



Enabling Industrial IoT

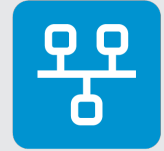


## QUARTZ-GOLD

Gigabit Ethernet Industrial Router Range

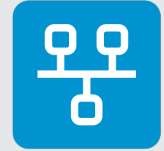
Software Manual

Rev 1.2



# Table of Contents

	Page
<b>Introduction</b>	<b>3</b>
<b>About Siretta</b>	<b>4</b>
<b>Configuration</b>	<b>5</b>
Router Setup	5
Connecting to the QUARTZ-GOLD Router	5
<b>Web Interface</b>	<b>7</b>
Important System Messages	8
Measuring and Debugging	9
Status	17
Basic Network	19
WLAN	34
Advanced Network	39
Firewall	58
VPN Tunnel	61
Administration	75
<b>Copyright Information</b>	<b>88</b>
Copyright Declaration	88
Trademarks	88
<b>Disclaimer</b>	<b>89</b>
<b>Definitions</b>	<b>90</b>



## Introduction

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

The reader of this hardware manual is expected to be educated to the level of at least a networking technician to understand its contents.

This document covers all the software features and configuration aspects of the QUARTZ-GOLD router. For physical installation of this product into a computer network, please refer to the '[QUARTZ-GOLD - Hardware Manual](#)'.

## About Siretta

Siretta is a wireless communications company located in Reading, United Kingdom manufacturing & supplying industrial IoT products since the early 2000s.

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 150 MHz to 6 GHz. These encompass modems, routers and antennas for:

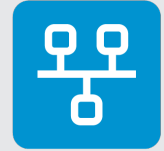
- » Cellular technologies: GSM/GPRS/3G/UMTS/4G/LTE & 5G NR, plus LTE CAT 1, LTE CAT M & LTE CAT NB-IoT
- » Global positioning: GPS/GNSS
- » WLAN/Wi-Fi

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.



# Configuration

## Router Setup

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

## Connecting to the QUARTZ-GOLD Router

To configure the QUARTZ-GOLD, you must first access the webserver integrated into the router. You may do this either with a directly wired Ethernet connection to the router (using either LAN port) or by WiFi. When connecting to the QUARTZ-GOLD for the first time, your computer will be assigned an IP address from the routers built in DHCP server.

If connecting to the router by LAN, please turn off your computers WiFi, and make sure that the PC is connected to the QUARTZ-GOLD and no other network device.

If connecting to the router via WiFi, please look for and connect to the WiFi network broadcasting an SSID of "Router-Wifi\_<nnnnnn>". <nnnnnn> is 6 digit hexadecimal number being the last 6 digits of the WiFi's MAC address. This will be the 2.4GHz WiFi. The 5GHz WiFi has "\_5G" appended to the SSID name (and will have a MAC address differing by 1 count). The WiFi is open and has no password set. Ensure that any wired Ethernet connections are unplugged from your PC.

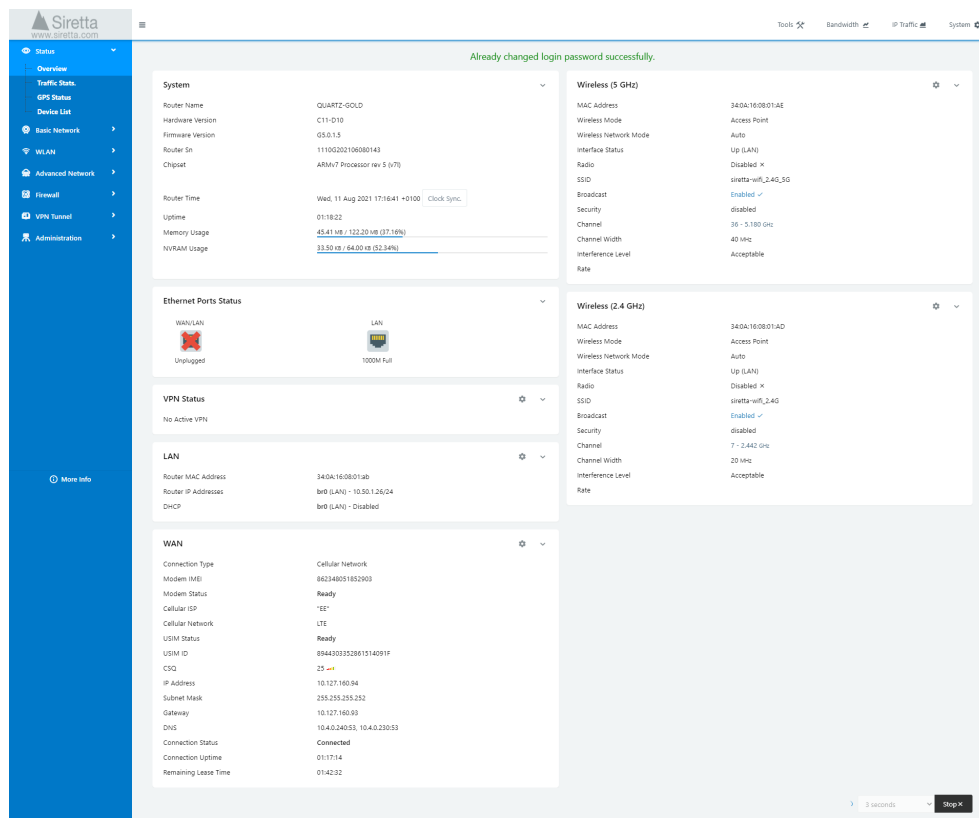
By following the above instructions, you will ensure that your PC is only networked with the QUARTZ-GOLD and will therefore obtain an IP address from the QUARTZ-GOLD's internal DHCP server. You may now connect to the internal web server using a web browser and browsing the QUARTZ-GOLDs gateway address.

The settings that you will require are:

- » **Gateway Address:** 192.168.1.1
- » **Username:** admin
- » **Password:** admin

Once connected, you will see the 'Status > Overview' page of the routers webserver, as shown over page.

Figure 1. 'Status > Overview' page of the routers webserver



### Important Warning

When first connecting to the QUARTZ-GOLD, all settings will be at factory default. This is so you can easily access the router for configuration, but this also means that anyone else could as well.

To prevent the QUARTZ-GOLD and your network from being compromised, it is recommended that you immediately do the following:

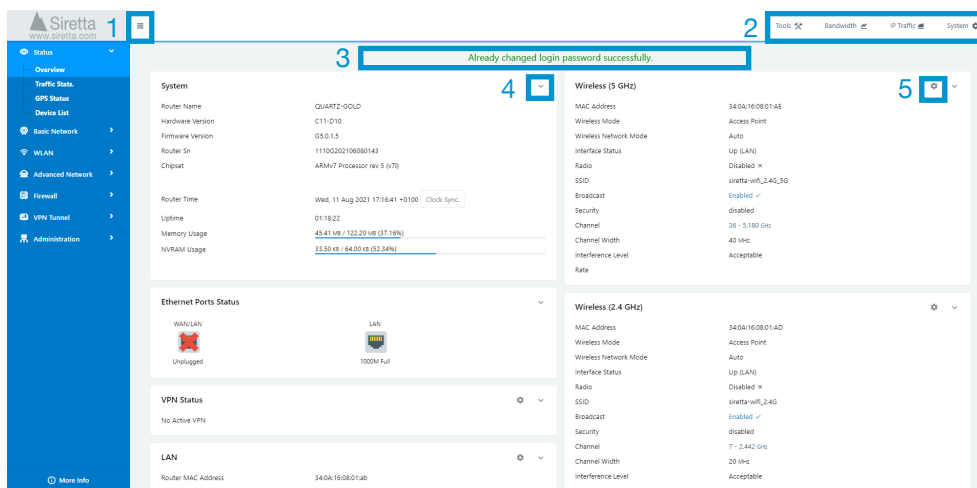
1. Change the login username/password. This can be done by accessing the 'Administration > Admin Access' page (that is also accessible from the password warning at the top of the page)
2. Either enable Security on the WiFi and set a password, or disable the WiFi if not being used. The 2.4GHz and 5GHz WiFi channels work independently, so they independently need to be configured. This can be done by accessing the 'WLAN > Basic Settings' page.

## Web Interface

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 configuration and operational status.

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

Figure 2. Web interface navigation



- 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 remind you to change the admin password:

Figure 3. System message - change 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' the above message will be displayed. Once the password has been changed, and no router reboots are required, the message will change.

Figure 4. System message - password changed

Already changed login password successfully.

When the QUARTZ-GOLD needs to be rebooted after a configuration change it will display the following system message:

Figure 5. System message - password changed

The settings changed, some settings will take effect after the router reboots. [Reboot Now](#)



## Measurement and Debugging

### Tools

Clicking the 'Tools' icon will offer several tools.

Figure 6. Measurement and debugging tool selection



### 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.

Figure 7. Ping

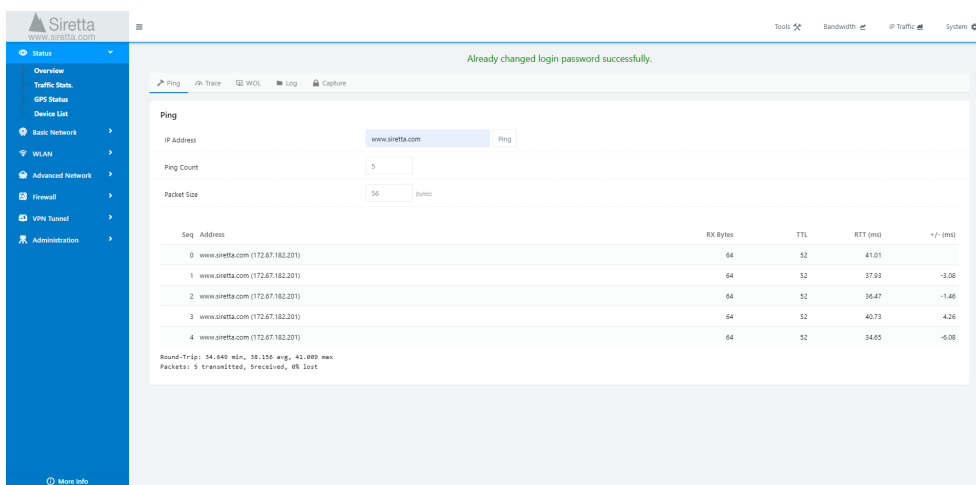


Table 1. Ping test tool

Tool	Description
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 hide the IP address.
RX Bytes	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	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).
RTT	Round Trip Time (to the destinate address and back again).
+ / -	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.

Figure 8. Trace

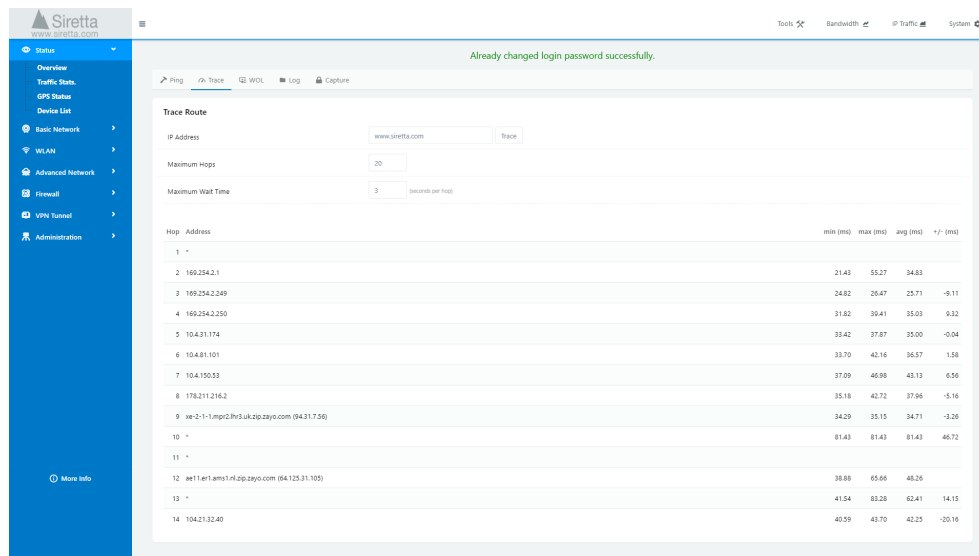


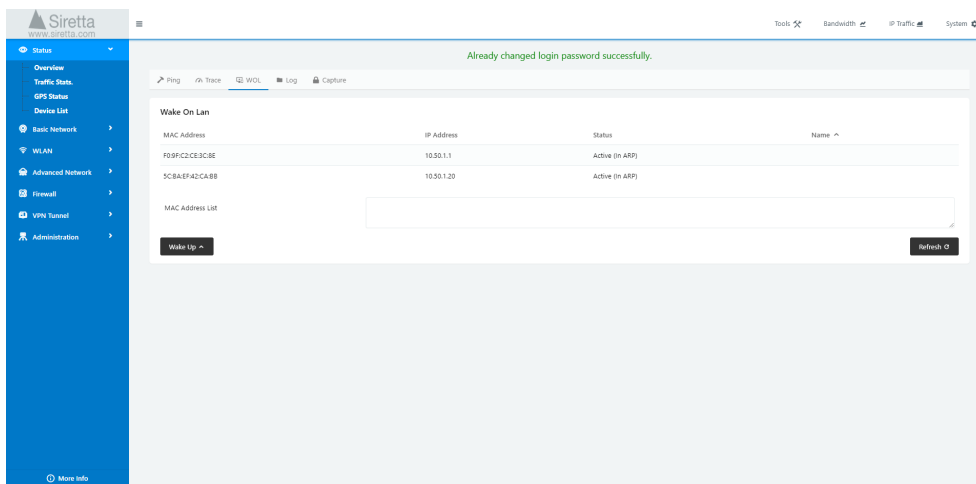
Table 2. Trace tool

Tool	Description
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 will respond, and these will be indicated by a '*'.

