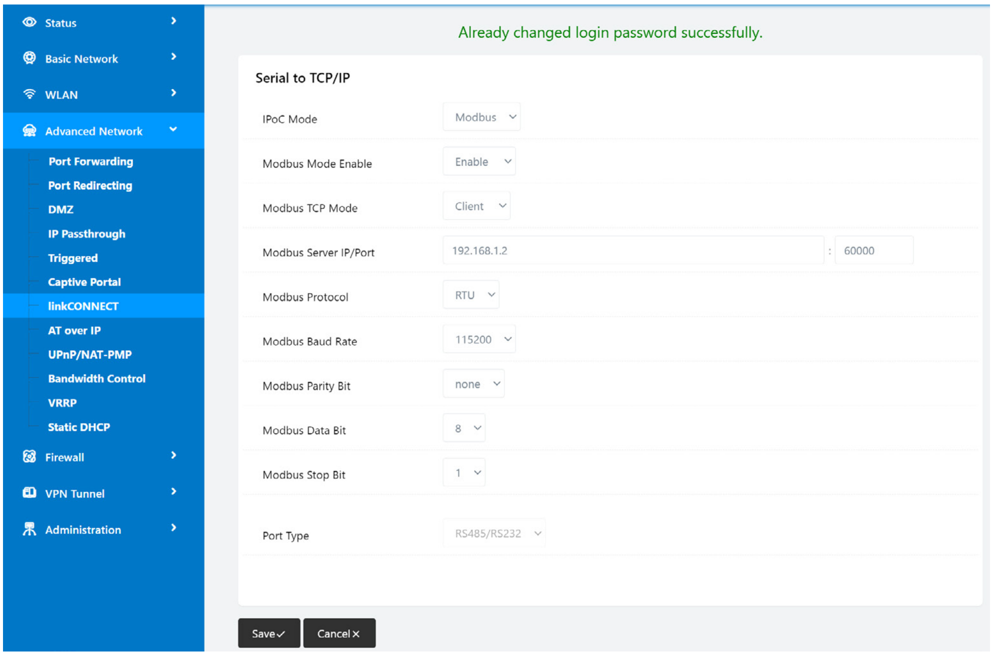
IPoC Mode	Serial
Serial to TCP/IPMode	Server
Bind Port	40001
Socket Type	TCP
Socket Timeout	500 *(milliseconds)*
Serial Timeout	500 *(milliseconds)*
Packet Payload	1024 *(bytes)*
Port Type	RS485/RS232
Cache Enable	☑
Debug Enable	□
Baud Rate	57600
Parity Bit	none
Data Bit	8
Stop Bit	1

linkCONNECT Setting	Options
IPoC Mode	Choose Serial
Serial to TCP/IP Mode	Choose Client
Bind Port	Enter IP address / domain name and port of server
Socket type	Choose TCP or UDP
Socket Timeout	Choose socket timeout in mS. This the time that the router will wait if there is no more data before closing the socket.
Serial Timeout	Choose serial timeout in mS. This is the maximum waiting time for the serial data packet to reach its desired size. The serial data packet will be transmitted on the earlier of it reaching the desired size or this timeout setting.
Packet Payload	Desired size of the serial data packet. See Serial Timeout for explanation.
Heart-Beat Content	Add heart-beat content to serial data message to identify sender. Leave blank to disable heartbeat.
Heart-Beat Interval	Choose heartbeat send interval in seconds.
Port Type	Greyed out
Cache Enable	Check to enable data caching to reduce chances of data loss in poor reception areas
Debug Enable	Check to enable writing of debug information into the debug log
Baud Rate	Choose 300, 600, 1200, 2400, 9600, 19200, 38400, 57600 or 115200
Parity Bit	Choose none, odd or even
Data Bit	Choose 5, 6 7 or 8
Stop Bit	Choose 1 or 2

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

RS485 Client

This defines how the serial ports on the connector shared with the power connection works. Up to two RS232 serial ports may be enabled or a single RS485 modbus port.



Already changed login password successfully.

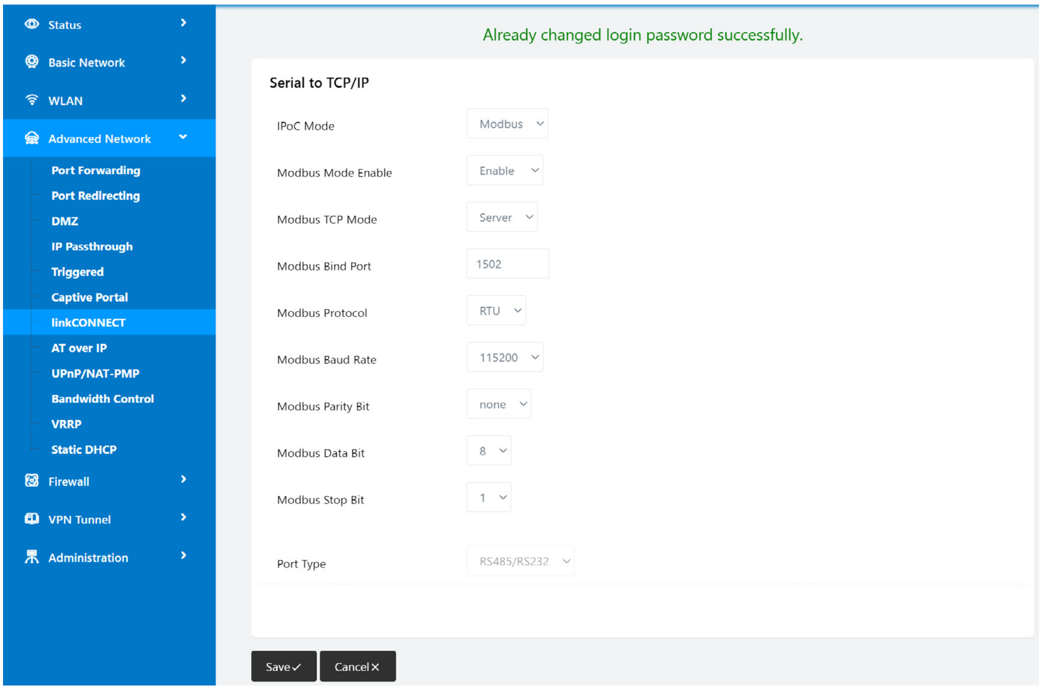
Serial to TCP/IP

IPoC Mode: Modbus
Modbus Mode Enable: Enable
Modbus TCP Mode: Client
Modbus Server IP/Port: 192.168.1.2 : 60000
Modbus Protocol: RTU
Modbus Baud Rate: 115200
Modbus Parity Bit: none
Modbus Data Bit: 8
Modbus Stop Bit: 1
Port Type: RS485/RS232

linkCONNECT Setting	Options
IPoC Mode	Set to Modbus
Modbus Mode Enable	Choose Enable
Modbus TCP Mode	Choose Client
Modbus Server IP/Port	Choose IP address and port of server to be connected to
Modbus Protocol	Always set to RTU
Modbus Baud Rate	Choose 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200
Modbus Parity Bit	Choose none, even or odd
Modbus Data Bit	Choose 5, 6, 7 or 8
Modbus Stop Bit	Choose 1 or 2
Port Type	Greyed out

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

RS485 Server



Already changed login password successfully.

Serial to TCP/IP

IPoC Mode: Modbus
Modbus Mode Enable: Enable
Modbus TCP Mode: Server
Modbus Bind Port: 1502
Modbus Protocol: RTU
Modbus Baud Rate: 115200
Modbus Parity Bit: none
Modbus Data Bit: 8
Modbus Stop Bit: 1
Port Type: RS485/RS232

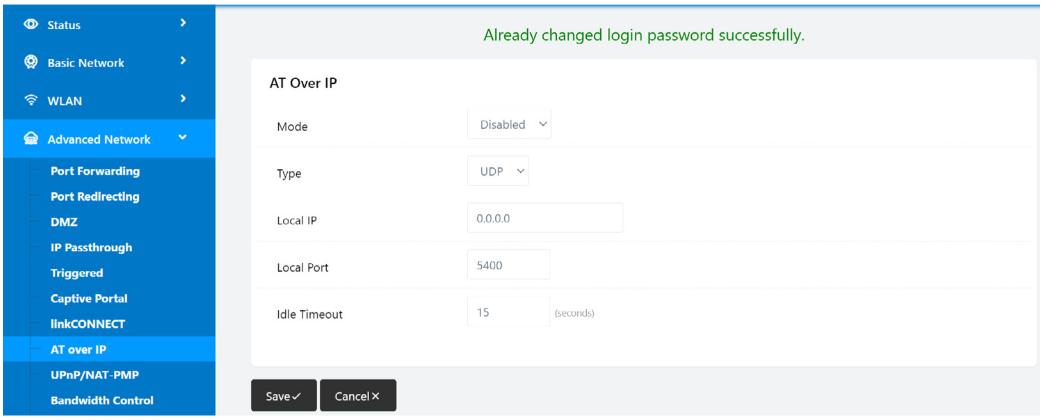
linkCONNECT Setting	Options
IPoC Mode	Set to Modbus
Modbus Mode Enable	Choose Enable
Modbus TCP Mode	Choose Server
Modbus Server Bind Port	Specify port for incoming connections
Modbus Protocol	Always set to RTU
Modbus Baud Rate	Choose 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200
Modbus Parity Bit	Choose none, even or odd
Modbus Data Bit	Choose 5, 6, 7 or 8
Modbus Stop Bit	Choose 1 or 2
Port Type	Greyed out

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

AT over IP

This allows for AT commands to be sent directly to the Cellular modem inside the QUARTZ-GOLD-5G router.

Important:Take care with the AT commands sent to the modem as it is possible to interfere with the router's cellular operation by use of this feature.



Already changed login password successfully.

AT Over IP

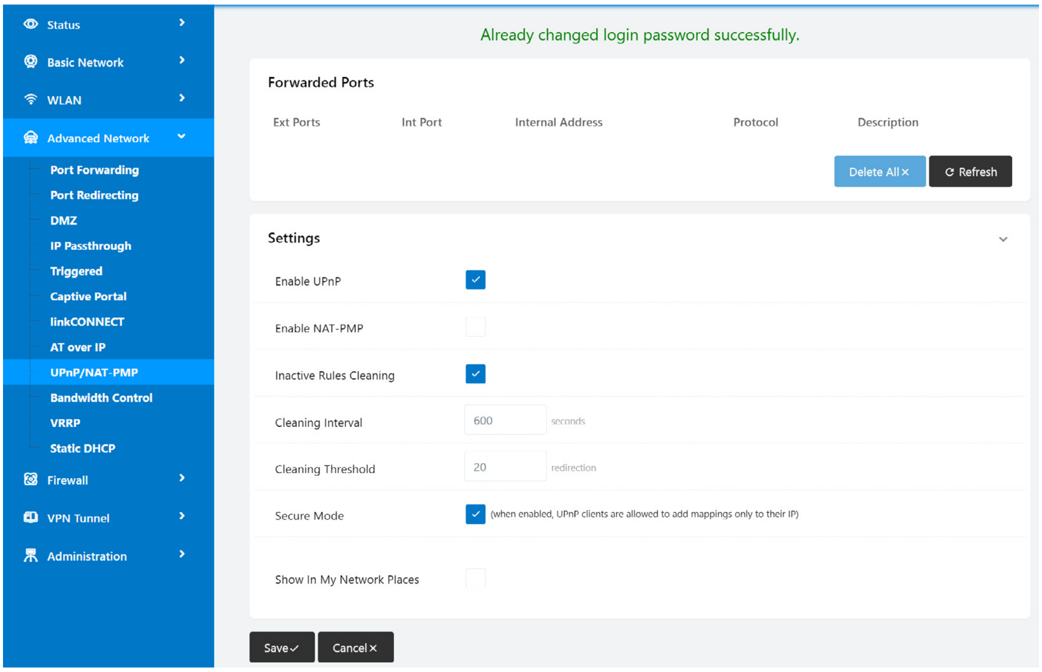
Mode	Disabled
Type	UDP
Local IP	0.0.0.0
Local Port	5400
Idle Timeout	15 (seconds)

AT over IP Setting	Options
Mode	Choose Disabled or Enabled
Type	Choose UDP or TCP
Local IP	Local IP address to be used to access the AT over IP function
Local Port	Local port to be used to access the AT over IP function
Idle Timeout	Choose socket timeout in mS. This the time that the router will wait if there is no more AT commands being sent before closing the socket.

IMPORTANT: After making all required changes, click 'Save' to apply them.

UNnP /NAT-PMP

Universal Plug and Play/NAT Port Mapping Protocol settings. Active triggered ports are show and cleanup rules may be applied.



Already changed login password successfully.