### WOL

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

Figure 9. Wake on LAN



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.

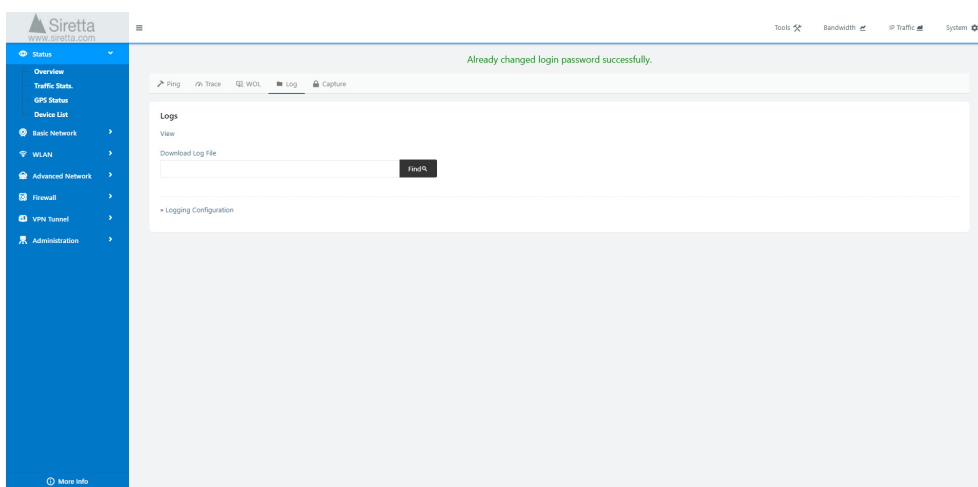
You may also enter one or more MAC addresses in the MAC Address List field. Separate multiple MAC addresses with a space or new line. Click 'Wake Up' to send the Magic Packet to all MAC addresses in the list. If your list is large, you can re-size the field by dragging the marker in the bottom right 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, you need to plan ahead. The ARP list is only refreshed when you browse to the page or hit the refresh button. Use the ARP list to identify the MAC addresses of the devices that you want to control 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.

Figure 10. Logs



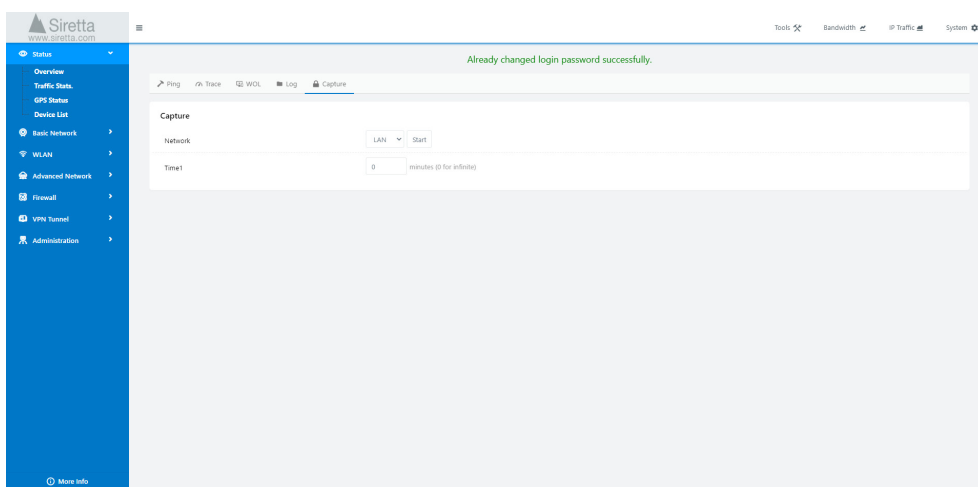
Click 'View' to open the log as a web page, or 'Download Log File' to download the log as a syslog.txt file.

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.

### 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.

Figure 11. Capture

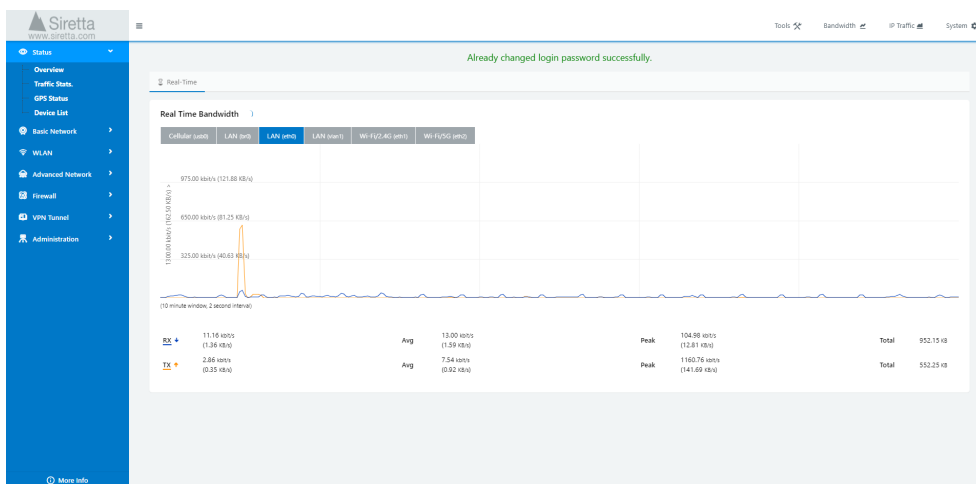


Select either LAN or WAN from the dropdown menu to choose the interface whose traffic will be captured, and the log duration and the click 'Start'. The .pcap file created, downloaded and added to for the time requested, or until 'Stop' is clicked.

### Bandwidth

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

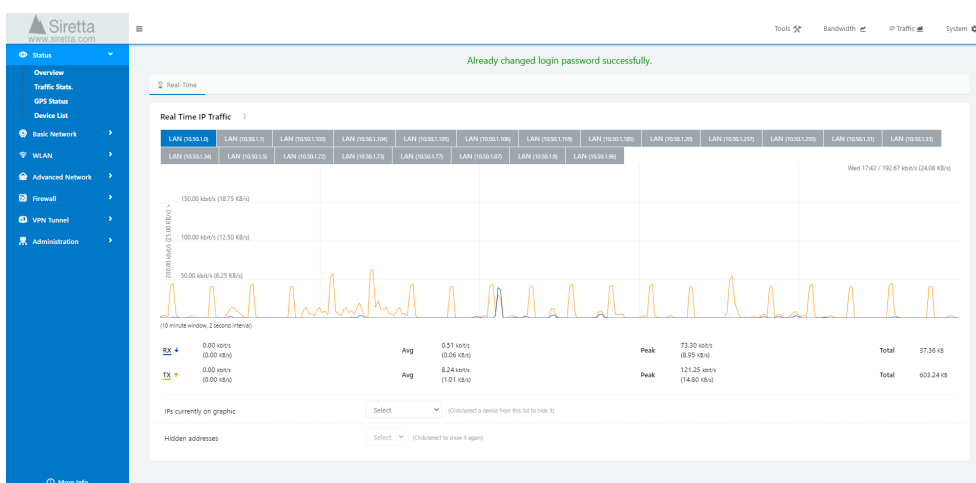
Figure 12. Measurement and debugging bandwidth selection



### IP Traffic

This reports the traffic by IP address in the QUARTZ-GOLD. This is shown both graphically and numerically.

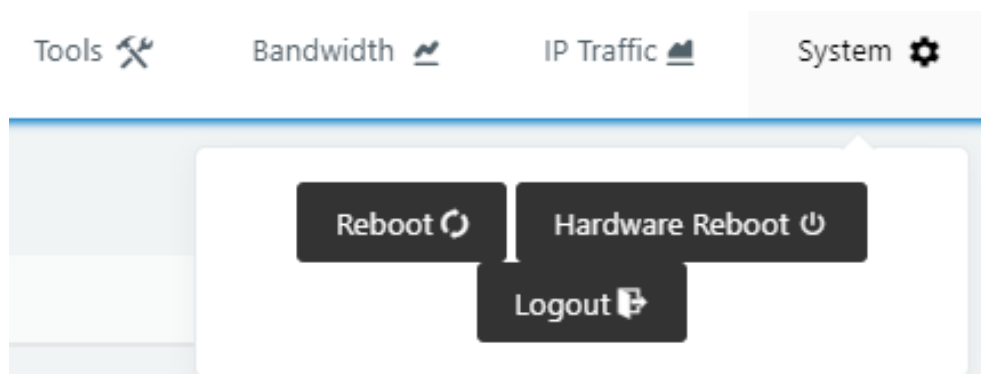
Figure 14. Measurement and debugging IP traffic selection



### System

The system menu allows for software reboot, hardware reboot and logging out from the QUARTZ-GOLD.

Figure 13. Measurement and debugging system selection



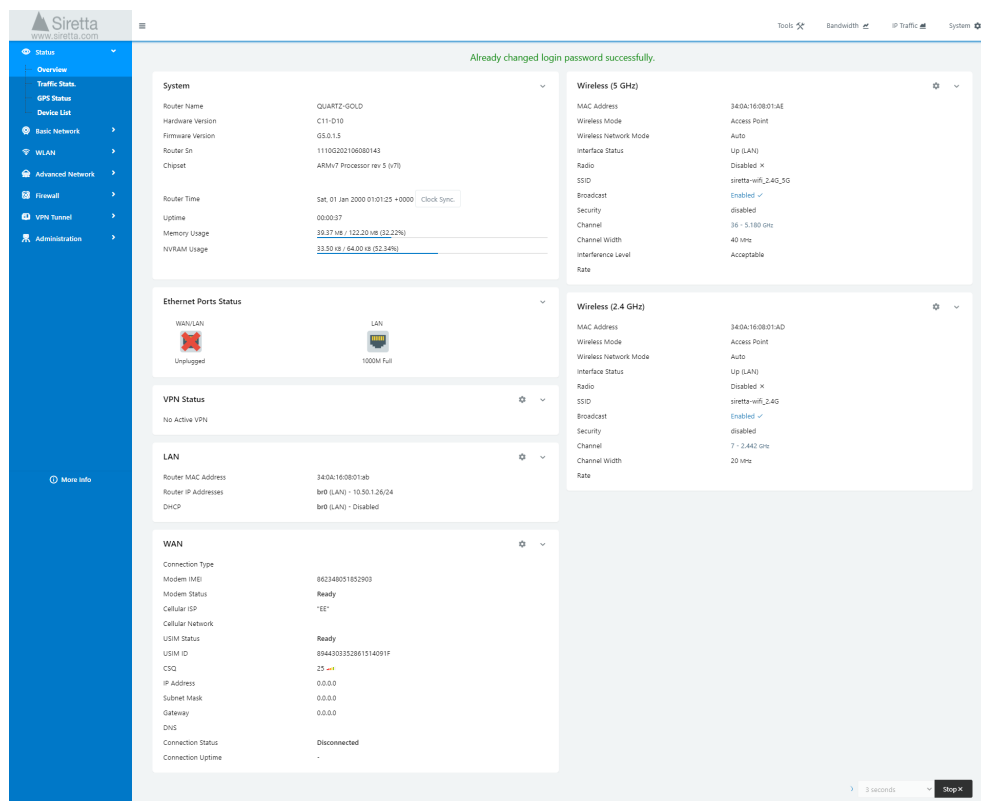


## Status

### Overview

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

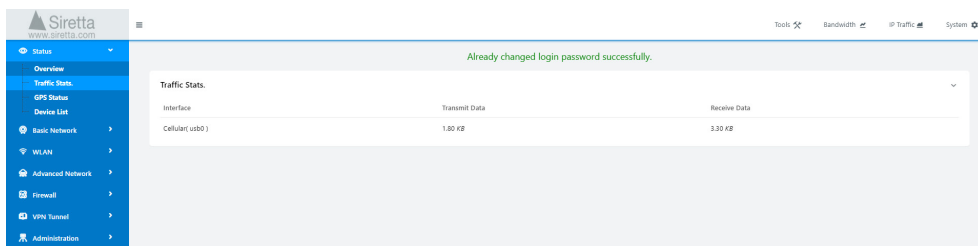
Figure 15. Overview



### Traffic Stats.

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

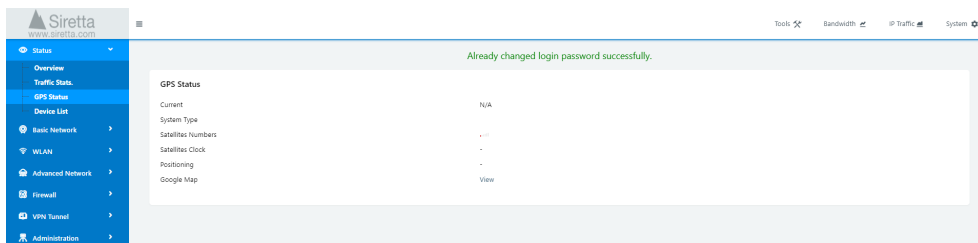
Figure 16. Traffic Stats



### GPS Status

If enabled (in 'Advanced Network > GPS') and if fitted with the GPS option, this will show the status of the GPS.

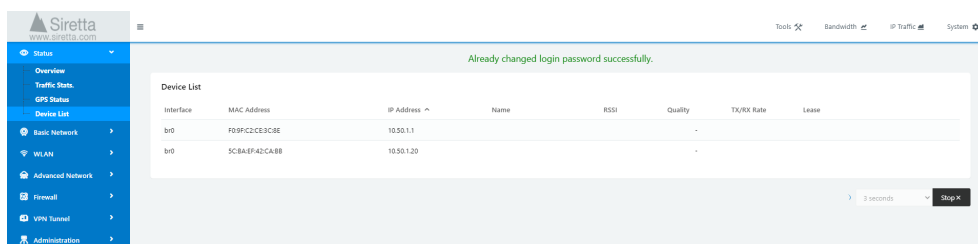
Figure 17. GPS Status



### Device List

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

Figure 18. Device List



## Basic Network

### WAN

This defines how the WAN port works. If WAN is disabled, the port will work as a LAN port.

Figure 19. WAN

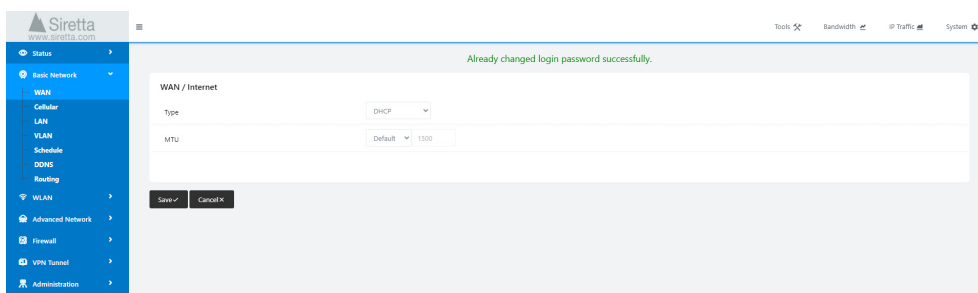


Table 3. WAN settings

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

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

### Cellular

The cellular settings allow the LTE modem to be enabled/disabled, as it contains the settings necessary for the LTE modem to be configured correctly for the cellular network used.

Figure 20. Cellular

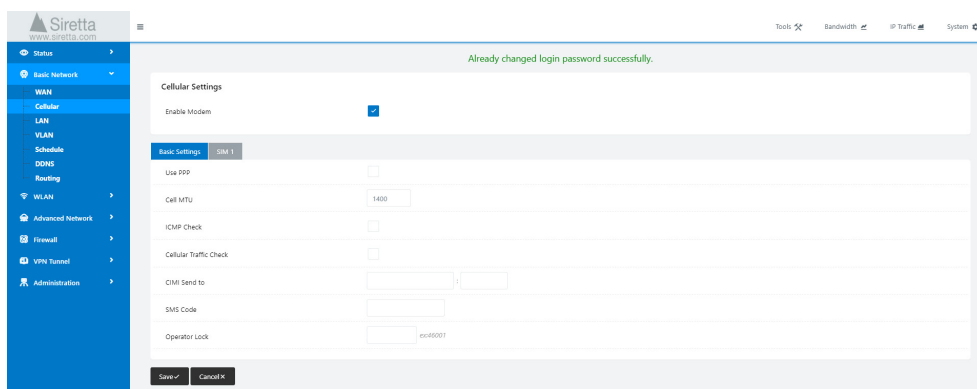


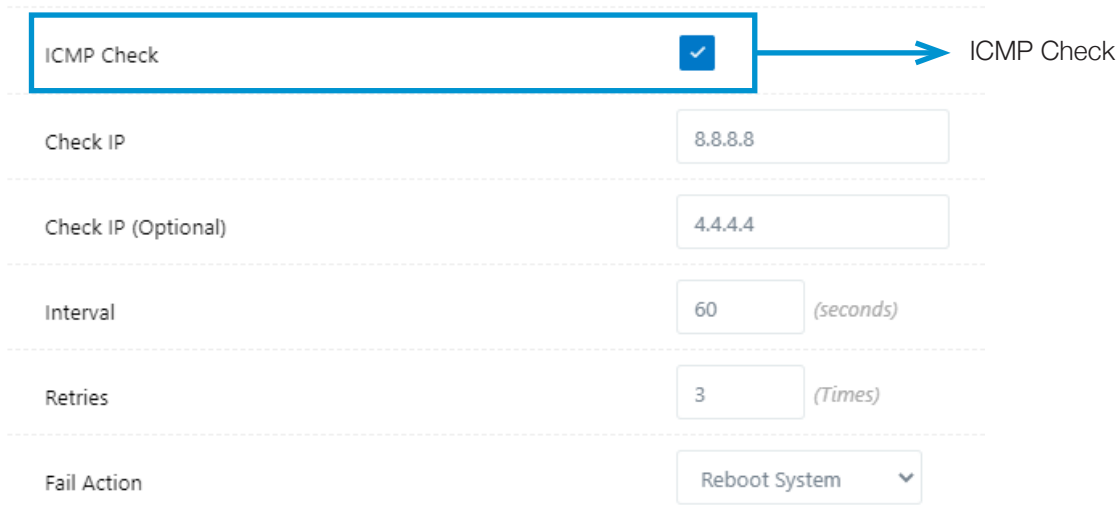
Table 4. Cellular settings

Setting	Options
Enable Modem	Enable / Disable LTE modem
Use PPP	ECM dialup used as default. PPP may be enabled if required
Cell MTU	Entered desired MTU size for the cellular interface
ICMP Check	When enabled, attempts to send an ICMP ping to a user specified address to check for connectivity. If the test fails, the router may be rebooted or cellular reconnect attempted. See below.
Cellular Traffic Check	Router checks for Tx/Rx data transmission. If the test fails, the router may be rebooted or cellular reconnect attempted. See below
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

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.

Figure 21. ICMP Check



The figure shows a configuration form for the ICMP Check feature. At the top, there is a toggle switch labeled 'ICMP Check' which is currently turned on (indicated by a blue checkmark). An arrow points from this toggle to the text 'ICMP Check'. Below the toggle, there are five rows of configuration options:

- Check IP:** A text input field containing '8.8.8.8'.
- Check IP (Optional):** A text input field containing '4.4.4.4'.
- Interval:** A text input field containing '60' followed by '(seconds)'.
- Retries:** A text input field containing '3' followed by '(Times)'.
- Fail Action:** A dropdown menu with 'Reboot System' selected.

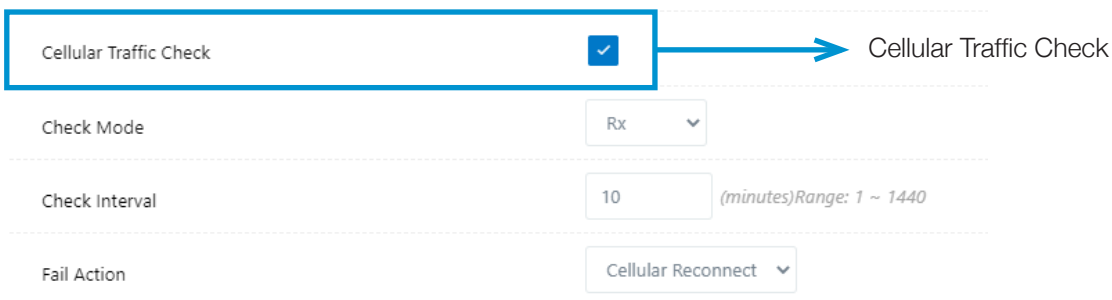
Table 5. ICMP settings

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.

Figure 22. Cellular Traffic Check



Cellular Traffic Check ☒

Cellular Traffic Check

Check Mode Rx

Check Interval 10 (minutes) Range: 1 ~ 1440

Fail Action Cellular Reconnect

Table 6. Cellular Traffic Check settings

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

**NOTE:** 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.

### SIM

Figure 23. SIM settings

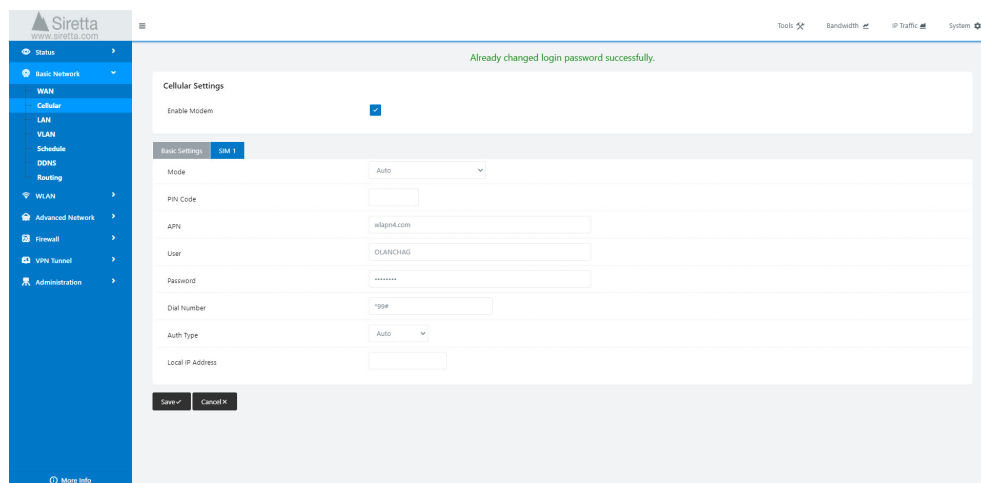


Table 7. SIM settings

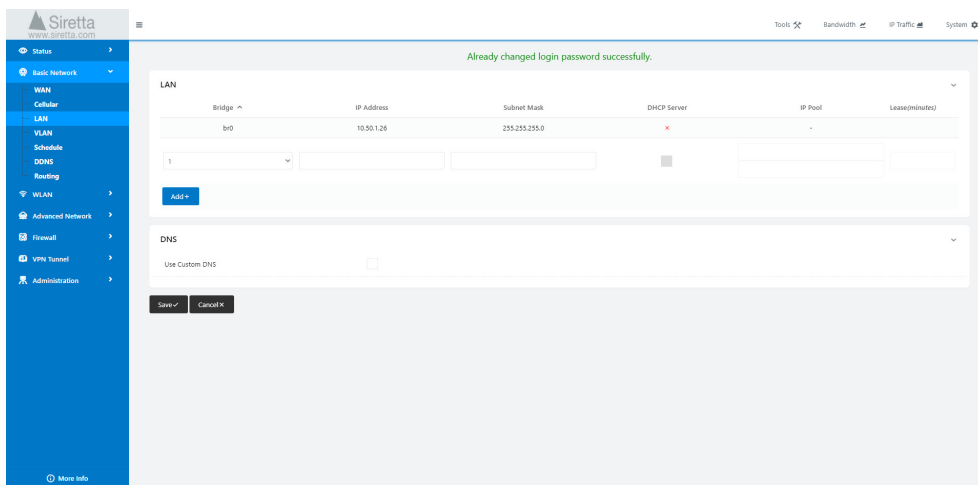
Setting	Options
Enable Modem	Enable / Disable LTE modem
Mode	Auto / LTE (FDD/TDD) / 3G (WCDMA/TD-SCDMA/HSPA) / 3G (CDMA 2000/CDMA 1x) / 2G (GSM). Using Auto will connect to the best network available, usually LTE.
PIN Code	Enter the PIN number assigned to the SIM Card if required
APN	Enter the APN provided by the cellular provider ( <b>always required</b> )
User	Enter User Name if provided by the cellular provider
Password	Enter Password if provided by the cellular provider
Dial number	Defaults to '*99#'. Only change if cellular provider requires you to do so.
Auth type	Auto / PAP / CHAP / MS-CHAP / MS-CHAPv2
Local IP address	From cellular provider if they have provided a fixed IP address

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

### LAN

The LAN settings define the LAN subnets, DHCP server and DNS settings.

Figure 24. LAN



### LAN

Table 8. LAN settings

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

After creating a new LAN, click 'Add+' to add it.



### DNS

Table 9. DNS settings

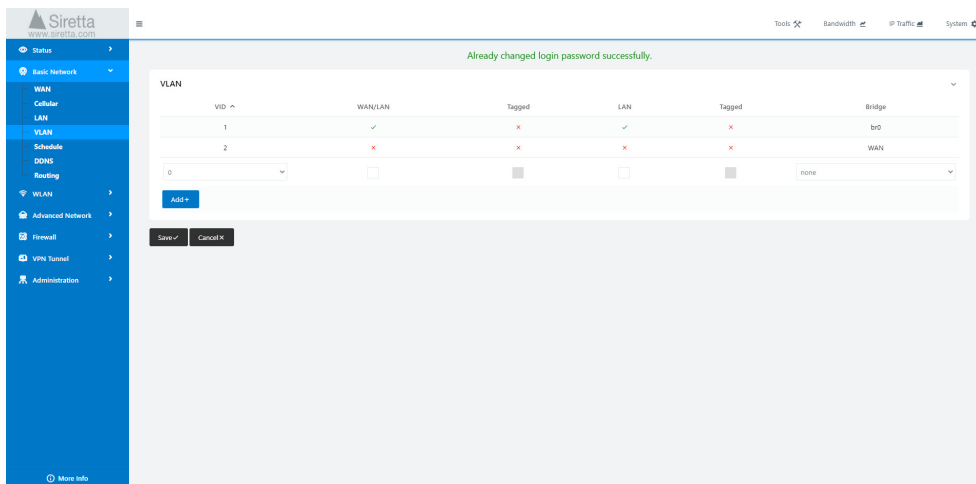
Setting	Options
Use Custom DNS	Enable to set custom DNS, otherwise DNS from the active WAN is used
Primary DNS	Custom primary DNS
Secondary DNS	Custom secondary DNS

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

### VLAN

VLANs may be set up and used in the QUARTZ-GOLD. If you will want to use a backup mode from WAN to Cellular or vice versa, configuring a VLAN is required.