Forwarded Ports

Ext Ports	Int Port	Internal Address	Protocol	Description

Settings

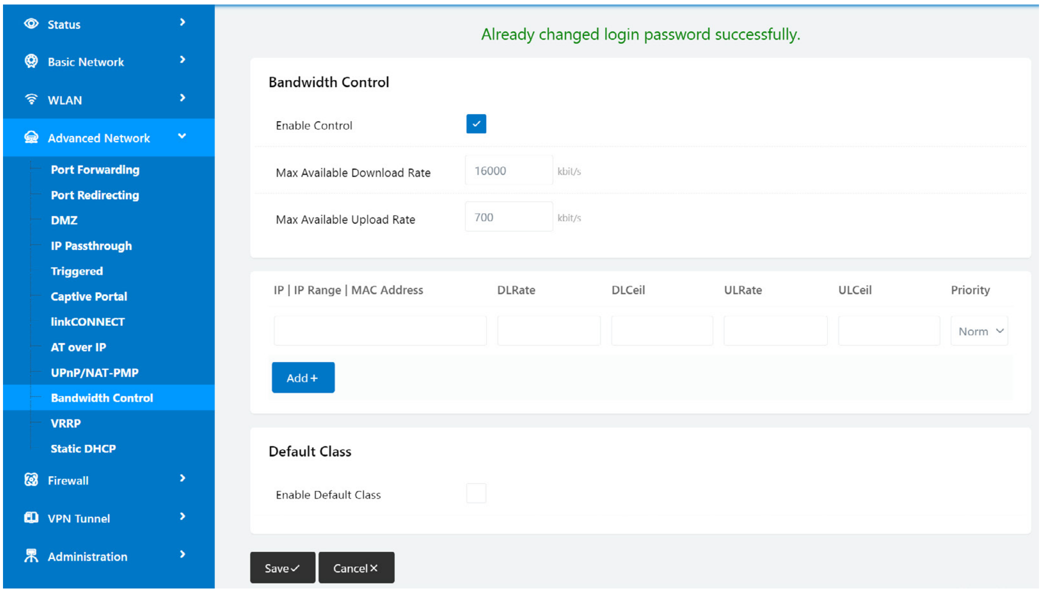
Enable UPnP	☑
Enable NAT-PMP	☐
Inactive Rules Cleaning	☑
Cleaning Interval	600 seconds
Cleaning Threshold	20 redirection
Secure Mode	☑ (when enabled, UPnP clients are allowed to add mappings only to their IP)
Show In My Network Places	☐

UPnP/NAT-PMP Setting	Options
Enable UPnP	Check to enable
Enable NAT-PMP	Check to enable
Inactive Rules Cleaning	Check to enable
Cleaning Interval	Choose time in seconds from when the last network traffic meeting the rule occurred.
Cleaning Threshold	Choose threshold if inactive rules cleaning enabled
Secure mode	Check to enable (when enabled, UPnP clients are allowed to add mappings only to their IP)
Show in my Network Places	Check to enable. This allows the router to appear as a gateway in a Windows browsable LAN network.

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Bandwidth Control

Settings to control the allowed bandwidth and priority by IP address, IP range or MAC address.



Already changed login password successfully.

Bandwidth Control

Enable Control	☑
Max Available Download Rate	16000 kbit/s
Max Available Upload Rate	700 kbit/s

IP | IP Range | MAC Address	DLRate	DLCeil	ULRate	ULCeil	Priority
					Norm

Default Class

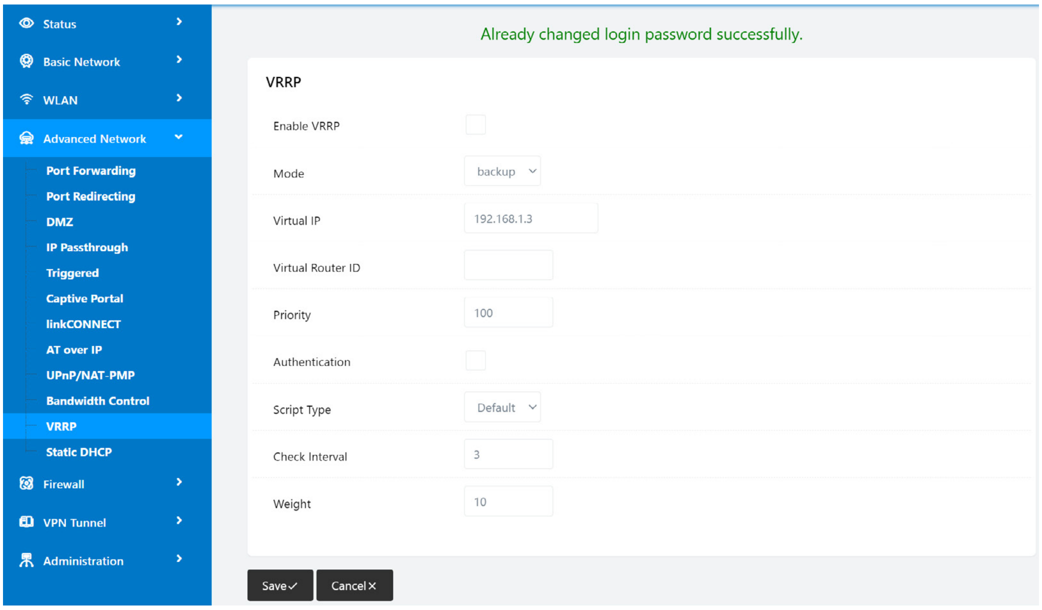
Enable Default Class	□

Bandwidth Limiter Setting	Options
Enable Control	Check to enable
Max Available Download Rate	Enter download speed of routers Internet connection if bandwidth control enabled in kbit/s
Max Available Upload Rate	Enter upload speed of routers Internet connection if bandwidth control enabled in kbit/s
IP | IP Range | MAC Address	Chose the device(s) to be limited by IP or MAC address
DL Rate	Average permitted download rate in kbit/s
DL Ceil	Absolute maximum download rate in kbit/s
UL Rate	Average permitted upload rate in kbit/s
UL Ceil	Absolute maximum upload rate in kbit/s
Priority	Choose highest, high, normal, low or lowest
Enable Default Class	Check to enable default rules for unspecified connections

IMPORTANT: After creating a new Bandwidth Control rule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

VRRP

Virtual Router Redundancy Protocol. Settings to switch routing path to different routers. The VRRP works in non-pre-emptive mode where the router configured as the master will operate as the master regardless of whether it has the highest priority, until such time that it fails.



Already changed login password successfully.

VRRP

Enable VRRP	□
Mode	backup
Virtual IP	192.168.1.3
Virtual Router ID	
Priority	100
Authentication	□
Script Type	Default
Check Interval	3
Weight	10

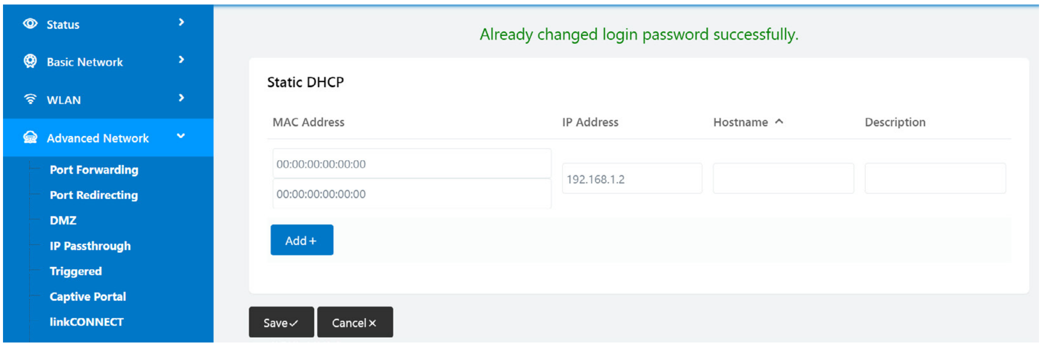
VRRP Setting	Options
Enable VRRP	Check to enable
Mode	Choose master or backup
Virtual IP	Chose the virtual gateway IP address of the virtual router. This must be an unused IP address of the subnet used by the VRRP. It may be the address of one of the routers.
Virtual Router ID	Enter an ID for the router (must be unique for each router in the network)
Priority	Set router priority. The highest priority router will be the active one. By default, use 100; the MAC address owner should use 255.
Authentication	Check to enable
Password	Enter password (required if authentication enabled)
Script Type	Chose default or ICMP
IP Address	Enter IP address or domain name if ICMP script selected
Check Interval	Interval in seconds to check the VRRP configuration
Weight	Weight setting to adjust the priority should the check fail

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Static DHCP

This allows the setup of binding a MAC address to an IP address. It is possible to assign 2 MAC addresses to one IP address. The usage case for this is to assign the same IP address to the LAN and WiFi ports of a client so that the client has the same IP address no matter what it's connection medium.

Warning: Binding two MAC addresses to a single IP address in any other situation is likely to cause networking problems.



Already changed login password successfully.

Static DHCP

MAC Address	IP Address	Hostname	Description
00:00:00:00:00:00 00:00:00:00:00:00	192.168.1.2		

Static DHCP Setting	Options
MAC Address	Enter MAC address
IP Address	Enter IP address to be bound to MAC address
Hostname	Enter host name. A space is not a valid DHCP hostname character and is inside used as a name separator if multiple hostnames are to be assigned to a single IP address.
Description	User description for the rule

IMPORTANT: After creating a new Static DHCP rule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

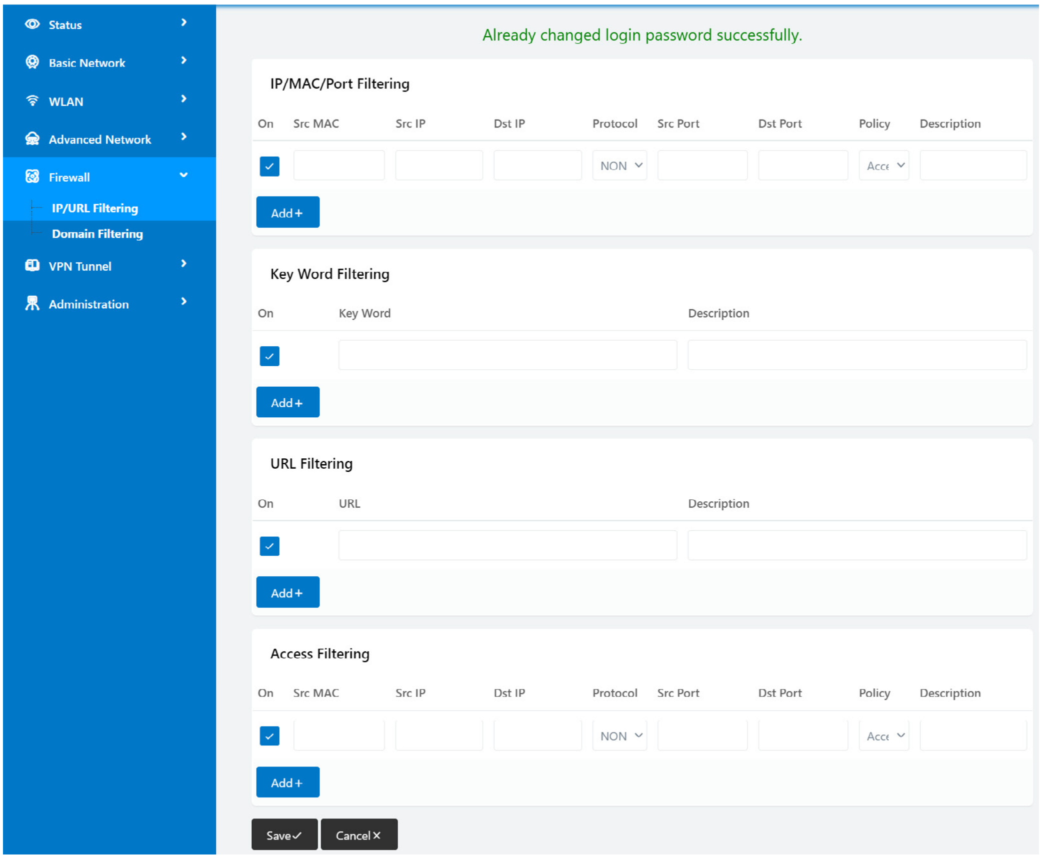
Firewall

IP/URL Filtering

This allows for the filtering of key words, MAC addresses and ports, as well as IP addresses and URLs.

IP/MAC/Port filtering, key word filtering and URL filtering control what passes from the routers WAN/Cellular interface to the Internet.

Access Filtering controls what passes from the Internet through the WAN/Cellular interface to the local subnets behind the router.



Already changed login password successfully.