Figure 25. VLAN



VID	WAN/LAN	Tagged	LAN	Tagged	Bridge
1	✓	✗	✓	✗	br0
2	✗	✗	✗	✗	WAN
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Table 10. VLAN settings

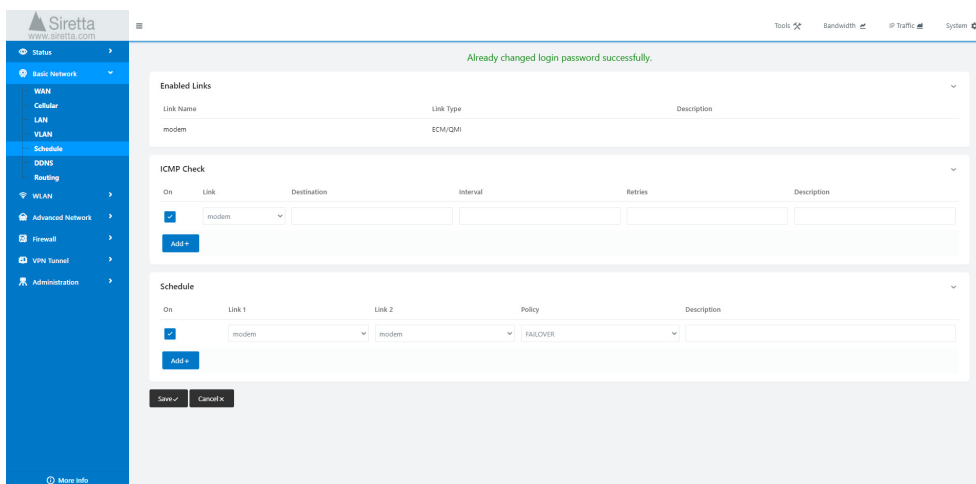
Setting	Options
VID	VLAN ID. Number between 0 and 15
WAN/LAN, LAN	Define the Ethernet jack
Tagged	Enable to add VLAN tag to the traffic
Bridge	Br0

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

### Schedule

Here you enter scheduled events 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.

Figure 26. Schedule



### ICMP Check

Table 11. ICMP Check settings

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

After creating a new ICMP Check, click 'Add+' to add it.

### Schedule

Table 12. Schedule settings

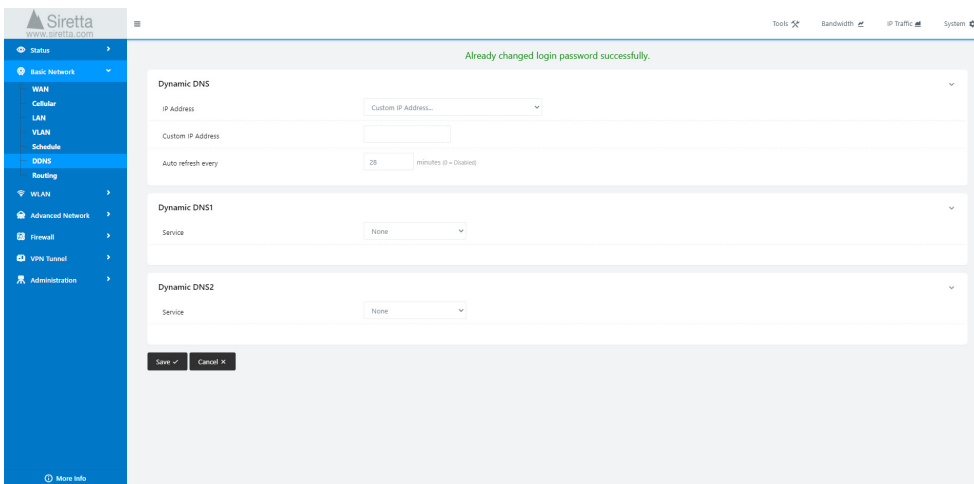
Setting	Options
On	Check to enable line
Link 1	Select primary interface from drop down
Link 2	Select secondary interface from drop down
Policy	Select Failover or Backup
Description	User description for the rule

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

### DDNS

Here you may enter Dynamic DNS settings. Please check carefully that the IP address that you are using is a public IP address. If you are using a cellular connection, almost certainly the address reported will be the IP address assigned by the cell that the connection is with. If your cellular provider has supplied a fixed IP address, it will need to be entered as a Custom IP address.

Figure 27. DDNS



### Dynamic DNS

Table 13. Dynamic DNS settings

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

Table 14. Dynamic DNS1 settings

Setting	Options
Service	Select DDNS provider or custom address.

### Dynamic DNS2

Table 15. Dynamic DNS2 settings

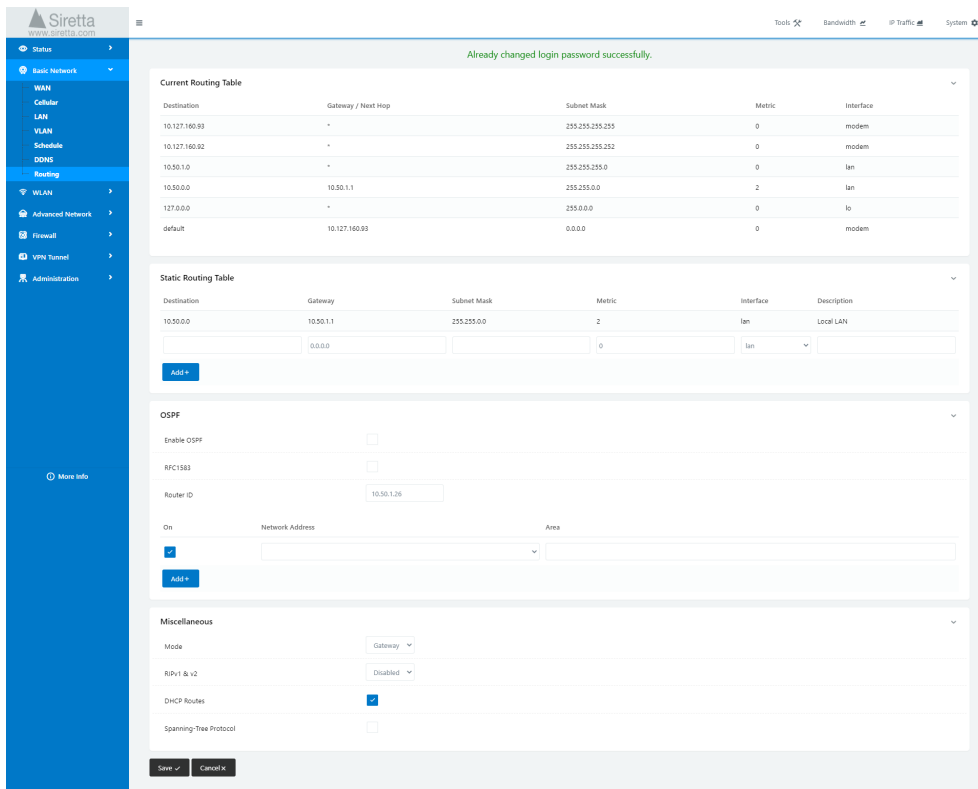
Setting	Options
Service	Select DDNS provider or custom address.

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 routes and OSPF to be set up and configured.\*

Figure 28. Routing



Already changed login password successfully.

#### Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
10.127.160.89	*	255.255.255.255	0	modem
10.127.160.92	*	255.255.255.252	0	modem
10.50.1.0	*	255.255.255.0	0	lan
10.50.0.0	10.50.1.1	255.255.0.0	2	lan
127.0.0.0	*	255.0.0.0	0	lo
default	10.127.160.89	0.0.0.0	0	modem

#### Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
10.50.0.0	10.50.1.1	255.255.0.0	2	lan	Local LAN
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Add +](#)

#### OSPF

Enable OSPF ☐

RFC1583 ☐

Router ID

On ☒ Network Address  Area

[Add +](#)

#### Miscellaneous

Mode

RIPv1 & v2

DHCP Routes ☒

Spanning-Tree Protocol ☐

[Save](#) [Cancel](#)

\*The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbours.

### Static Route

Table 16. Static Route settings

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
Interface	Select the interface to be used to reach the Gateway
Description	User description for the rule

After creating a new Static Route, click 'Add+' to add it.

### OSPF

Table 17. OSPF settings

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.

After creating a new OSPF, click 'Add+' to add it.



### Miscellaneous

Table 18. Miscellaneous settings

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

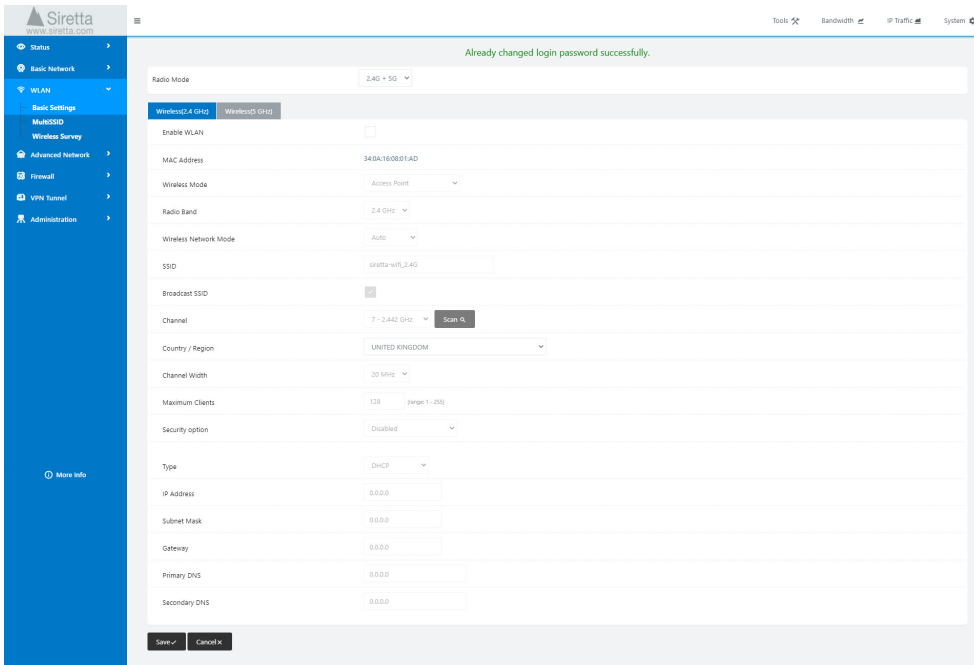
After making all required changes, click 'Save' to apply them.

## WLAN

### Basic Settings

Here you can set up and configure the WiFi. There are 2 radio channels that may be combined to work on 2.4GHz or 5GHz only, or they can be split with one 2.4GHz channel and one 5GHz channel.

Figure 29. WLAN settings



Already changed login password successfully.

Radio Mode: 2.4G + 5G

Wireless (2.4 GHz) | Wireless (5 GHz)

Enable WLAN: ☐

MAC Address: 345A1608D1AD

Wireless Mode: Access Point

Radio Band: 2.4 GHz

Wireless Network Mode: Auto

SSID: siretta-wifi\_2.4G

Broadcast SSID: ☐

Channel: 7 - 2.442 GHz Scan Q

Country / Region: UNITED KINGDOM

Channel Width: 20 MHz

Maximum Clients: 128 (range 1 - 255)

Security option: Disabled

Type: DHCP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Save Cancel X

### Wireless 2.4GHz

Table 19. Wireless 2.4GHz settings

Setting	Options
Radio Mode	Select 2.4G + 5G, 2.4G or 5G
Enable WLAN	Check to enable 2.4GHz wireless
MAC Address	MAC address of wireless interface
Wireless Mode	Choose Access Point, Wireless Client or Wireless Ethernet Bridge
Wireless Network Mode	Choose Auto, B Only, G Only, B/G Mixed, or N only
SSID	User name for SSID
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 20MHz, 40MHz
Maximum Clients	Upper bound for number of clients
Security Option	Choose WEP, WPA / WPA2 Personal / Enterprise, Radius
Security Settings	Set as required dependant on Security option selected

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

### Wireless 5GHz

Table 20. Wireless 5GHz settings

Setting	Options
Radio Mode	Select 2.4G + 5G, 2.4G or 5G
Enable WLAN	Check to enable 5GHz wireless
MAC Address	MAC address of wireless interface
Wireless Mode	Choose Access Point, Wireless Client or Wireless Ethernet Bridge
Wireless Network Mode	Choose Auto, A Only
SSID	User name for SSID
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 20MHz, 40MHz or 80MHz
Control Sideband	Choose lower or upper (not for 20MHz channel width)
Maximum Clients	Upper bound for number of clients
Security Option	Choose WEP, WPA / WPA2 Personal / Enterprise, Radius
Security Settings	Set as required dependant on Security option selected

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

### MultiSSID

Set up Multi SSID here. You may configure an additional 3 per radio, for a maximum of 8 SSIDs.

Figure 30. MultiSSID settings

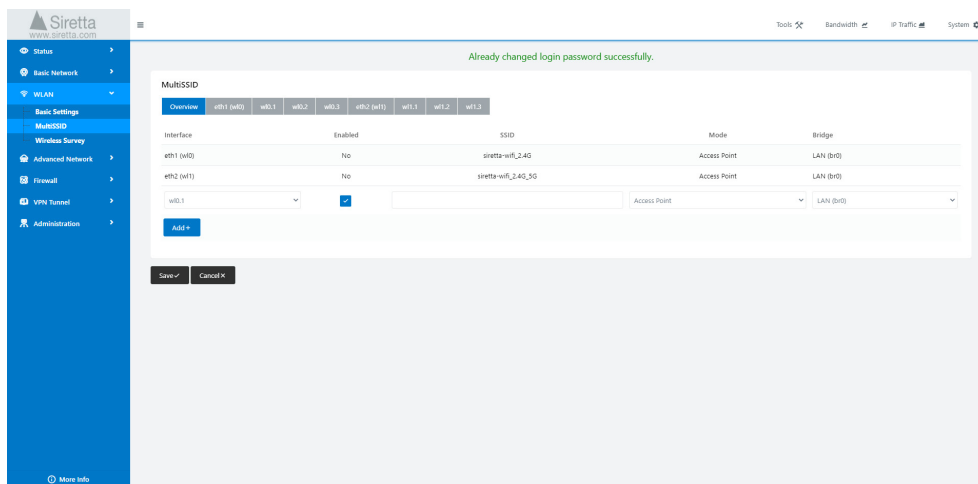


Table 21. MultiSSID settings

Setting	Options
Interface	WiFi Interface used
Enabled?	Check to enable
SSID	User chosen SSID name
Mode	Choose Access Point or Wireless Client
Bridge	Choose an existing LAN to connect to the SSID

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

## Wireless Survey

This shows details of the surrounding WiFi networks.

Figure 31. Wireless Survey settings

Already changed login password successfully.

Last Seen	SSID	BSSID	RSSI	Noise	Quality	Ch	Capabilities	Rates
Wed 16:54:02 1601 (Sec)	Production Lab	00:1D:AA:89:78:68	-79 dBm	0 dBm	0	6 40 kHz	infra wep shortprn shortslot 802.11n sg20 rg40	1,2,5,5,11 6,5,12,16,24,36,48,54
Wed 16:54:02 1601 (Sec)	Kooks	04:18:D6:22:6E:96	-90 dBm	0 dBm	0	11 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)		04:18:D6:22:72:71	-79 dBm	0 dBm	0	13 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)		06:18:D6:21:72:71	-86 dBm	-23 dBm	0	52 20 kHz	infra wep spectrum shortslot 802.11n sg20	6,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless Guest	06:18:D6:22:8C:F8	-93 dBm	0 dBm	0	1 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)		06:18:D6:22:6E:96	-90 dBm	0 dBm	0	11 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless	44:D9:E7:91:2D:8A	-74 dBm	-23 dBm	0	52 20 kHz	infra wep spectrum shortslot 802.11n sg20	6,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless	44:D9:E7:92:2D:8A	-74 dBm	0 dBm	0	6 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless Guest	46:D9:E7:92:2D:8A	-72 dBm	0 dBm	0	6 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless	74:83:C2:16:2C:C8	-53 dBm	-23 dBm	0	122 10 kHz	infra wep spectrum shortslot 802.11n sg20 rg40	6,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless	74:83:C2:16:2C:CC	-62 dBm	0 dBm	0	13 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	DIRECT-02-HP M477 LaserJet	76:40:8B:EF:9A:82	-74 dBm	0 dBm	0	11 20 kHz	infra wep spectrum shortslot 802.11n sg20	6,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	Siretta Wireless Guest	76:83:C2:16:2C:CC	-71 dBm	0 dBm	0	13 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,6,11,12,24 9,18,36,48,54
Wed 16:54:02 1601 (Sec)	PLUSNET-COKS	A0:39:EE:59:92:DA	-82 dBm	0 dBm	0	1 20 kHz	infra wep shortprn shortslot 802.11n sg20	1,2,5,5,11 6,5,12,16,24,36,48,54

14 added, 0 removed, 14 total.  
Last updated: Wed 16:54:02

Auto Expire Auto Refresh Refresh

## Advanced Network

### Port Forwarding

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

Figure 32. Port Forwarding settings

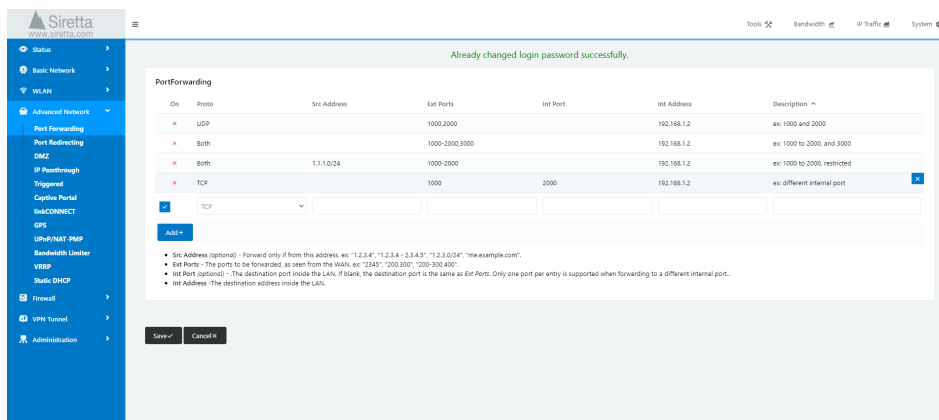


Table 22. Port Forwarding settings

Setting	Options
On	Check to enable the line
Protocol	Choose TCP, UDP or Both
Src Address	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	Internal port that matching packets will be forwarded to
Int Address	Internal IP address that matching packets will be forwarded to
Description	User description for the rule

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.

Figure 33. Port Redirecting settings

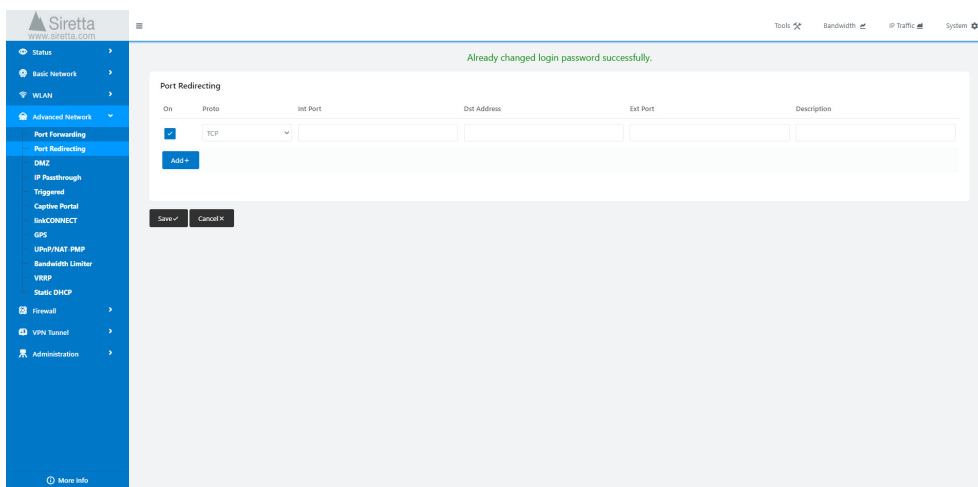


Table 23. Port Redirecting settings

Setting	Options
On	Check to enable the line
Proto	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
Description	User description for the rule

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.

Figure 34. DMZ settings

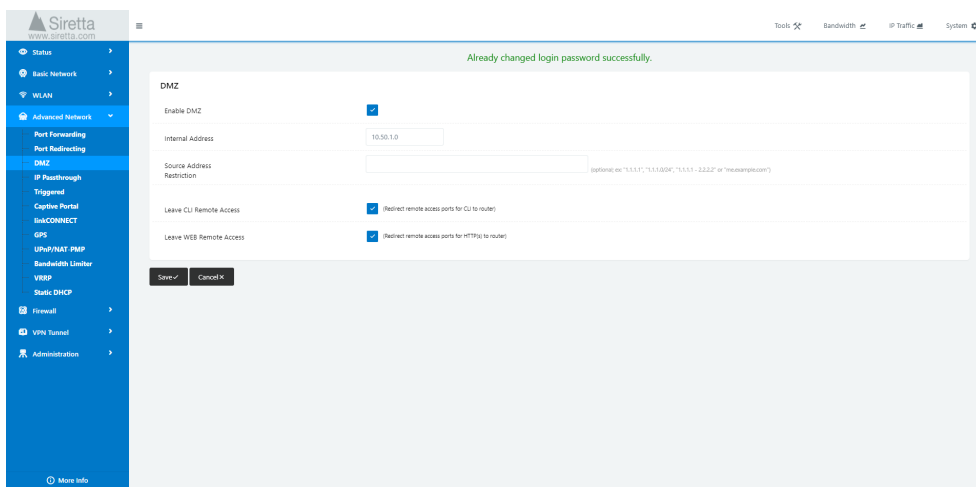


Table 24. DMZ settings

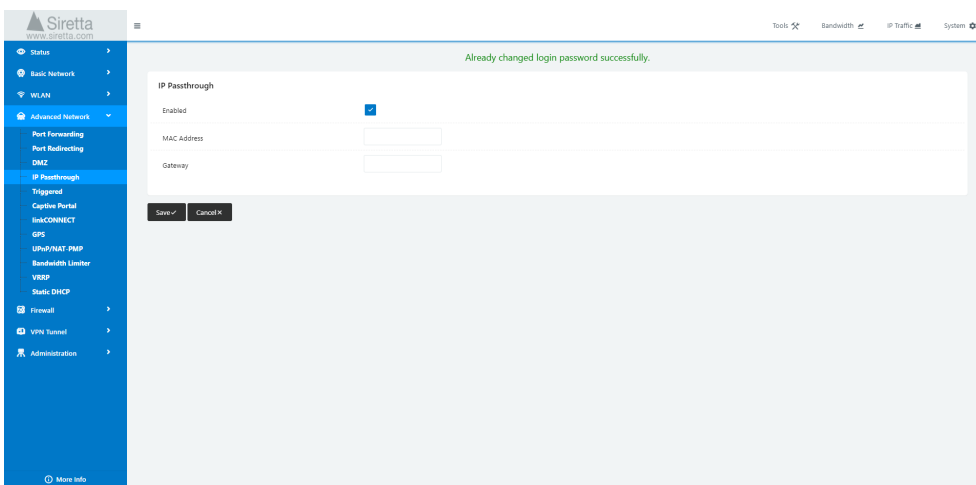
Setting	Options
Enable DMZ	Options
Internal Address	Check to enable the DMZ
Source Address Restriction	Internal IP address that packets on the WAN external interface will be forwarded to
Leave CLI Remote Access	Limit the DMZ to pass only packets from specific IP addresses or domains
Leave WEB Remote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

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

### 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.

Figure 35. IP Passthrough settings



Already changed login password successfully.

IP Passthrough

Enabled ☒

MAC Address

Gateway

Save Cancel

Table 25. IP Passthrough settings

Setting	Options
Enabled	Check to enable IP Passthrough
MAC Address	Enter MAC address of device on LAN being bridged to (this device should have a DHCP assigned address)
Gateway	Enter an IP address that may be used by a second device on the LAN to access the router (because the bridged device will not be able to)

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. 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.

Figure 36. Triggered settings

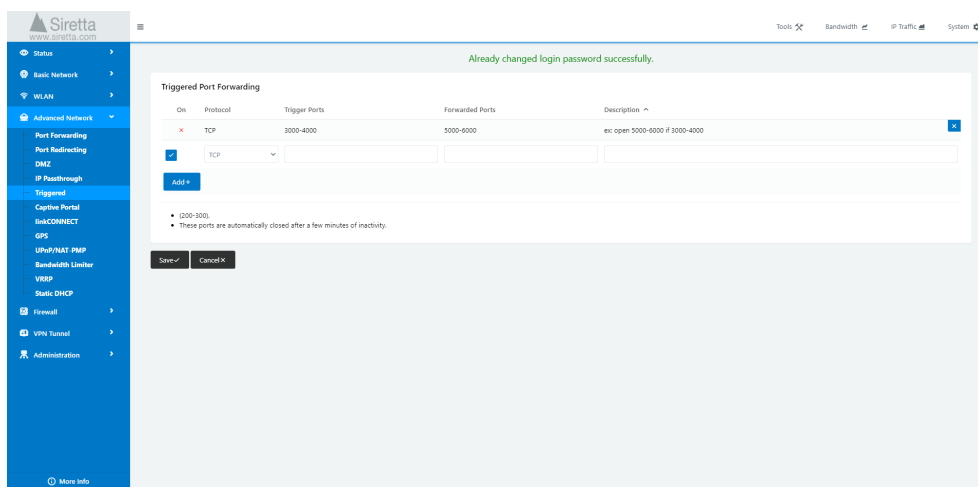


Table 26. Triggered settings

Setting	Options
On	Check to enable the line
Protocol	Choose TCP, UDP or Both
Trigger Ports	Choose port to use as a trigger to open a port
Forwarded Ports	Choose the ports that will be forwarded from the WAN to the LAN
Description	User description for the rule

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.

Figure 37. Captive Portal settings

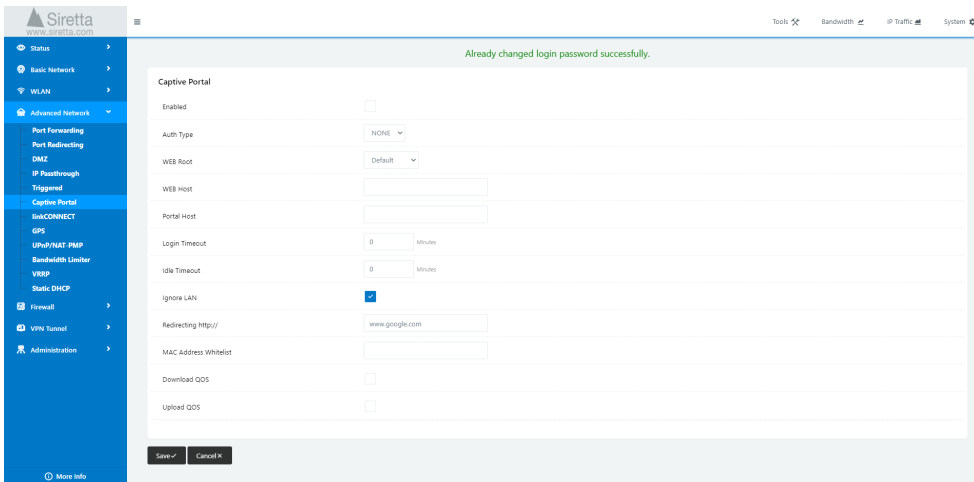


Table 27. Captive Portal settings

Setting	Options
Enabled	Check to enable the Captive Portal
Auth Type	<p>Select captive portal file storage:</p> <ul style="list-style-type: none"> <li>» Default: Stored in router firmware</li> <li>» In-Storage: Stored in internal flash memory</li> <li>» Ex-Storage: Stored in extended storage such as internal flash drive</li> </ul>
WEB Root	Choose port to use as a trigger to open a port
WEB Host	Enter domain name for the captive portal access
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

Table 27 (continued). Captive Portal settings

Setting	Options
Ignore LAN	Enable to allow devices on the LAN to bypass the captive portal
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

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.