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NON			Acce	

Key Word Filtering

On	Key Word	Description
☑		

URL Filtering

On	URL	Description
☑		

Access Filtering

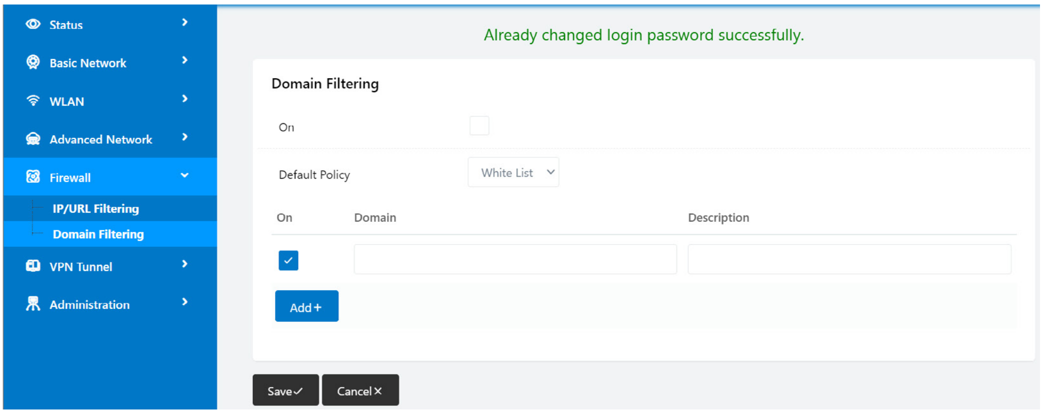
On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NON			Acce	

IP/URL Setting	Options
On	Check to enable rule
Src MAC	Enter source MAC address (optional)
Src IP	Enter source IP address (defaults to any/0 if left blank)
Dst IP	Enter destination IP address (defaults to any/0 if left blank)
Protocol	Choose none, TCP, UDP or ICMP
Src Port	Enter source port (optional)
Dst Port	Enter destination port (optional)
Policy	Choose drop or accept
Key Word	Enter a key word
URL Filter	Enter a URL
Description	User description for the rule

IMPORTANT: After creating a new firewall rule, click Add+ to add it. After making all required changes, click 'Save' to apply them.

Domain Filtering

This can be used to either allow specified domains, or reversed so that it blocks specified domains.



Already changed login password successfully.

Domain Filtering

On □

Default Policy: White List

On	Domain	Description
☑		

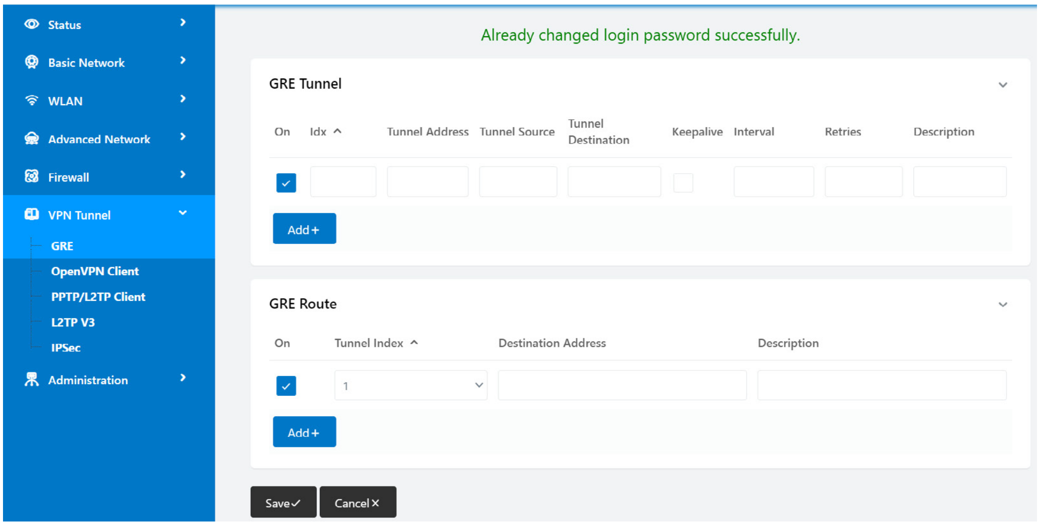
Domain Filtering Setting	Options
On	Check to enable rule
Default Policy	Choose whitelist or blacklist
Domain	Choose domain
Description	User description for the rule

IMPORTANT: After creating a new default policy rule, click Add+ to add it. After making all required changes, click ‘Save’ to apply them.

VPN Tunnel

GRE

GRE (Generic Routing Encapsulation) support for up to 8 tunnels may be set up here.



Already changed login password successfully.

GRE Tunnel

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
☑					□			

Add+

GRE Route

On	Tunnel Index	Destination Address	Description
☑	1		

Add+

Save✓ Cancel✕

GRE Tunnel Setting	Options
GRE Tunnel Setting	Options
On	Check to enable rule
Idx	Enter index number between 1 and 8
Tunnel Address	GRE tunnel local address
Tunnel Source	Routers public IP address from WAN/LTE
Tunnel Destination	Remote IP address of GRE tunnel, typically a public IP address
Keepalive	Check to always keep tunnel alive
Interval	Interval between keep alive retries
Retries	Number of keep alive retry times before a tunnel will be re-established

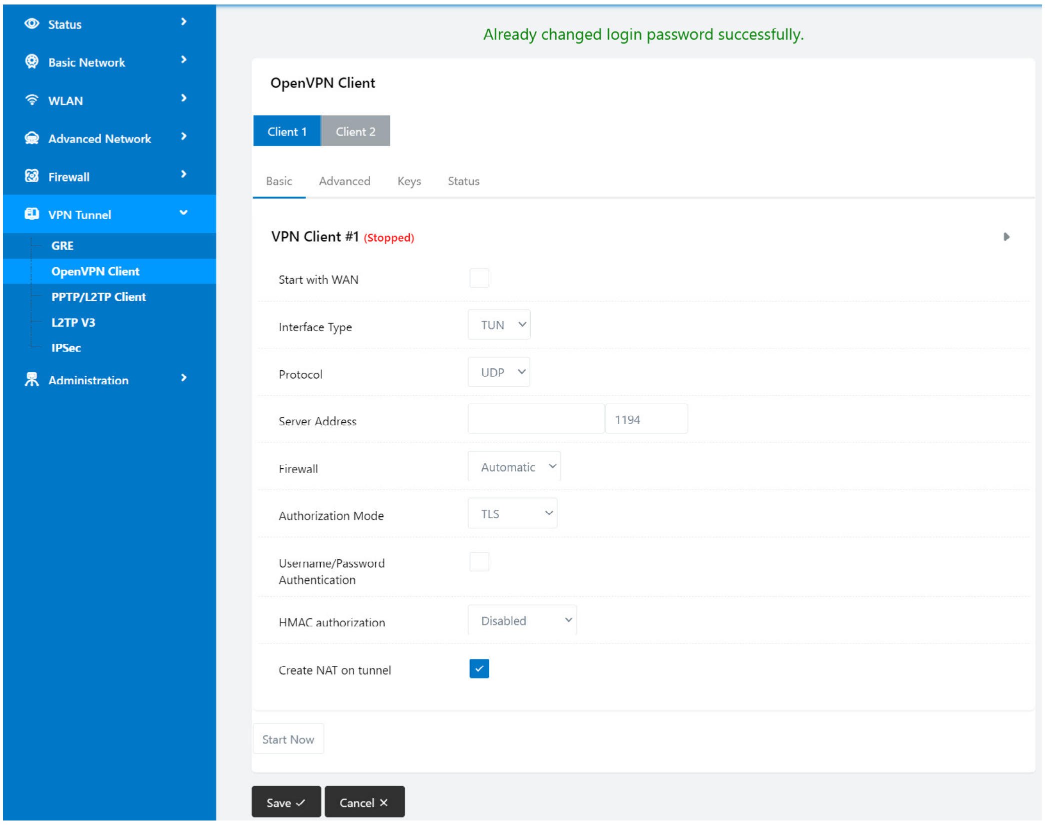
IMPORTANT: After creating a new GRE tunnel, click Add+ to add it. After making all required changes, click ‘Save’ to apply them.

GRE Route Setting	Options
Tunnel Index	Select between 1 and 8
Destination Address	Enter remote network IP address and mask
Description	User description for the rule

IMPORTANT: After creating a new GRE route, click Add+ to add it. After making all required changes, click 'Save' to apply them.

OpenVPN Client

Configure up to two OpenVPN Clients here.



Already changed login password successfully.

OpenVPN Client

VPN Client #1 (Stopped)

Start with WAN □

Interface Type: TUN

Protocol: UDP

Server Address: 1194

Firewall: Automatic

Authorization Mode: TLS

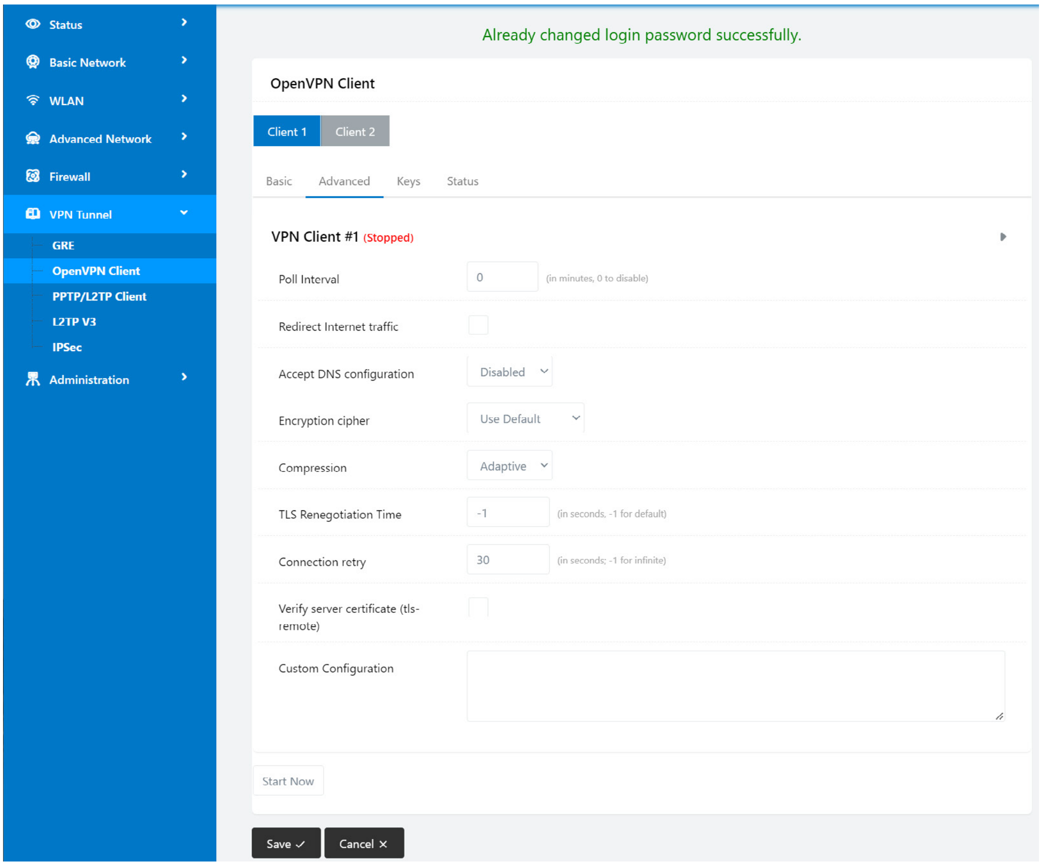
Username/Password Authentication □

HMAC authorization: Disabled

Create NAT on tunnel ☑

OpenVPN Basic Setting	Options
Start with WAN	Check to enable
Interface type	Select TAP or TUN (optional settings, TAP is bridge mode, TUN is routing mode)
Protocol	Select UDP or TCP (optional settings)
Server Address	Select OpenVPN server address and port
Firewall	Choose Automatic or Custom (optional settings)
Authorization Mode	Choose TLS, Static Key or Custom (optional settings)
Username/Password Authentication	Enable and complete as required by OpenVPN server
HMAC authorization	Choose Disabled, Bi-directional, Incoming (0) or Outgoing (1) as required by OpenVPN server
Create NAT on tunnel	Check for automatic route creation (otherwise they need to be created manually)

IMPORTANT: After making all required changes, click ‘Save’ to apply them.



Already changed login password successfully.

OpenVPN Client

VPN Client #1 (Stopped)

Poll Interval: 0 (in minutes, 0 to disable)

Redirect Internet traffic: □

Accept DNS configuration: Disabled

Encryption cipher: Use Default

Compression: Adaptive

TLS Renegotiation Time: -1 (in seconds, -1 for default)

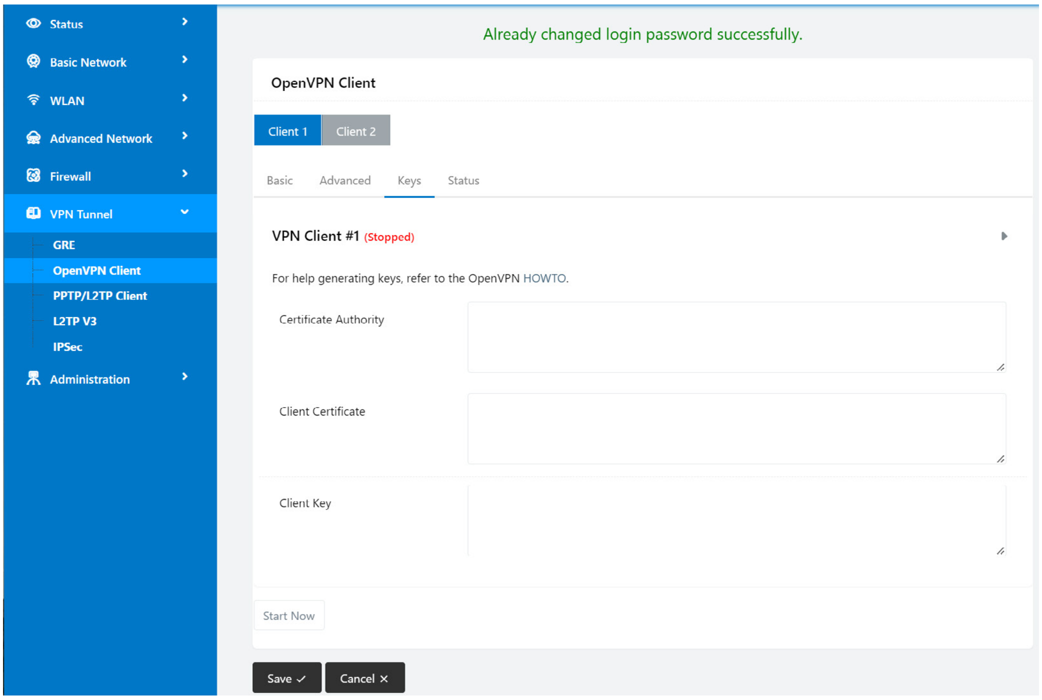
Connection retry: 30 (in seconds; -1 for infinite)

Verify server certificate (tls-remote): □

Custom Configuration:

OpenVPN Advanced Setting	Options
Poll Interval	OpenVPN client status check interval (in minutes)
Redirect Internet Traffic	Check to make OpenVPN the default route
Accept DNS configuration	As required by OpenVPN server
Encryption cipher	As required by OpenVPN server
Compression	As required by OpenVPN server
TLS renegotiation time	TLS negotiation time (in seconds)
Connect retry	OpenVPN connection retry interval
Verify server certificate (tls-remote)	As required by OpenVPN server
Custom Configuration	As required by OpenVPN server

IMPORTANT: After making all required changes, click ‘Save’ to apply them.



Already changed login password successfully.

OpenVPN Client

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

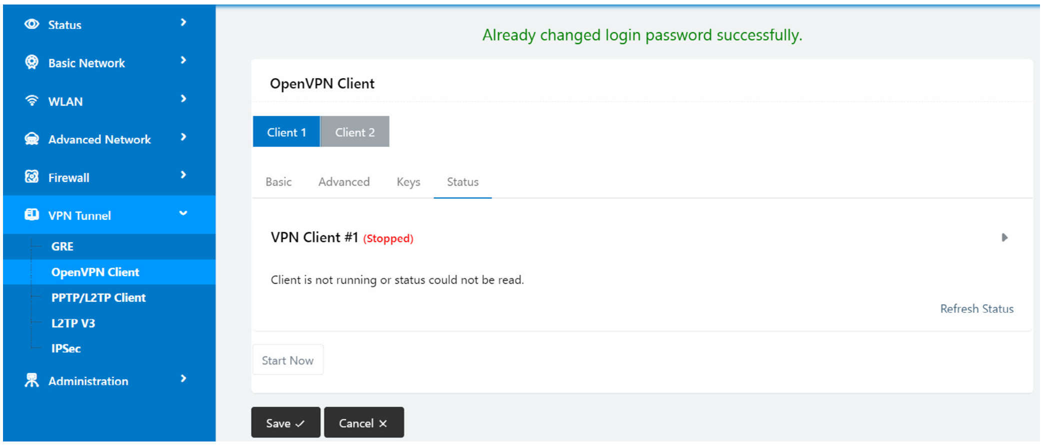
Certificate Authority

Client Certificate

Client Key

OpenVPN Key Setting	Options
Certificate Authority	As required by OpenVPN server
Client Certificate	As required by OpenVPN server
Client Key	As required by OpenVPN server

Click refresh status to see the status of the OpenVPN tunnel and data statistics.



Already changed login password successfully.

OpenVPN Client

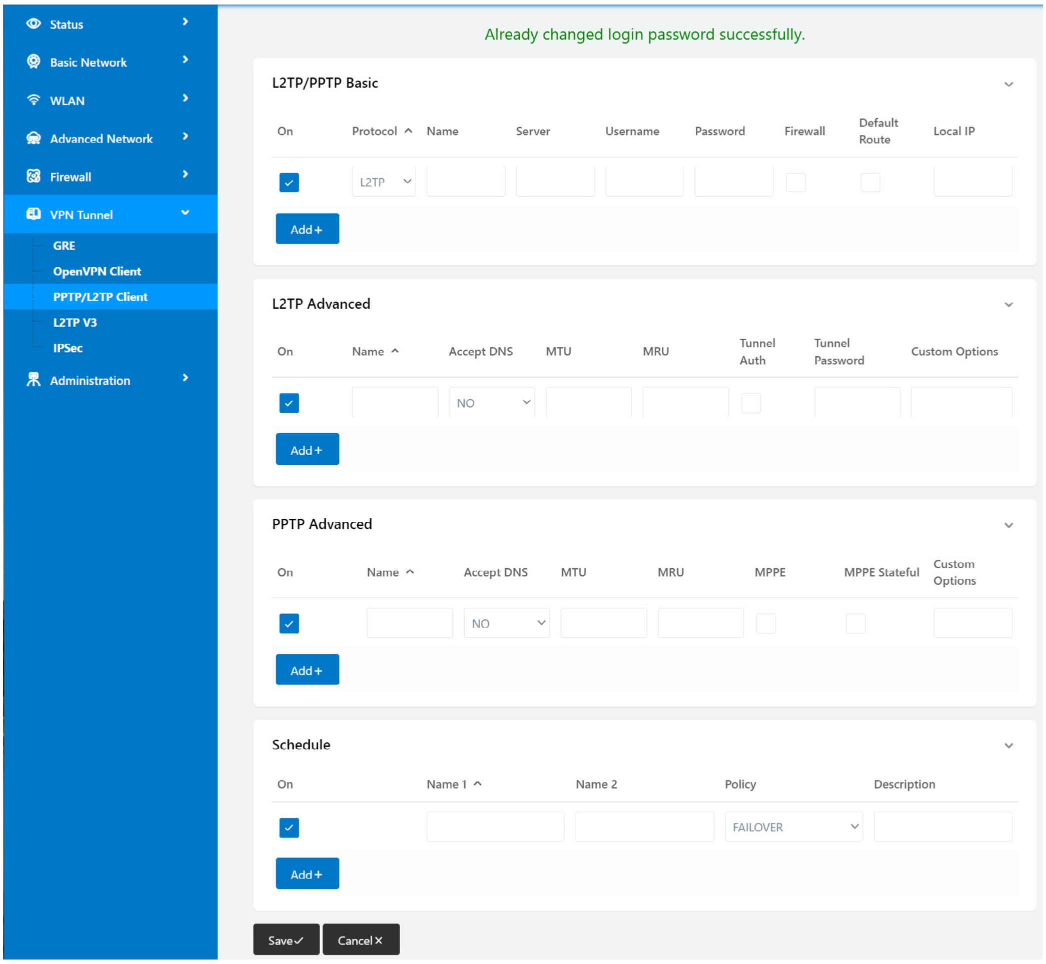
VPN Client #1 (Stopped)

Client is not running or status could not be read.

Click refresh status to see the status of the OpenVPN tunnel and data statistics.

PPTP/L2TP Client

Configure PPTP and L2TP tunnels here.



Already changed login password successfully.

L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
☑	L2TP					□	□	

L2TP Advanced

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
☑		NO			□		

PPTP Advanced

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
☑		NO			□	□	

Schedule

On	Name 1	Name 2	Policy	Description
☑			FAILOVER	

L2TP/PPTP Basic Setting	Options
On	Check to enable rule
Protocol	Choose L2TP or PPTP
Name	User chosen name for the VPN tunnel
Server	IP address of VPN server
Username	As required by VPN server
Password	As required by VPN server
Firewall	Check to apply firewall to VPN tunnel
Default Route	Check to make this runnel the routers default route
Local IP	Local IP address for the tunnel

IMPORTANT: After creating a new L2TP/PPTP VPN, click Add+ to add it. After making all required changes, click 'Save' to apply them.

L2TP Advanced Setting	Options
On	Check to enable rule
Name	User chosen name for the L2TP VPN tunnel
Accept DNS	Choose Yes or No
MTU	Suggest 1450
MRU	Suggest 1450
Tunnel Auth	Check to enable tunnel authentication if required by L2TP server
Tunnel Password	As required by L2TP VPN server if authentication enabled
Custom Options	Not normally necessary

IMPORTANT: After creating new L2TP advanced options, click Add+ to add it. After making all required changes, click 'Save' to apply them.

PPTP Advanced Setting	Options
On	Check to enable rule
Name	User chosen name for the L2TP VPN tunnel
Accept DNS	Choose Yes or No
MTU	Suggest 1450
MRU	Suggest 1450
MPPE	As required by PPTP VPN server
MPPE Stateful	As required by PPTP VPN server
Custom Options	Not normally necessary

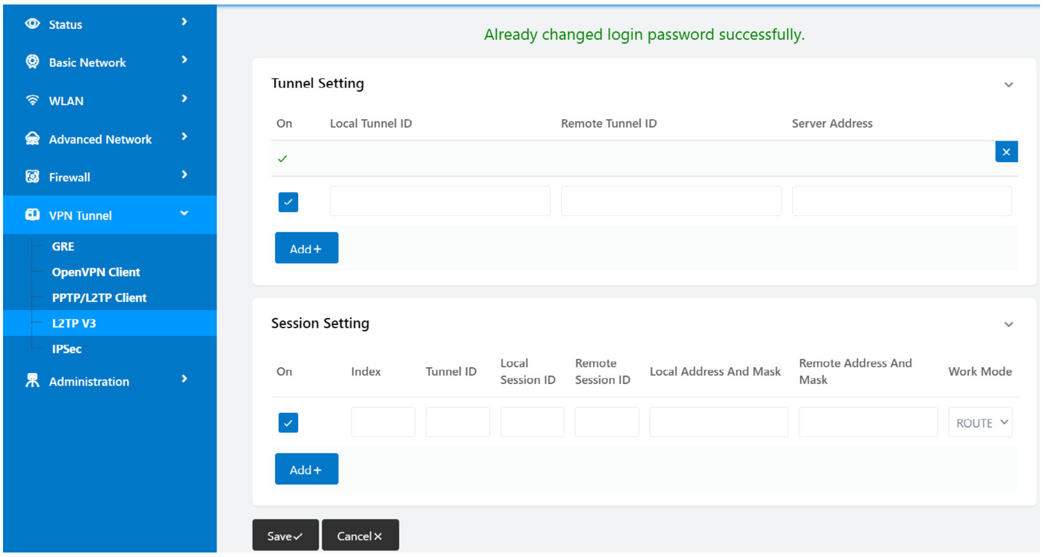
IMPORTANT: After creating new PPTP advanced options, click Add+ to add it. After making all required changes, click 'Save' to apply them.

Schedule Setting	Options
On	Check to enable rule
Name 1	VPN tunnel name
Name 2	VPN tunnel name
Policy	Choose FAILOVER or BACKUP
Description	User description for the rule

IMPORTANT: After creating new Schedule setting, click Add+ to add it. After making all required changes, click 'Save' to apply them.

L2TP V3

L2TP V3 ‘Pseudo Wire’ Configuration settings. L2TP v3 is a mechanism to connect two LANs allowing them to transparently exchange layer 2 packet data such as PPP and ATM through a packet switched network.



Already changed login password successfully.