Figure 38. LinkCONNECT settings

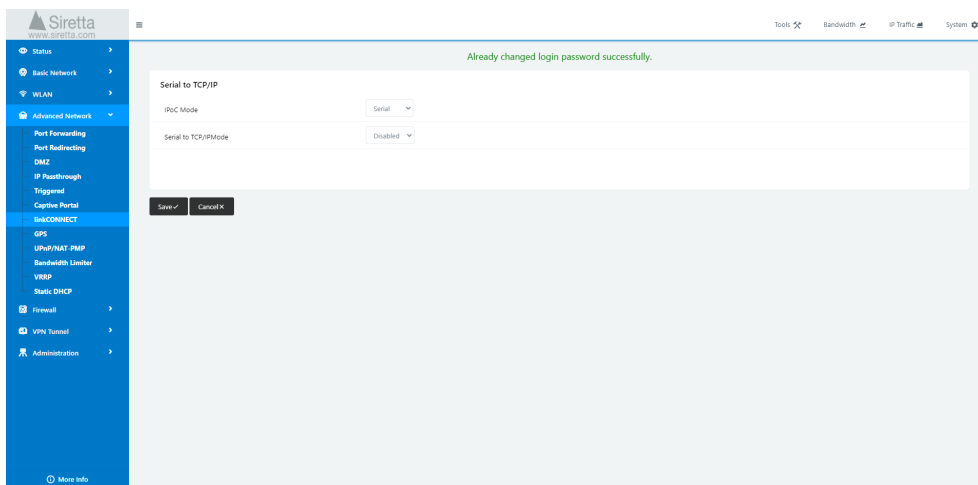


Table 28. LinkCONNECT settings

Setting	Options
IPoC Mode	Choose Serial or Modbus
Serial to TCP/ IPMode	Choose Disable / Server or Client (Serial) or Enable / Disable (Modbus)

After making these selections, further options pertinent to the mode of operation will be displayed as shown over page.

Figure 39. Extended LinkCONNECT settings

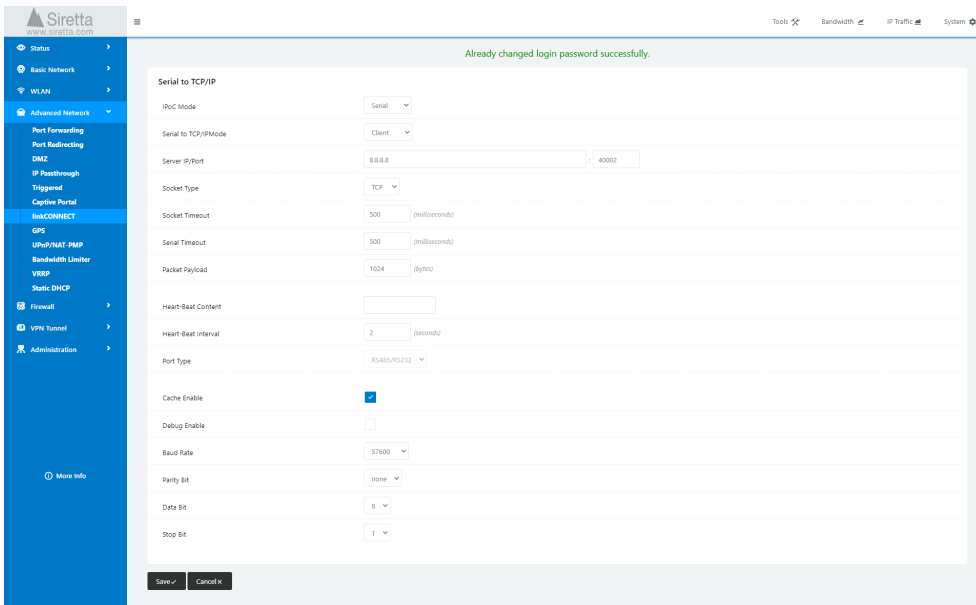


Table 29. Extended LinkCONNECT settings

Setting	Options
Server IP/Port	Enter IP address / domain name and port
Socket type	Choose TCP or UDP
Socket Timeout	Choose socket timeout in mS. This is the time that the router will wait before sending data to the serial port.
Serial Timeout	Choose serial timeout in mS. This is the maximum waiting time for the serial port packet to reach its desired size. The serial port packet will be transmitted on the earlier of it reaching the desired size or this timeout setting.
Packet Payload	Desired size of the serial port packet
Heart-Beat Content	Send heart beat to server to keep the router online and allow the server to confirm that the link is open.
Heart-Beat Interval	Choose heart beat interval in seconds
Port Type	Always RS485 / RS232
Cache Enable	Check to enable Cache

Table 29 (continued). Extended LinkCONNECT settings

Setting	Options
Debug Enable	Check to enable debug
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

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



### GPS

Here the GPS can be enabled (in client or server mode). When enabled in either mode, the current location may be viewed in Status > GPS Status.

In client mode, the router sends the GPS messages to the specified IP address and port. In server mode the router makes the GPS messages available on a specified port.

Figure 40. GPS settings

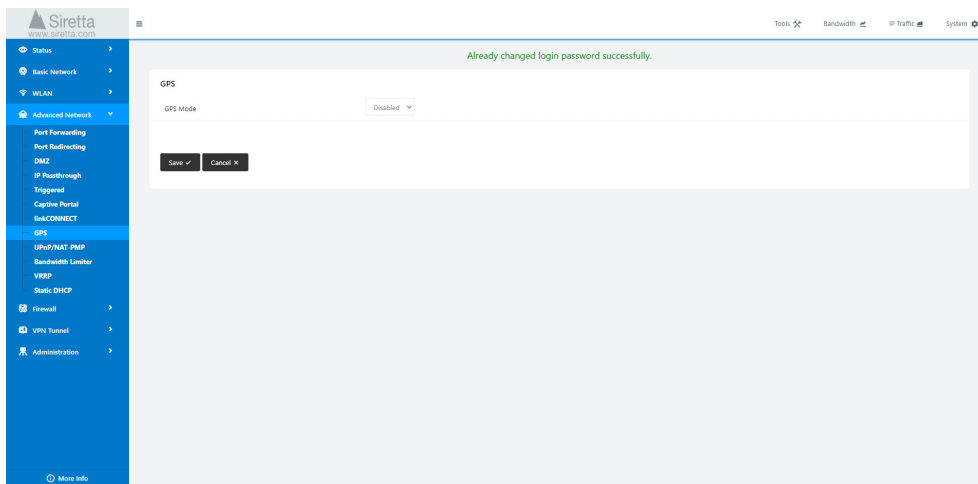


Table 30. GPS settings

Setting	Options
GPS Mode	Choose Disabled, Server or Client

After making this selection, further options pertinent to the mode of operation will be displayed as shown over page.

### Server Mode

Figure 41. Extended GPS settings - Server Mode

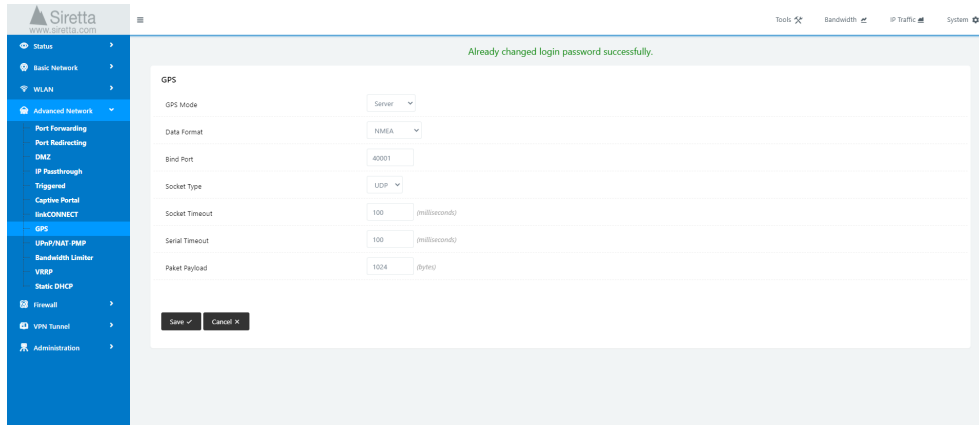


Table 31. Extended GPS settings - Server Mode

Setting	Options
GPS Mode	Server chosen
Data Format	Choose NMEA or M2M_FMT
Bind Port	Choose port for connection
Socket Type	Choose TCP or UDP
Socket Timeout	Choose socket timeout in mS. This is the time that the router will wait before sending data to the serial port.
Serial Timeout	Choose serial timeout in mS. This is the maximum waiting time for the GPS packet to reach its desired size. The GPS packet will be transmitted on the earlier of it reaching the desired size or this timeout setting.
Packet Payload	Desired size of the GPS packet
Heart-Beat Content	Add heart-beat content to GPS message to identify sender (M2M_FMT only).
Heart-Beat Interval	Choose GPS send interval in seconds (M2M_FMT only).

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

### Client Mode

Figure 42. Extended GPS settings - Client Mode

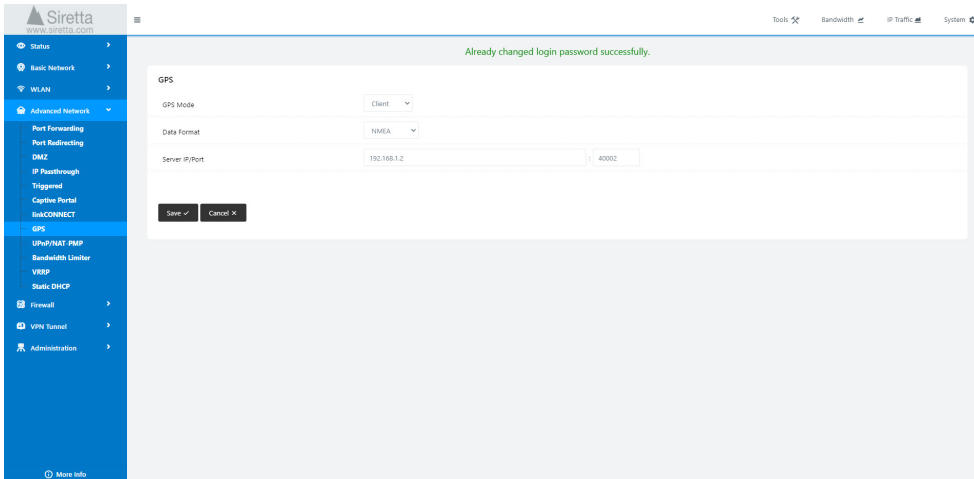


Table 32. Extended GPS settings - Client Mode

Setting	Options
GPS Mode	Client chosen
Data Format	Choose NMEA or M2M_FMT
Server IP port	Choose IP address and port to send GPS data to
Heart-Beat Content	Add heart-beat content to GPS message to identify sender (M2M_FMT only).
Heart-Beat Interval	Choose GPS send interval in seconds (M2M_FMT only).

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

### Example NMEA Data

24/06/2021;15:36:55;;;;;8;;;;;\$GPGV,3,1,12,03,23,213,32,08,54,158,42,10,20,049,40,17,06,309,30,1\*66

\$GPGSV,3,2,12,21,80,305,32,27,23,143,42,32,31,082,48,14,27,302,,1\*6A

\$GPGSV,3,3,12,22,49,209,,24,,,36,,,43,49,,,34,1\*5F

\$GPGGA,143655.00,5116.638985,N,00045.207534,W,1,07,0.8,86.2,M,47.0,M,,\*42

\$GPVTG,180.8,T,184.4,M,0.0,N,0.0,K,A\*2B

\$GPRMC,143655.00,A,5116.638985,N,00045.207534,W,0.0,180.8,240621,3.5,W,A,V\*47

\$GPGSA,A,3,03,08,10,21,22,27,32,,,,,1.1,0.8,0.7,1\*2D

### Example M2M\_FMT Data

24/06/2021;15:37:34;;;;;8;;;;;210624,143734.00,08,5116.638965,N,00045.207544,W,0.0,180.8,1,0.7,86.2

**Explanation:** Date;Time;;;;;Satellites used;;;;;YMD,HMS,No. Satellites,Latitude,N or S,Longitude,W or E,speed,degrees,Fix indication,HDOP,Altitude

### UPnP/NAT-PMP

Universal Plug and Play/NAT Port Mapping Protocol settings.