Tunnel Setting

On	Local Tunnel ID	Remote Tunnel ID	Server Address
✓			
☑			

Add+

Session Setting

On	Index	Tunnel ID	Local Session ID	Remote Session ID	Local Address And Mask	Remote Address And Mask	Work Mode
☑							ROUTE

Add+

Save✓ Cancel✕

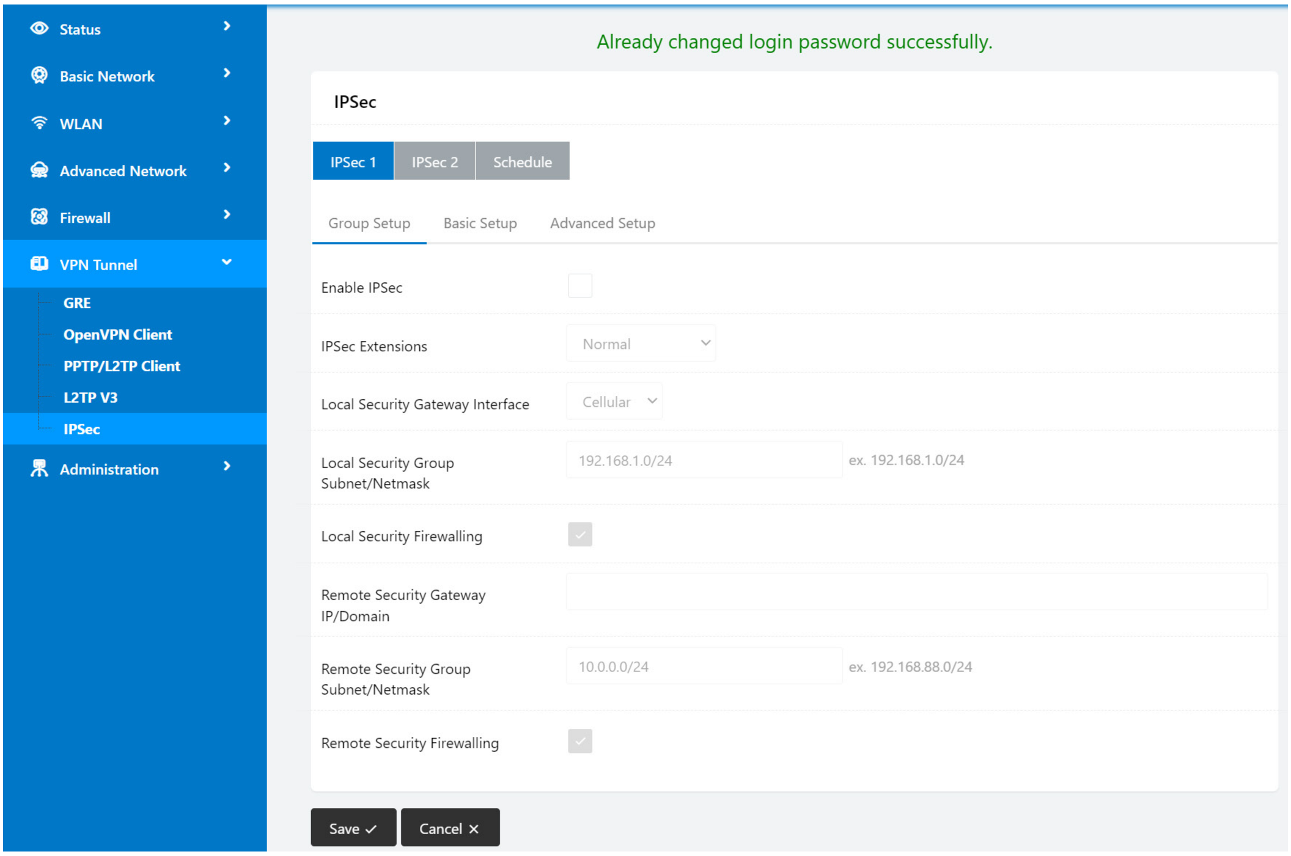
L2TP V3 Tunnel Setting	Options
On	Check to enable rule
Local Tunnel ID	User chosen number for local tunnel ID
Remote Tunnel ID	User chosen number for remote tunnel ID
Server Address	IP address or domain name of server

L2TP V3 Session Setting	Options
On	Check to enable rule
Index	User chosen number for Index
Tunnel ID	Set to required Tunnel ID
Local Session ID	User chosen number for local session ID
Remote Session ID	User chosen number for remote session ID
Local Address and Mask	IP address and mask of the local network
Remote Address and mask	IP address and mask of the remote network
Work Mode	Select Router, Gateway or Bridge

IMPORTANT: After making all required changes, click 'Save' to apply them.

IPSec

IPSec configuration settings. Configure up to two IPSec tunnels and their schedule.



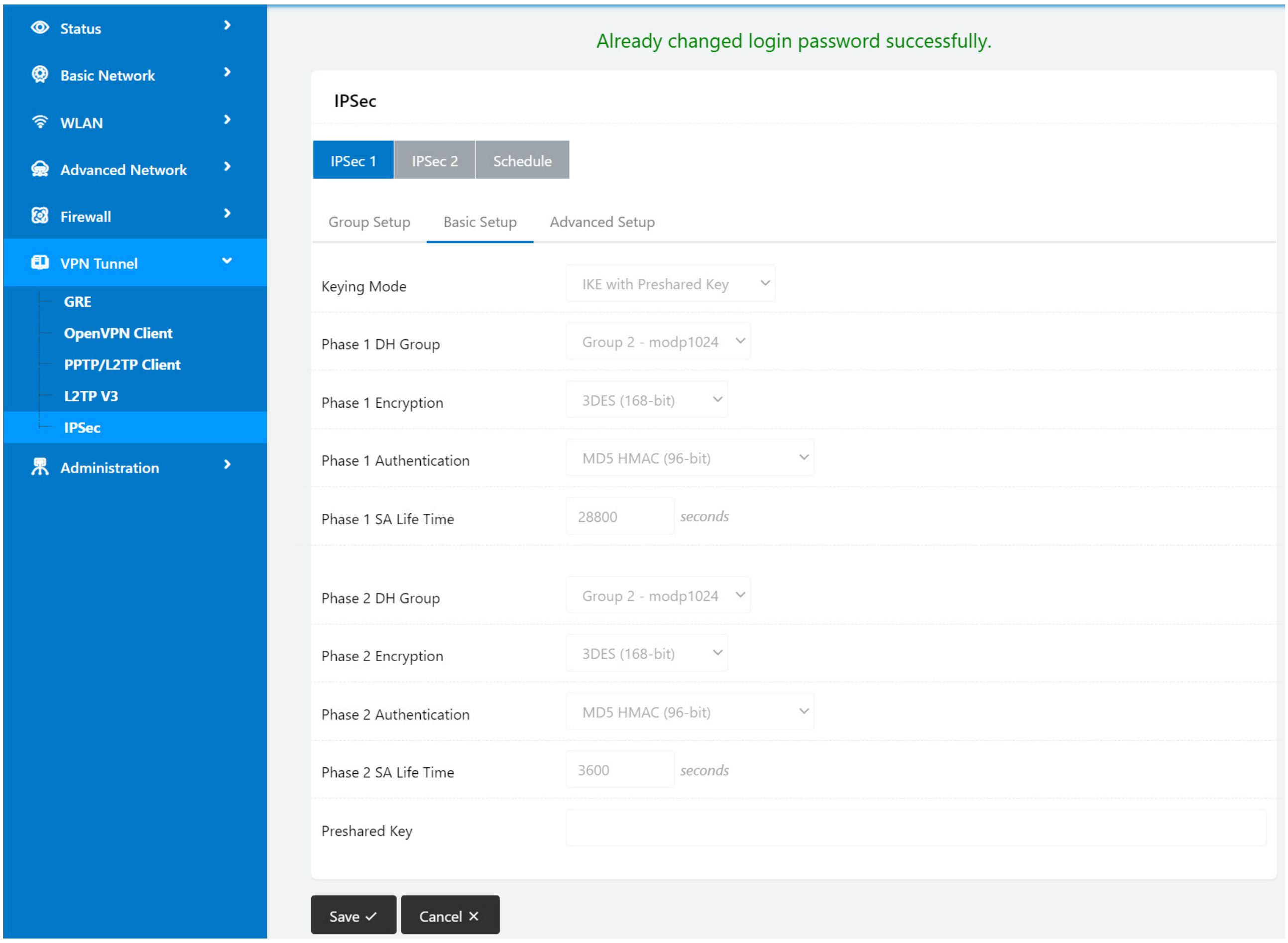
Already changed login password successfully.

IPSec

Enable IPSec	□	
IPSec Extensions	Normal	
Local Security Gateway Interface	Cellular	
Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24
Local Security Firewalling	☑	
Remote Security Gateway IP/Domain		
Remote Security Group Subnet/Netmask	10.0.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling	☑	

IPsec Group Setting	Options
Enable IPSec	Check to enable rule
IPSec Extensions	Choose Normal, GRE over IPSec or L2TP over IPSec
Local Security Gateway Interface	Choose interface to be used for IPSec VPN
Local Security Group Subnet/Netmask	Local subnet and mask for IPSec VPN
Local Security Firewalling	Check to enable local firewall
Remote Security Gateway IP/Domain	Enter IP address of IPSec VPN server WAN port
Remote Security Group Subnet/Netmask	Enter IPSec remote subnet and mask
Remote Security Firewalling	Check to enable firewalling for the remote subnet

IMPORTANT: After making all required changes, click ‘Save’ to apply them.



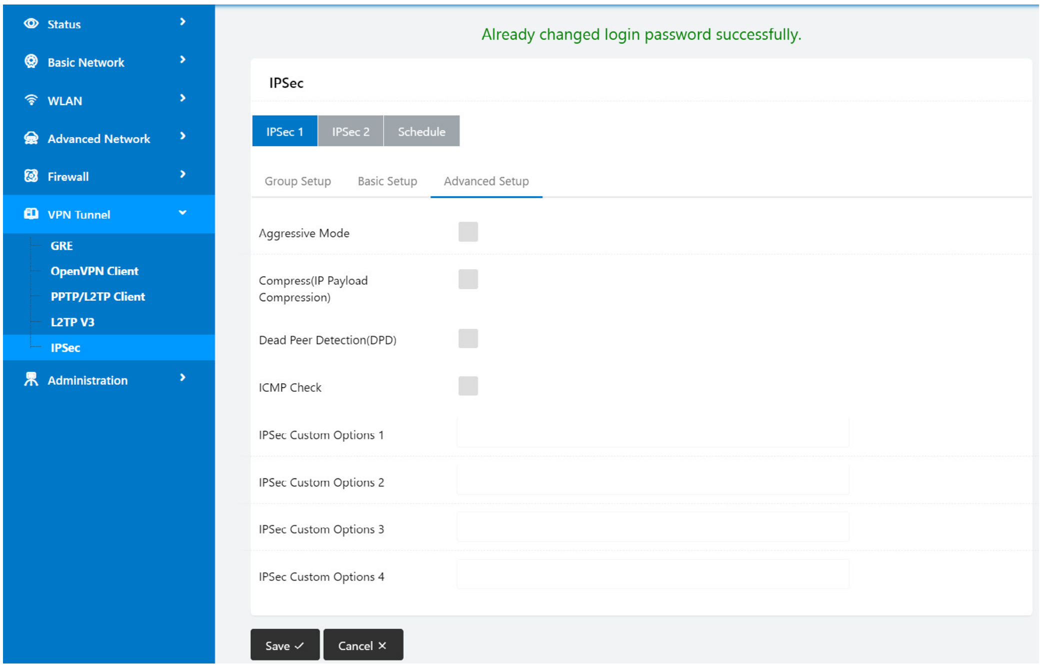
Already changed login password successfully.

IPSec

Keying Mode	IKE with Preshared Key
Phase 1 DH Group	Group 2 - modp1024
Phase 1 Encryption	3DES (168-bit)
Phase 1 Authentication	MD5 HMAC (96-bit)
Phase 1 SA Life Time	28800 seconds
Phase 2 DH Group	Group 2 - modp1024
Phase 2 Encryption	3DES (168-bit)
Phase 2 Authentication	MD5 HMAC (96-bit)
Phase 2 SA Life Time	3600 seconds
Preshared Key	

IPsec Basic Setting	Options
Keying Mode	Choose IKE with Preshared Key or IKEv2 with Preshared Key
Phase 1 DH Group	Choose Group 1 – modp768, Group 2 – modp1024 or Group 5 – modp1536
Phase 1 Encryption	Choose 3DES (168-bit), AES-128 (128-bit), AES-192 (192-bit) or AES-256 (256-bit),
Phase 1 Authentication	Choose MD5 HMAC (96-bit), SHA1 HMAC (96-bit), SHA2_256_128 HMAC (128-bit), SHA2_384_192 HMAC (192-bit) or SHA2_512_256 HMAC (256-bit),
Phase 1 SA Life Time	Enter Phase 1 SA lifetime in seconds
Phase 2 DH Group	Choose NONE, Group 1 – modp768, Group 2 – modp1024 or Group 5 – modp1536
Phase 2 Encryption	Choose 3DES (168-bit), AES-128 (128-bit), AES-192 (192-bit) or AES-256 (256-bit),
Phase 2 Authentication	Choose MD5 HMAC (96-bit), SHA1 HMAC (96-bit), SHA2_256_128 HMAC (128-bit), SHA2_384_192 HMAC (192-bit) or SHA2_512_256 HMAC (256-bit),
Phase 2 SA Life Time	Enter Phase 2 SA lifetime in seconds
Preshared Key	As required by IPSec VPN server

IMPORTANT: All values set in the IPSec VPN basic settings must match that of the IPSec VPN server. After making all required changes, click ‘Save’ to apply them.



Already changed login password successfully.

IPSec

Aggressive Mode □

Compress(IP Payload Compression) □

Dead Peer Detection(DPD) □

ICMP Check □

IPSec Custom Options 1

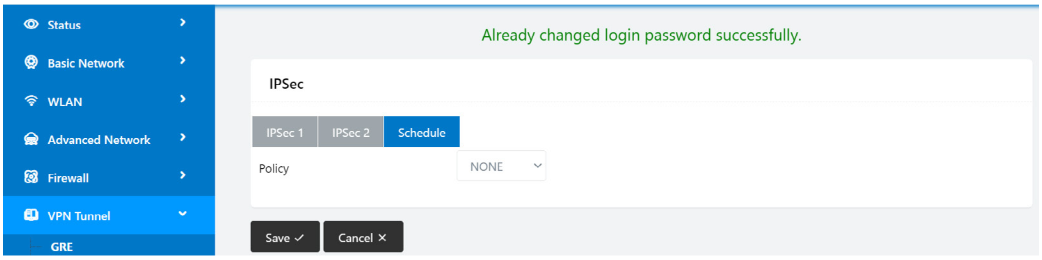
IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

IPsec Advanced Setting	Options
Aggressive Mode	Check to enable aggressive mode if required.
Compress (IP Payload Compression)	Check to enable ID payload compression if required.
Dead Peer Detection (DPD)	Check to enable dead peer detection (and then enter check period and timeout intervals)
ICMP Check	Check to enable ICMP check (and then enter IP address to be checked, check period and timeout intervals)
IPSec Custom Options 1	Enter advanced settings such as left/right ID if required
IPSec Custom Options 2	Additional custom settings
IPSec Custom Options 3	Additional custom settings
IPSec Custom Options 4	Additional custom settings

IMPORTANT: After making all required changes, click 'Save' to apply them.



Already changed login password successfully.

IPSec

Policy: NONE

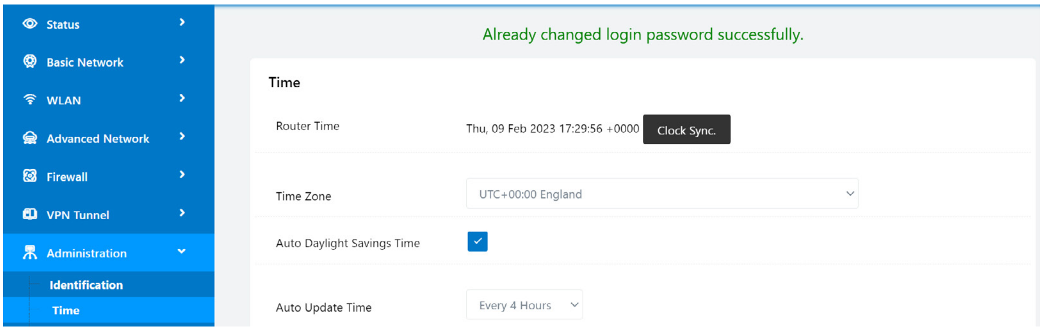
Schedule Setting	Options
Policy	Choose NONE, FAILOVER or BACKUP

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Administration

Identification

Setup the router name, hostname and domain name here.



Already changed login password successfully.

Time

Router Time: Thu, 09 Feb 2023 17:29:56 +0000

Time Zone: UTC+00:00 England

Auto Daylight Savings Time: ☑

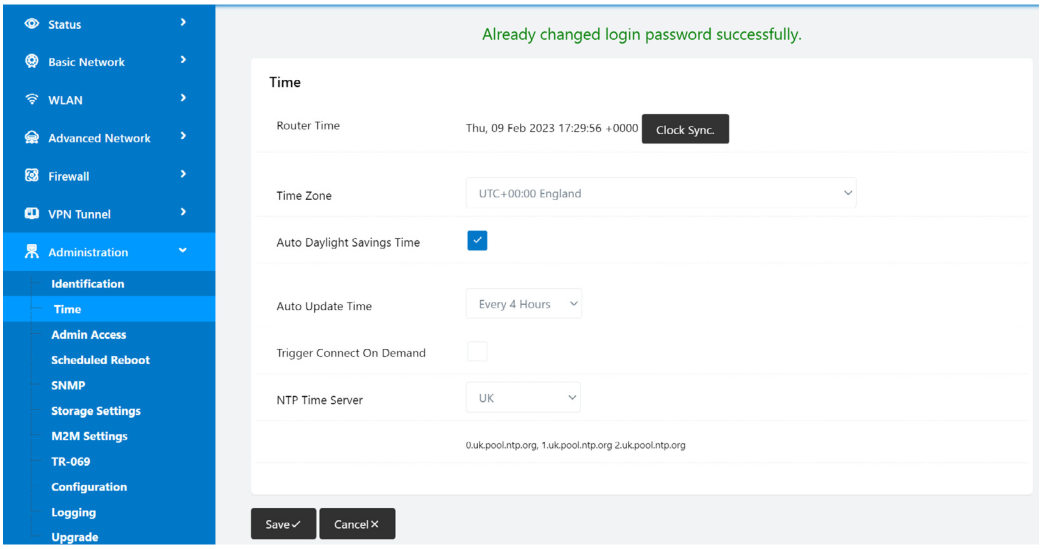
Auto Update Time: Every 4 Hours

Identification Setting	Options
Router Name	Enter an identifying name for the router
Hostname	Enter required hostname
Domain name	Enter domain name used by the WAN (if used, usually left blank)

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Time

Enter NTP details, timezone, etc here. The QUARTZ-GOLD-5G sets its time from the Internet, but is not an NTP server.



Already changed login password successfully.

Time

Router Time Thu, 09 Feb 2023 17:29:56 +0000

Time Zone UTC+00:00 England

Auto Daylight Savings Time ☑

Auto Update Time Every 4 Hours

Trigger Connect On Demand □

NTP Time Server UK

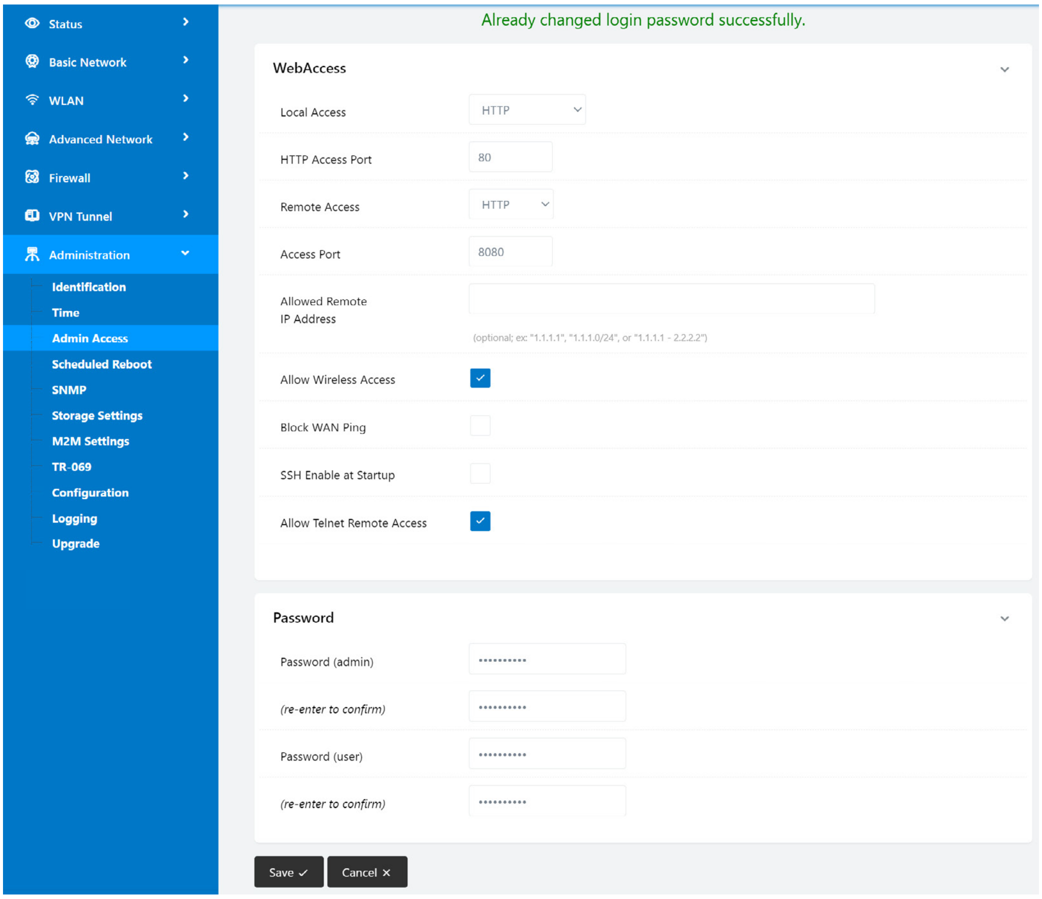
0.uk.pool.ntp.org, 1.uk.pool.ntp.org 2.uk.pool.ntp.org

Time Setting	Options
Time Zone	Set time zone from the drop down list.
Custom TZ String	Used if timezone set to Custom. Uses data format found at https://www.iana.org/time-zones which allows time zones which non-integer GMT offsets to be supported.
Auto Daylight Savings Time	Check to enable automatic application of daylight savings time
Auto Update Time	Select frequency of Internet time update from dropdown list
Trigger Connect on Demand	Enable to allow connect on demand (recommended if auto-update is set to never)
NTP Server	Choose NTP server from list or enter a custom server.

IMPORTANT: After making all required changes, click ‘Save’ to apply them. Click Clock Sync to start an immediate time update.

Admin Access

Set the allowed methods of access to the QUARTZ-GOLD-5G configuration settings here. There are two account types: ‘Admin’ which has unlimited access and ‘User’ which has read only access.



Already changed login password successfully.

WebAccess

Local Access	HTTP
HTTP Access Port	80
Remote Access	HTTP
Access Port	8080
Allowed Remote IP Address	(optional; ex: "1.1.1.1", "1.1.1.0/24", or "1.1.1.1 - 2.2.2.2")
Allow Wireless Access	☑
Block WAN Ping	□
SSH Enable at Startup	□
Allow Telnet Remote Access	☑

Password

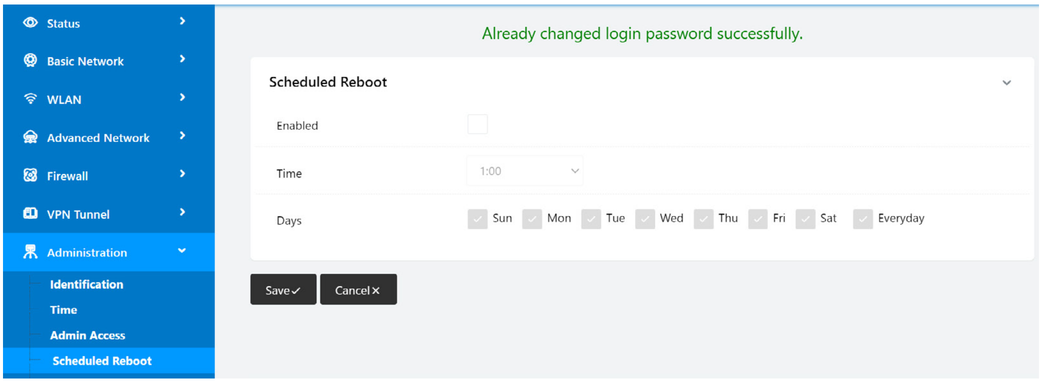
Password (admin)	••••••••••
(re-enter to confirm)	••••••••••
Password (user)	••••••••••
(re-enter to confirm)	••••••••••

Admin Access Setting	Options
Local Access	Choose Disabled, HTTP, HTTPS or HTTP & HTTPS. Warning: If Disabled is selected, access will only be possible via Telnet or SSH (if enabled!). Ensure that there is a method to access configuration, otherwise a hardware reset will be required to regain access.
HTTP Access Port	Enter HTTP access port
Remote Access	WAN access. Choose Disabled, HTTP or HTTPS
Access Port	Enter port used for remote access via WAN
Allowed Remote IP Address	Enter IP address or range of IP addresses that are allowed to remote access via WAN.
Allow Wireless Access	Check to allow admin access via WiFi
Block WAN Ping	Check to block WAN ping
SSH Enable at Startup	Check to enable SSH ate startup
Allow Telnet Remote Access	Check to allow Telnet remote access (Telnet local access always allowed)
Password (admin)	Choose and re-enter the admin password
Password (user)	Choose and re-enter the user password

IMPORTANT: After making all required changes, click 'Save' to apply them.

Scheduled Reboot

Allows the QUARTZ-GOLD-5G router to periodically reboot itself.



Already changed login password successfully.