Figure 43. UPnP/NAT-PMP settings

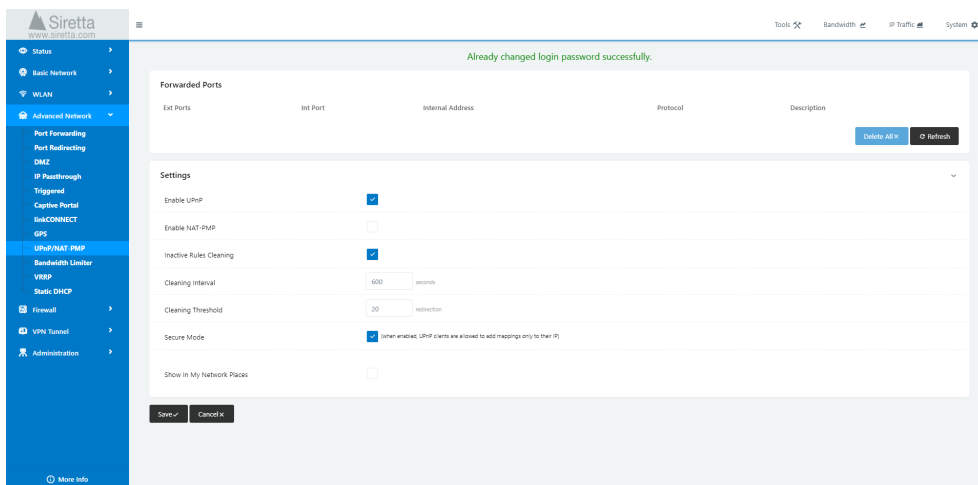


Table 33. UPnP/NAT-PMP settings

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 if inactive rules cleaning enabled
Cleaning Threshold	Choose threshold if inactive rules cleaning enabled
Secure mode	Check to enable
Show in my Network Places	Check to enable

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

### Bandwidth Limiter

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

Figure 44. Bandwidth Limiter settings

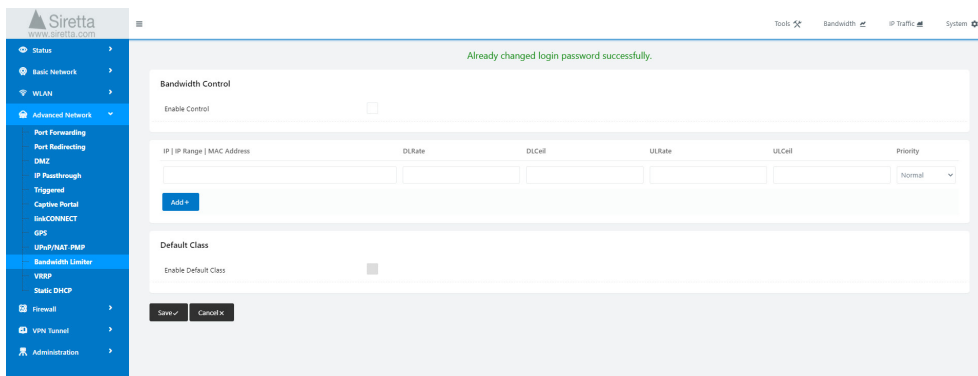


Table 34. Bandwidth Limiter settings

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	Choose 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 rule for unspecified connections

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.

Figure 45. VRRP settings

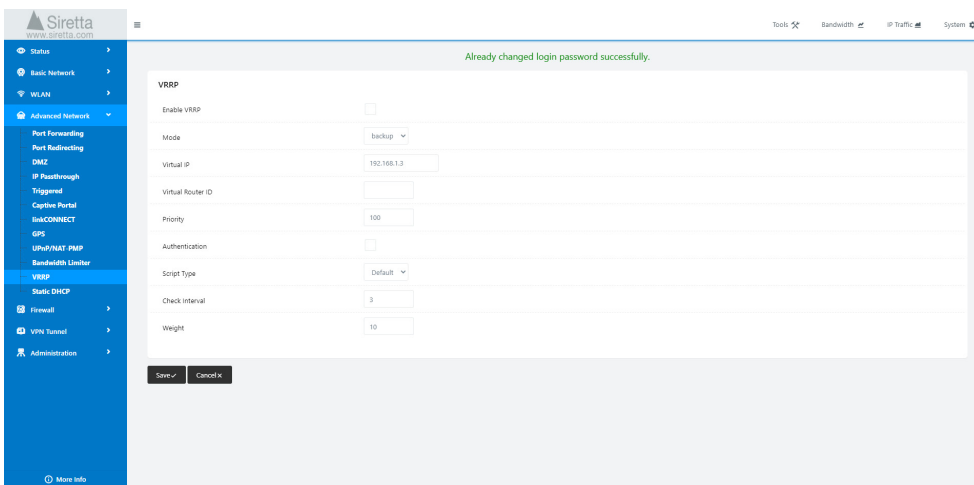


Table 35. VRRP settings

Setting	Options
Enable VRRP	Check to enable
Mode	Choose master or backup
Virtual IP	Choose 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)

Table 35 (continued). VRRP settings

Setting	Options
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

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. This is not advised as it can be unreliable.

Figure 46. Static DHCP settings

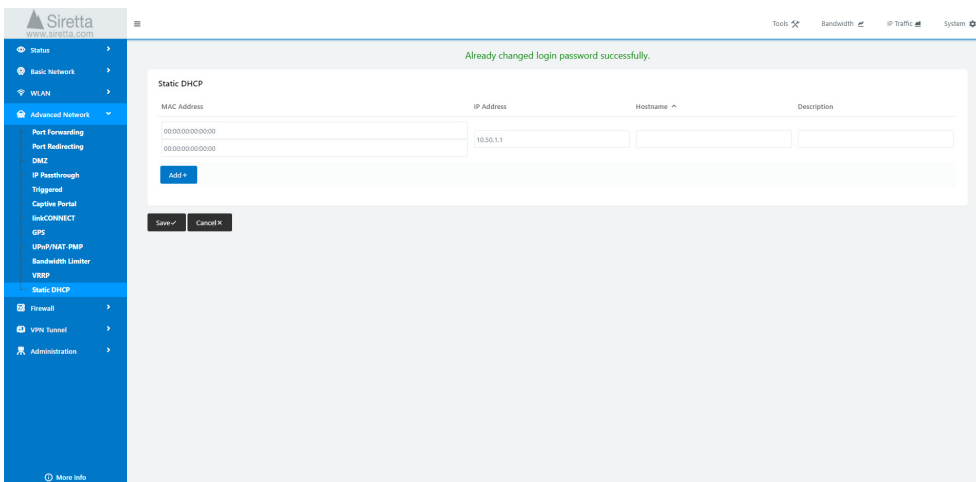


Table 36. Static DHCP settings

Setting	Options
MAC Address	Enter MAC address
IP Address	Enter IP address to be bound to MAC address
Hostname	Enter host name (names will be truncated by a space)
Description	User description for the rule

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.

Figure 47. IP/URL Filtering settings

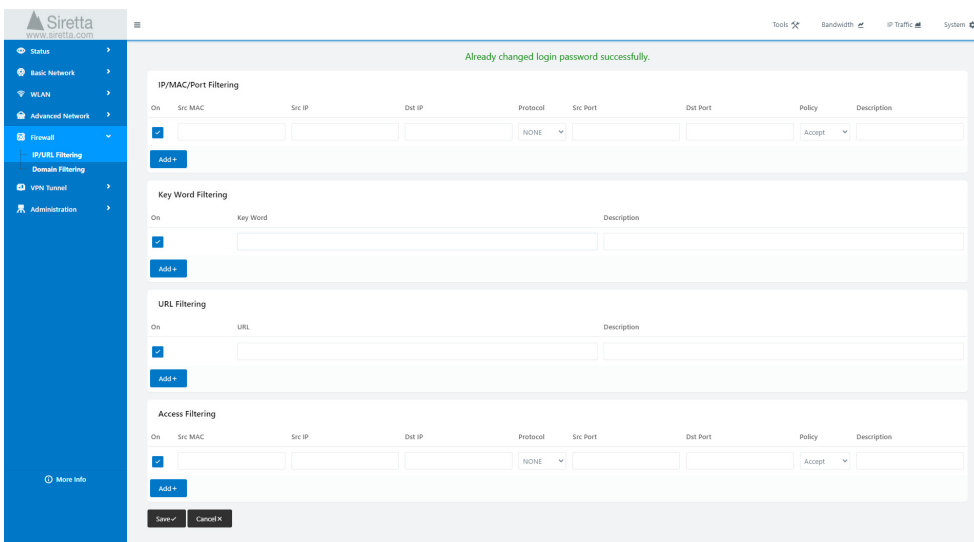


Table 37. IP/URL Filtering settings

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)

Table 37 (continued). IP/URL Filtering settings

Setting	Options
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

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

### Domain Filtering

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. This is not advised as it can be unreliable.

Figure 48. Domain Filtering settings

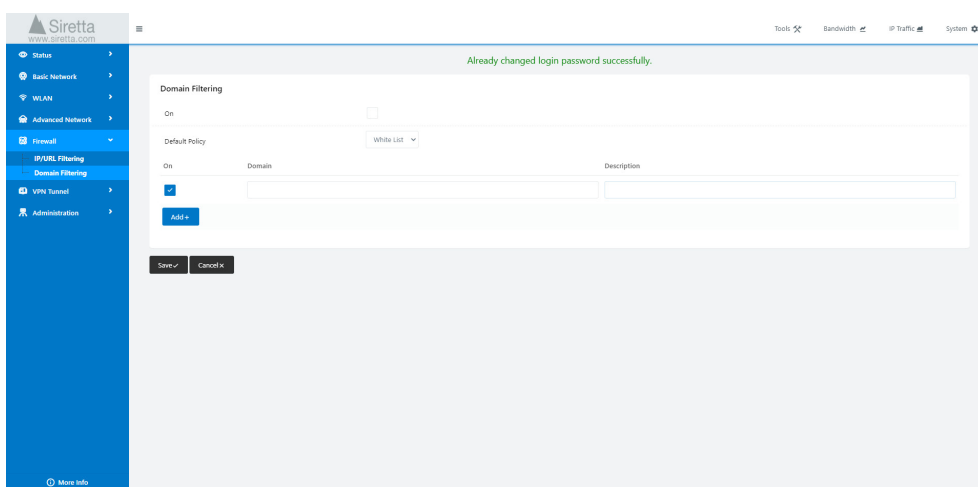


Table 38. Domain Filtering settings

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

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.

Figure 49. GRE Tunnel settings

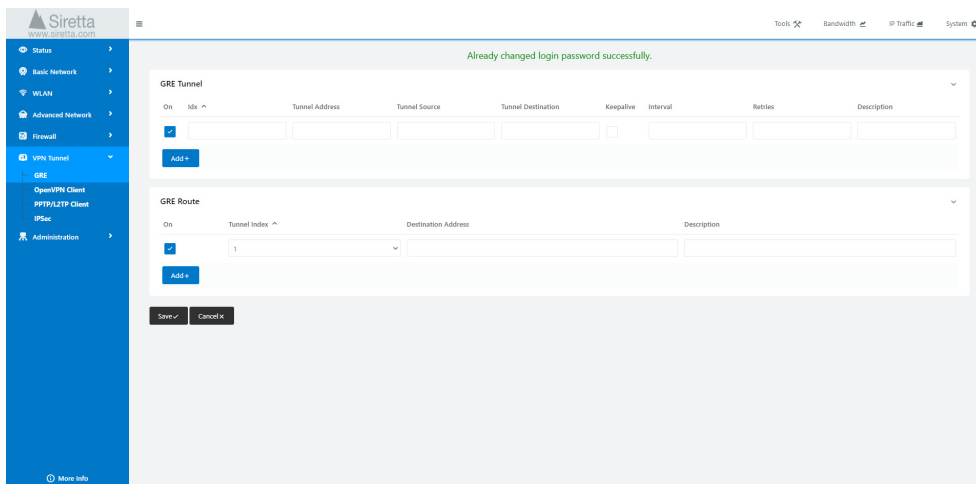


Table 39. GRE Tunnel settings

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
Tunnel Index	Select between 1 and 8

Table 39 (continued). GRE settings

Setting	Options
Destination Address	Enter remote network IP address and mask
Description	User description for the rule

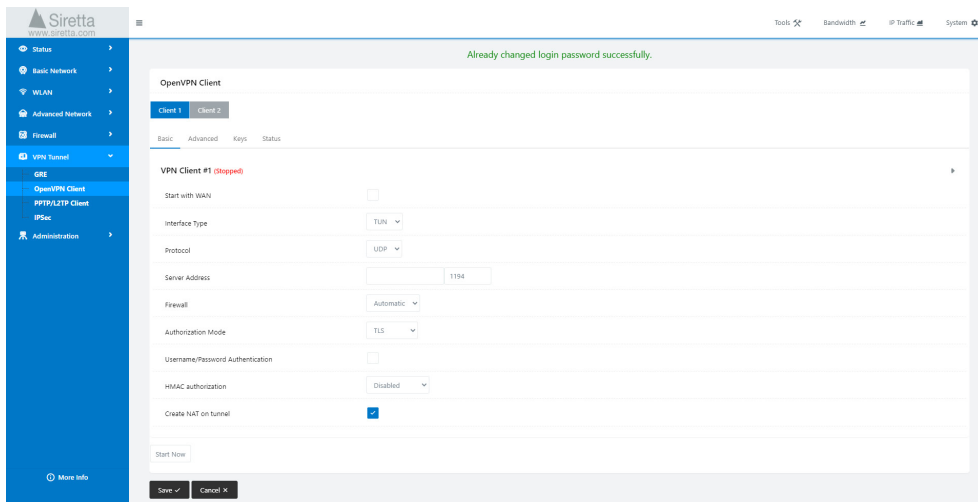
After creating a new default policy rule, click 'Add+' to add it. After making all required changes, click 'Save' to apply them.

## OpenVPN Client

Configure up to two OpenVPN Clients here.

### Basic

Figure 50. OpenVPN Client - Basic settings



Already changed login password successfully.