Scheduled Reboot

Enabled □

Time 1:00

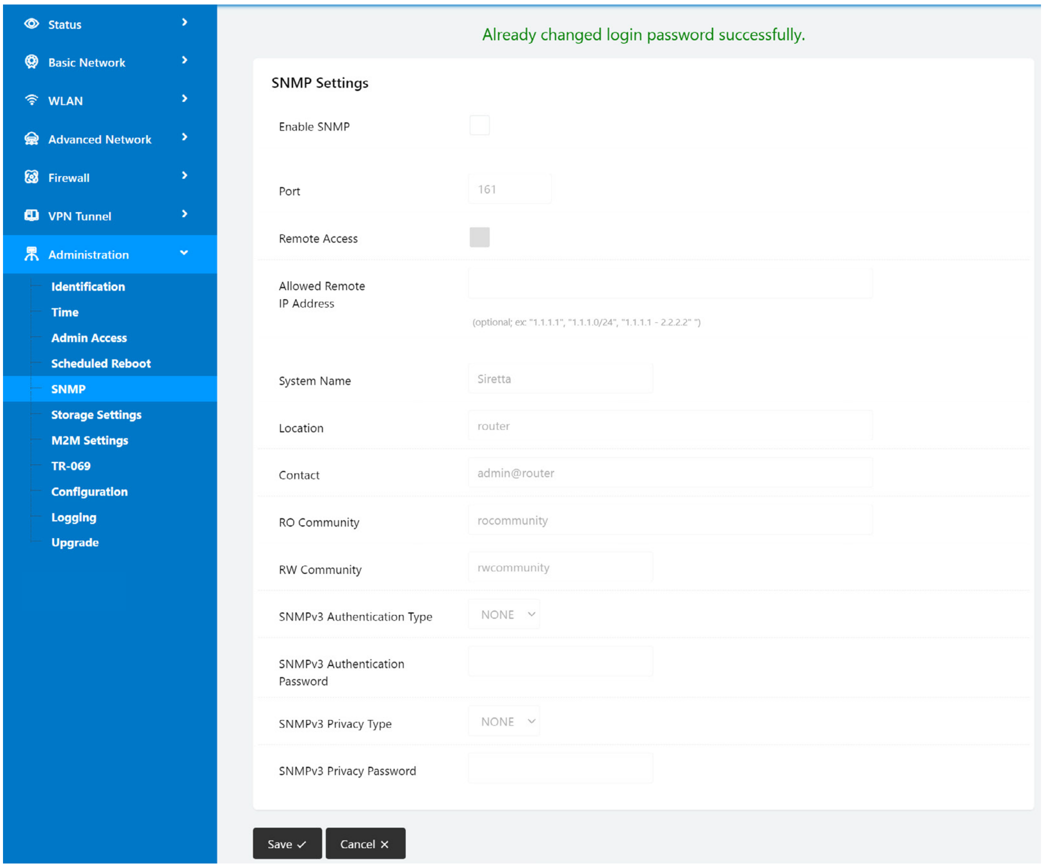
Days ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Everyday

Scheduled Reboot Setting	Options
Enabled	Check to enable rule
Time	Choose reboot time or interval from drop down list (between hourly and every 60 days)
Days	Select which days the reboot should occur on

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

SNMP

Controls SNMP settings for remote monitoring of the performance of the QUARTZ-GOLD-5G router.



Already changed login password successfully.

SNMP Settings

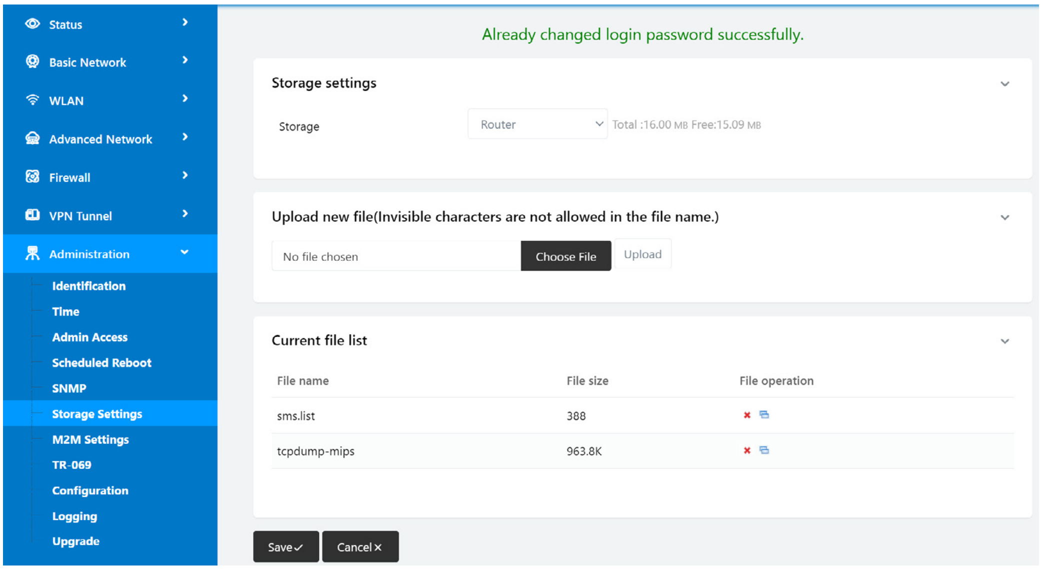
Enable SNMP	□
Port	161
Remote Access	□
Allowed Remote IP Address	(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")
System Name	Siretta
Location	router
Contact	admin@router
RO Community	rocommunity
RW Community	rwcommunity
SNMPv3 Authentication Type	NONE
SNMPv3 Authentication Password	
SNMPv3 Privacy Type	NONE
SNMPv3 Privacy Password	

SNMP Setting	Options
Enable SNMP	Check to enable SNMP
Port	Enter port
Remote Access	Check to enable remote access
Allowed Remote IP address	Whitelist of IP addresses allowed to access if emote access is enabled
System Name	Enter a name for the router
Location	Enter the location of the router
Contact	Enter a contact email address
RO Community	Enter Read Only community password used for SNMP access
RW Community	Enter Read/Write community password used for SNMP access
SNMPv3 Authentication Password	Enter password used for SNMPv3 authentication
SNMPv3 Authentication Type	Choose NONE, MD5 or SHA
SNMPv3 Privacy Password	Enter password used for SNMPv3 Privacy
SNMPv3 Privacy Type	Choose NONE, DES or AES

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Storage Settings

Settings for the local file storage, and the capability to upload and download files. Files for the Captive Portal are stored here. Received SMS messages received by the router are appended to the file sms.list (which is created if it doesn't exist in router storage).



Already changed login password successfully.

Storage settings

Storage: Router — Total :16.00 MB Free:15.09 MB

Upload new file(Invisible characters are not allowed in the file name.)

No file chosen

Current file list

File name	File size	File operation
sms.list	388	✕ ⧉
tcpdump-mips	963.8K	✕ ⧉

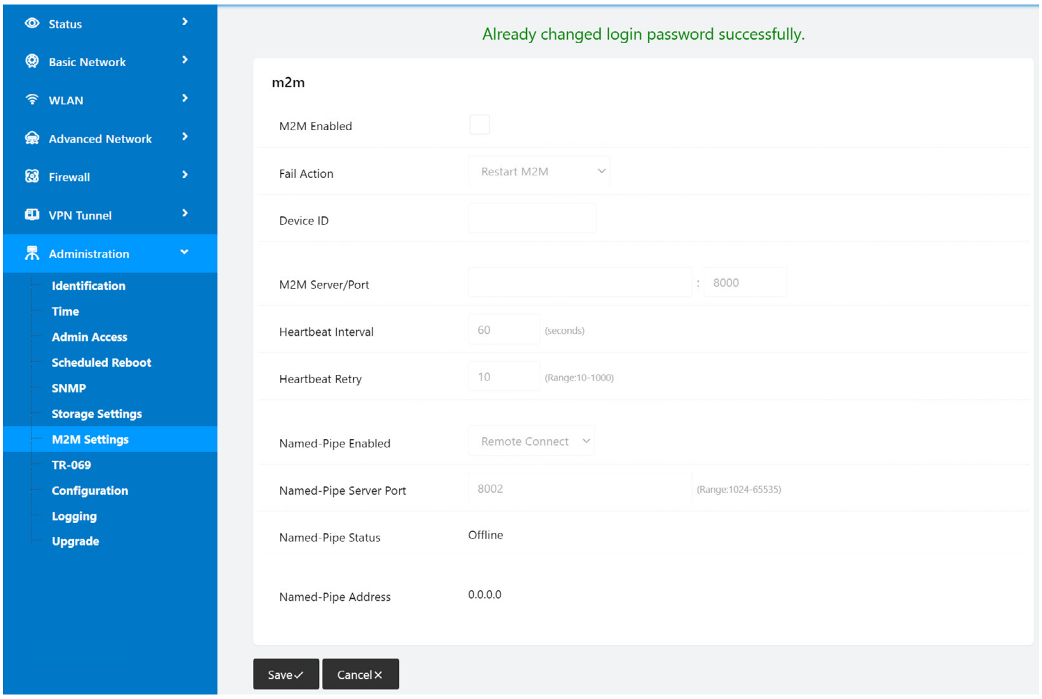
Storage Setting	Options
Storage	Select the file system to view. Always set to Router as the QUARTZ-GOLD-5G has no external storage options.
Upload new file	Choose a file and click the upload button to upload it. File names must never include spaces.
Current File List	List of files stored on the QUARTZ-GOLD-5G. Click the icons to the right of the file names to download or delete them.

IMPORTANT: After making all required changes, click 'Save' to apply them.

M2M Settings

Siretta offer a M2M portal (https://quartz.siretta.com) to allow users to view and manage many routers from a cloud-based portal. Configure the settings to connect the QUARTZ-GOLD-5G to this portal here.

Note: Contact Siretta support for portal account creation.



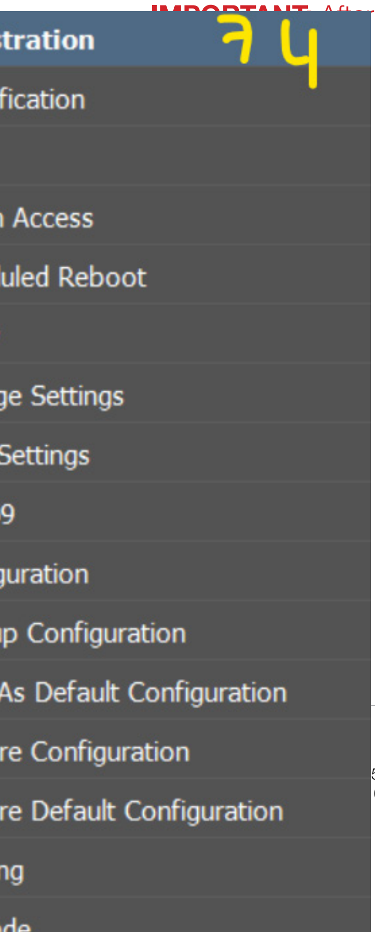
Already changed login password successfully.

m2m

M2M Enabled	□
Fail Action	Restart M2M
Device ID	
M2M Server/Port	: 8000
Heartbeat Interval	60 (seconds)
Heartbeat Retry	10 (Range:10-1000)
Named-Pipe Enabled	Remote Connect
Named-Pipe Server Port	8002 (Range:1024-65535)
Named-Pipe Status	Offline
Named-Pipe Address	0.0.0.0

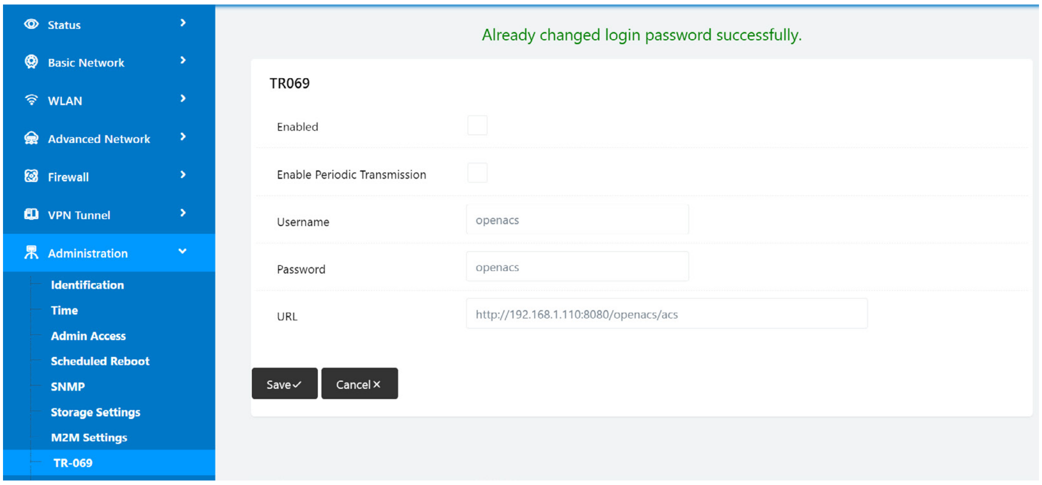
M2M Setting	Options
M2M Enabled	Check to enable M2M
Fail action	Select action for router to take if it cannot access the M2M server: Restart M2M, Reconnect to Network or Reboot System
Device ID	Name supplied by Siretta support to identify router to M2M portal
M2M Server/Port	Enter router.siretta.com:8000 for Siretta M2M portal
Heartbeat Interval	Time period between router connections to portal. Note: every connection will use data, so do not use a frequent heartbeat interval unless necessary
Heartbeat Retry	Number of heatbeat retry attempts before the fail action is implemented
Named-Pipe Enabled	Choose Remote Connect for Siretta M2M portal
Named-Pipe Server Port	Chose 8002 for Siretta M2M portal
Named-Pipe Status	Reported status, online/offline (output field)
Named-Pipe Address	Address of named Pipe.

IMPORTANT: After making all required changes, click ‘Save’ to apply them.



TR-069

Configure TR-069 client for remote management settings here.



Already changed login password successfully.

TR069

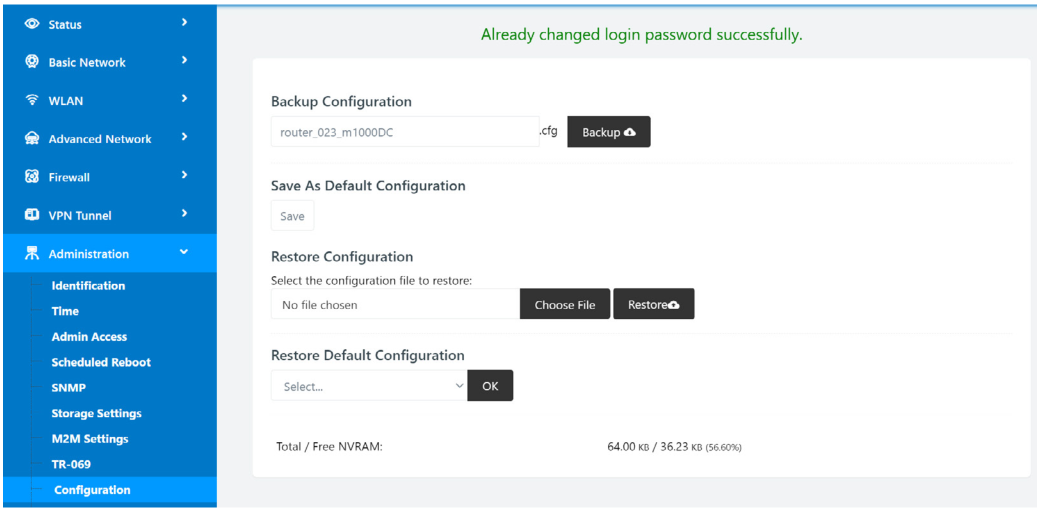
Enabled	□
Enable Periodic Transmission	□
Username	openacs
Password	openacs
URL	http://192.168.1.110:8080/openacs/acs

TR-069 Setting	Options
Enabled	Check to enable TR-069
Enable Periodic Transmission	Check to enable periodic transmission
Username	Username as required for server
Password	Password as required for server
URL	URL and port of server

IMPORTANT: After making all required changes, click ‘Save’ to apply them.

Configuration

Backup and restore configurations here.



Already changed login password successfully.

Backup Configuration
router_023_m1000DC .cfg Backup

Save As Default Configuration
Save

Restore Configuration
Select the configuration file to restore:
No file chosen Choose File Restore

Restore Default Configuration
Select... OK

Total / Free NVRAM: 64.00 KB / 36.23 KB (56.60%)

Backup Configuration

Enter a file name for the backup file and click the ‘backup’ button to download a .cfg file containing the routers configuration.

Save As Default Configuration

Click the ‘Save’ button to save the current configuration into the routers NVRAM as the users default configuration. This is different from the factory default configuration. This is useful if configurations are being experimented with to allow for easy return to this configuration.

Restore Configuration

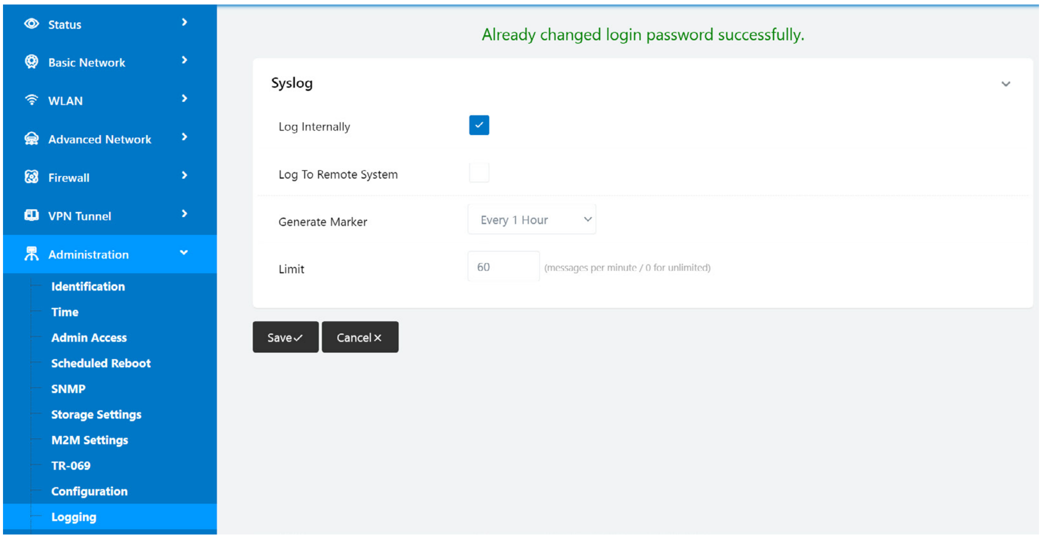
Click ‘Choose File to navigate to and select a .cfg file containing the configuration to be restored, then click ‘Restore’ to restore the routers settings to those in the backup file.

Restore Default Configuration

Select ‘Restore Custom Configuration’ to choose the configuration chosen as the default configuration (above) or ‘Restore Factory Configuration’ to select factory settings, and then click ‘OK’ to restore these settings. It is also possible to restore either configuration by using the reset button (see factory reset section at the end of this manual).

Logging

Status messages for debugging purposes can be logged by the QUARTZ-GOLD-5G, either internally or to an external syslog recorder. The logs can be accessed via the Tools > logs menu at the top of the routers home page.



Already changed login password successfully.

Syslog

Log Internally ☑

Log To Remote System □

Generate Marker: Every 1 Hour

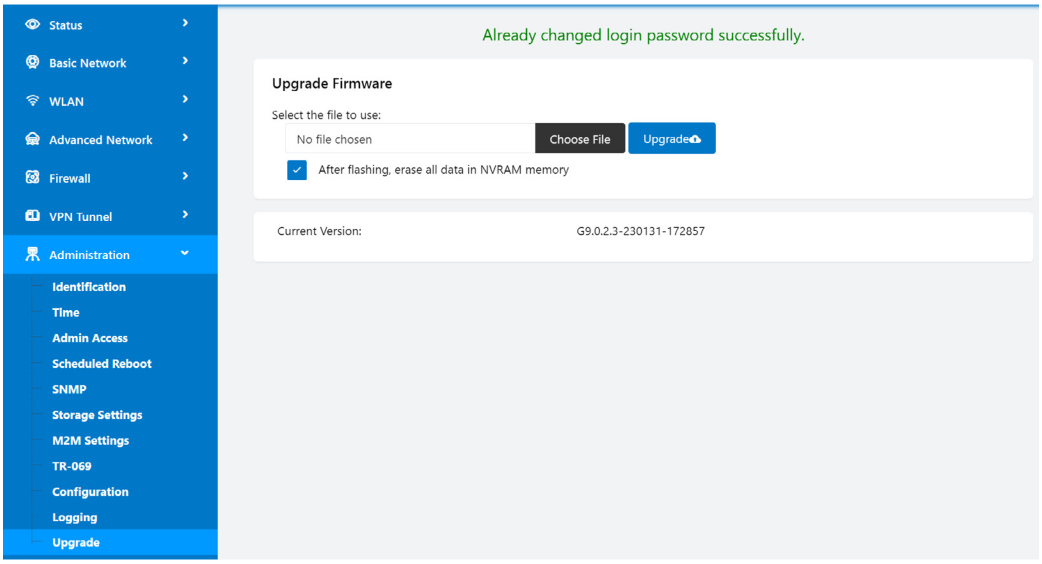
Limit: 60 (messages per minute / 0 for unlimited)

Storage Setting	Options
Log Internally	Check to enable internal logging
Log to remote System	Check to enable external logging (and then enter target IP address and port)
Generate Marker	Choose marker insertion rate from dropdown menu
Limit	Enter a limit to the number of messages/minute logged.

IMPORTANT: After making all required changes, click 'Save' to apply them.

Upgrade

Firmware used in the QUARTZ-GOLD-5G may be updated here. Siretta may periodically make updates available which fix any bugs discovered and/or add new features.



Already changed login password successfully.

Upgrade Firmware

Select the file to use: No file chosen

☑ After flashing, erase all data in NVRAM memory

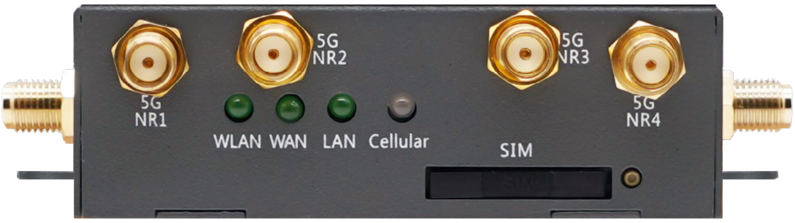
Current Version: G9.0.2.3-230131-172857

Press ‘Choose file’ to navigate to and select the new firmware image to be applied to the router. Before clicking the blue ‘upgrade’ button, consider carefully if the configuration settings currently in the router should be preserved. By default, the ‘After flashing, erase all data in NVRAM memory’ option is checked – it may be desirable to uncheck this.

It is always a good idea to backup the configuration before doing a firmware update (Administration > Configuration, Backup Configuration).

The Current Version shows the full firmware detail which is the version with date and time stamp.

Status LEDs



The status LEDS indicate activity on the QUARTZ-GOLD-5G interfaces. Note that while the LEDs may illuminate on or shortly after application of power, the status indication is not valid until approximately 60 seconds after the application of power.

Table 23. Router status LEDs

Label	Indication		Meaning
WLAN	Green	Solid Blinking activity Off	WLAN connected WLAN connected, LAN network activity WLAN disconnected
WAN	Green	Solid Blinking activity Off	WAN connected WAN connected, WAN network activity WAN disconncted
LAN	Green	Solid Blinking activity Off	LAN connected LAN connected, LAN network activity LAN disconnected
Cellular	Green (good cellular signal) Red (poor cellular signal)	Slow blink Fast blink Solid	Registering to cellular network / Cellular disabled / No SIM inserted Connected to cellular network, obtaining IP address Connected to cellular network & connected to Internet

IMPORTANT: On first power up, it may take 4-5 minutes for the QUARTZ-GOLD-5G to connect to the cellular network and for the cellular status LED to remain lit. On subsequent power-ups it should take considerably less time to connect to the cellular network. If the cellular status LED does not light continuously, check that the SIM card is inserted correctly, that the SIM is enabled by the network operator, that the correct APN and password settings have been entered (see QUARTZ-GOLD-5G software manual), and that the antennas have been correctly attached.

Reset

The QUARTZ-GOLD-5G can be returned to default settings by pressing and holding down the recessed reset switch while the router is powered.

Three forms of reset are possible depending on how long the reset switch is pressed for until released:

1.	>2 seconds	Router reboot with current settings
2.	>10 seconds	Router reboot with custom reset configuration loaded
3.	>30 seconds	Router reboot with factory default configuration loaded

Note: Rebooting with factory default configuration also sets the custom reset configuration back to default.

The custom reset configuration is set up in the software interface. This is a useful mode of operation to return to known working settings rather than full factory reset if the configuration settings are being experimented with.

Copyright Information

Copyright Declaration

Trademarks

Windows and Microsoft are registered trademarks of Microsoft Corporation. Siretta Ltd is an independent business and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation.

Google Maps is a trademark of Google LLC. Siretta Ltd is not endorsed by or affiliated with Google in any way.

Wireshark is a registered trademark of the Wireshark Foundation, Inc.

All other trademarks are the property of their respective owners.

Disclaimer

The information contained in this document is proprietary to Siretta Ltd. Siretta Ltd has made every effort to ensure that the information contained within this document is accurate. Siretta Ltd does not make any warranty as to the information contained within this document and does not accept any liability for any injury, loss or damage of any kind incurred using this information.

Siretta does not take responsibility for any application developed using the product characterized in this document and notes that any application implemented with this product must comply with the safety standards of the applicable country and comply with the relevant wiring rules. Siretta reserves the right to make modifications, additions, and deletions to this document due to typographical errors, inaccurate information, or improvements to equipment at any time and without notice. Such changes will be incorporated into new editions of this document.

Please refer to the Siretta Ltd website for the latest version of this document.

Approvals

- **CE** - European Conformity
- **UKCA** - UK Conformity Assessed
- **RoHS** - Restriction of the Use of Certain Hazardous Substances Compliant
- **FCC** - (TBC)

Definitions

Term	Definition
3G	3rd Generation Mobile Telecommunications
4G	4th Generation Mobile Telecommunications
5G	5th Generation Mobile Telecommunications
ADSL	Asymmetric Digital Subscriber Line
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
FDD	Frequency Division Duplex
GbE	Gigabit Ethernet
GPS	Global Positioning System
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LTE	Long-Term Evolution
MDI	Medium Dependent Interface
MIMO	Multiple-input and Multiple-output
RHCP	Right-handed Circular Polarization
RXD	Recieve Data
SIM	Subscriber Identity Module
SMS	Short Message Service
TDD	Time Division Duplex
TXD	Transmit Data
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
VSWR	Voltage Standing Wave Ratio
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Siretta

Enabling Industrial IoT

sales +44 (0)118 976 9000
email sales@siretta.com

www.siretta.com

Siretta Ltd
Basingstoke Road
Spencers Wood
Reading
Berkshire
RG7 1PW
United Kingdom

Company No. 08405712
VAT Registration No. GB163 04 0349

Rev 1.0 - May 2023