### OpenVPN Client

Client 1 Client 2

Basic Advanced Keys Status

**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 ☒

Start Now

Save Cancel

Table 40. OpenVPN Client - Basic settings

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)

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

### Advanced

Figure 51. OpenVPN Client - Advanced settings

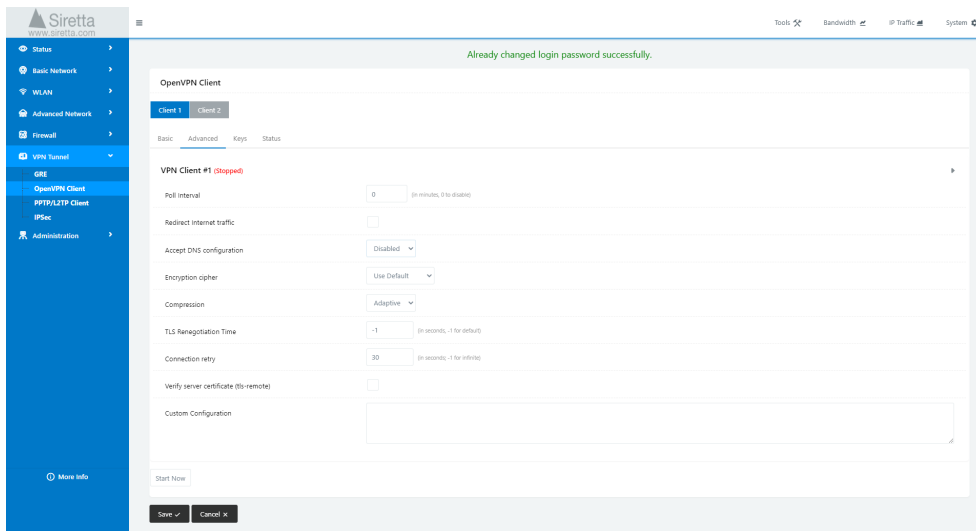


Table 41. OpenVPN Client - Advanced settings

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

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

Registered in England No. 08405712  
VAT Registration No. GB163 04 0349

[Download Latest Edition](#)

Siretta Ltd  
Basingstoke Road  
Spencers Wood  
Reading  
Berkshire RG7 1PW

sales  
email  
web

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



Table 41 (continued). OpenVPN Client - Advanced settings

Setting	Options
Custom Configuration	As required by OpenVPN server

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

## Keys

Figure 52. OpenVPN Client - Keys settings

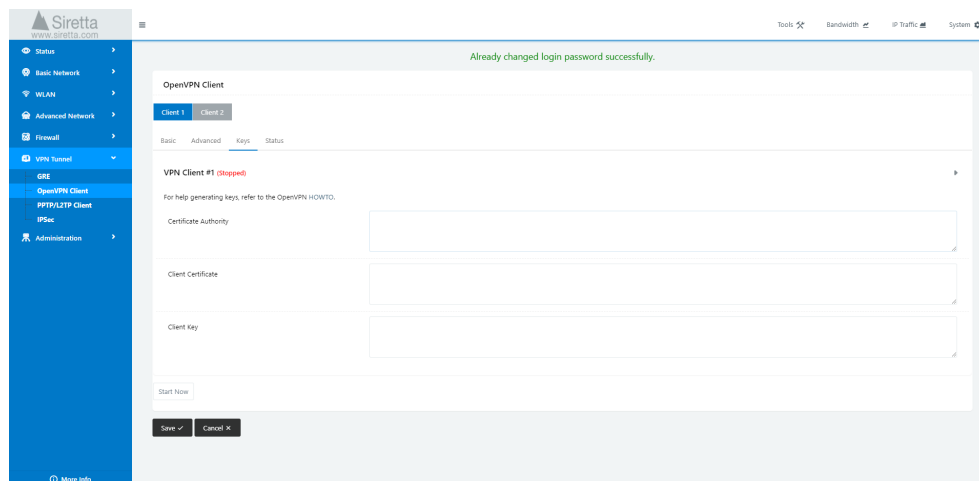


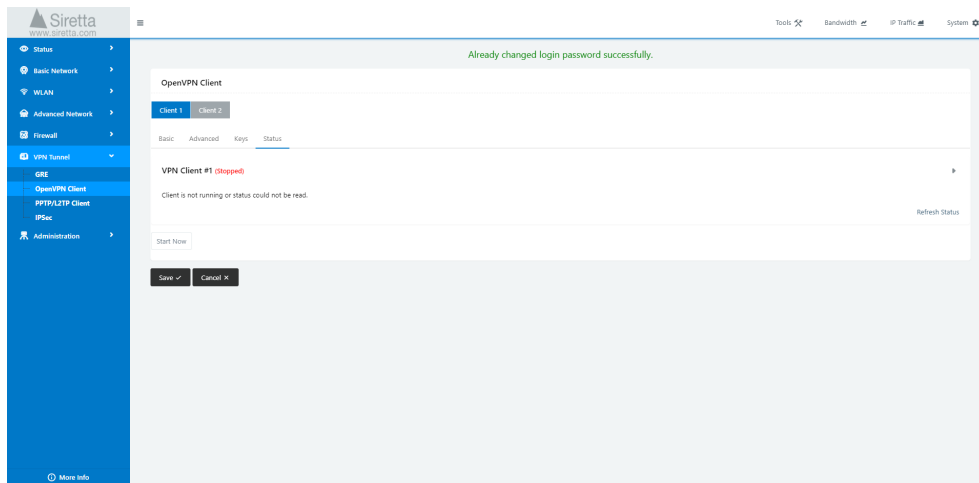
Table 42. OpenVPN Client - Advanced settings

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

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

### Status

Figure 53. OpenVPN Client - Status settings

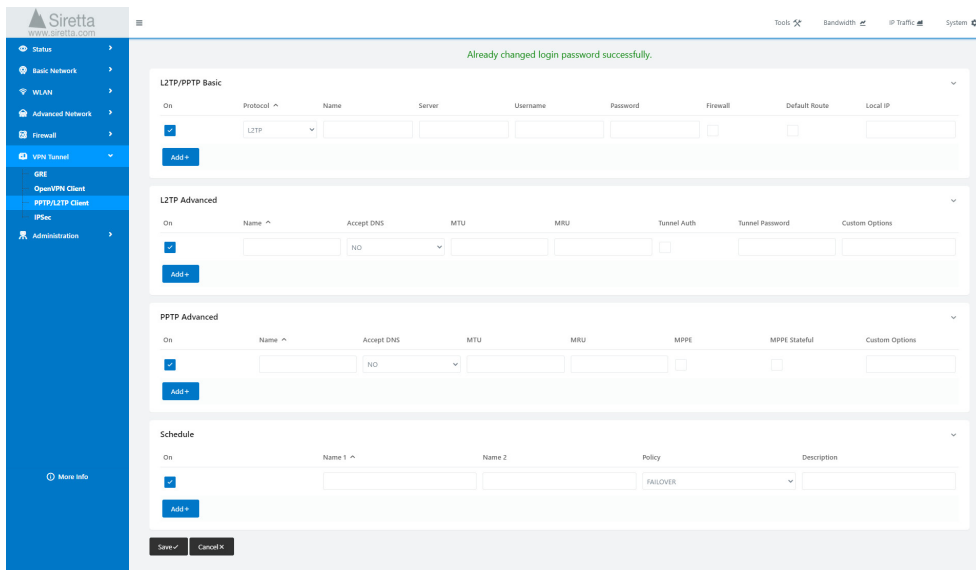


Click refresh status to see the status of the OpenVPN tunnel and data statistics.

### PPTP/L2TP Client

Configure PPTP and L2TP tunnels here.

Figure 54. PPTP/L2TP settings



### L2TP/PPTP Basic

Table 43. L2TP/PPTP - Basic settings

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 tunnel the routers default route
Local IP	Local IP address for the tunnel

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

### L2TP Advanced

Table 44. L2TP - Advanced settings

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

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

### Schedule

Table 45. Schedule settings

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

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

### PPTP Advanced

Table 46. PPTP - Advanced settings

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

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

### IPSEC

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

### IPSEC Group Setup

Figure 55. IPSEC - Group Setup

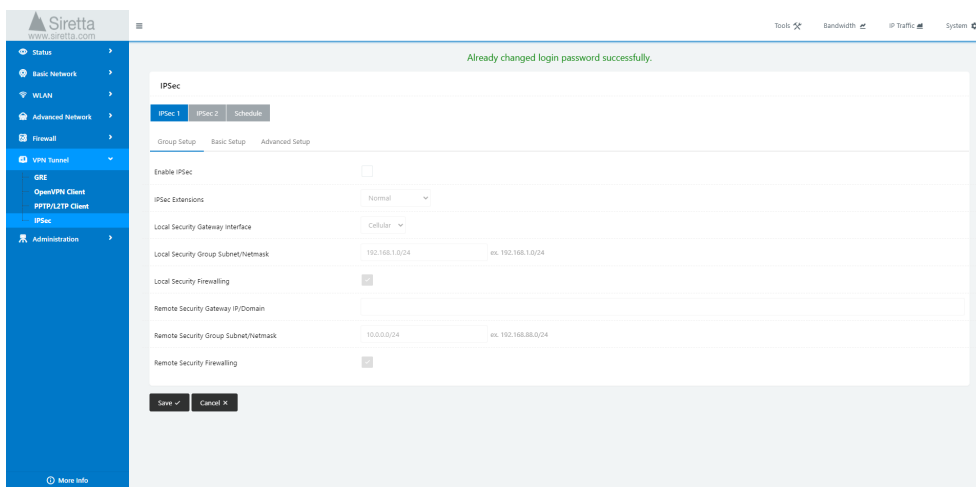


Table 47. IPSEC - Group setup settings

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

Table 47 (continued). IPSEC - Group setup settings

Setting	Options
Remote Security Group Subnet/Netmask	Enter IPsec remote subnet and mask
Remote Security Firewalling	Check to enable firewalling for the remote subnet

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

### IPSEC Basic Setup

Figure 56. IPSEC Basic Setup

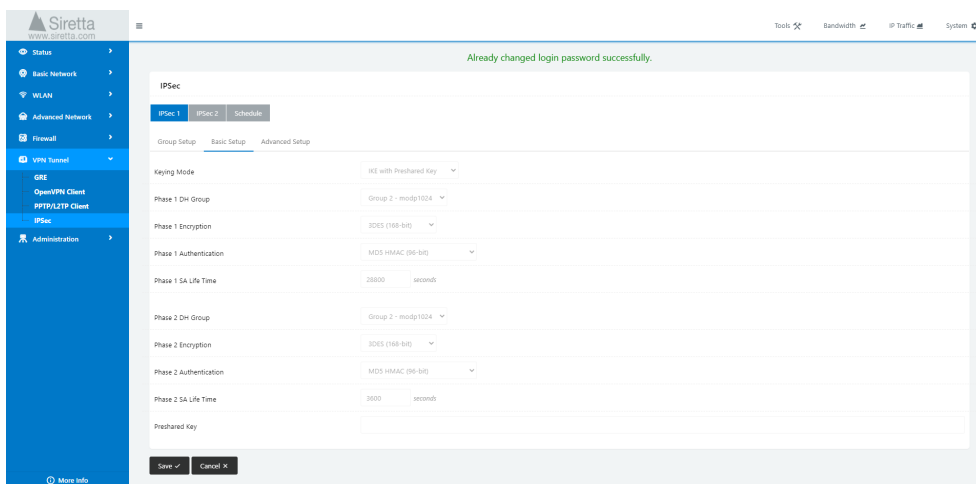


Table 48. IPSEC - Basic setup settings

Setting	Options
Keyring 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

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.



### IPSEC Advanced Setup

Figure 57. IPSEC - Advanced Setup

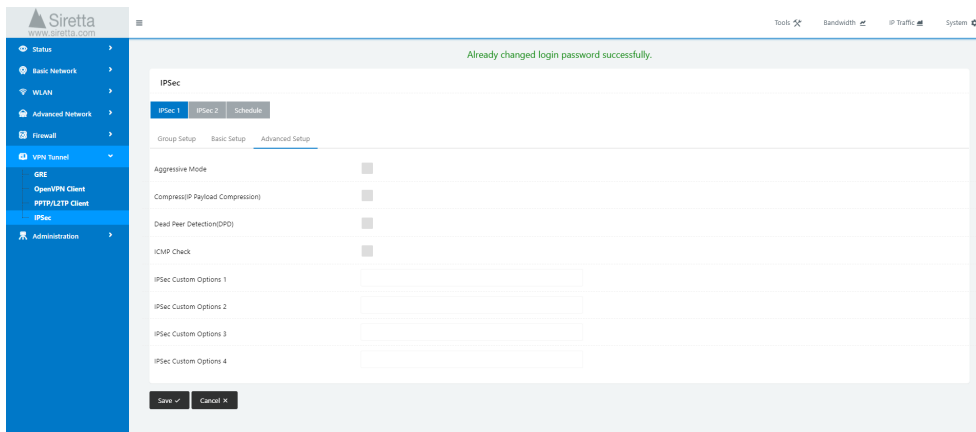


Table 49. IPSEC - Advanced setup settings

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

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

### IPSEC Schedule

Figure 58. IPSEC - Schedule

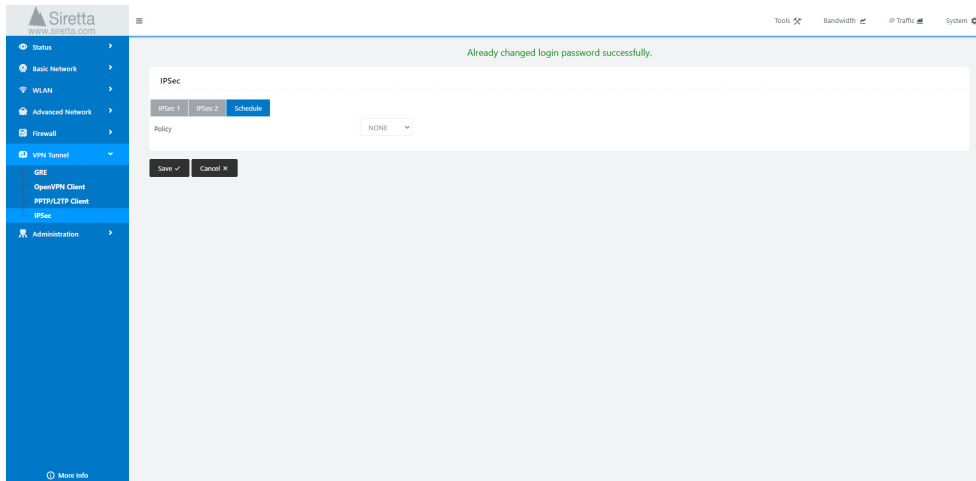


Table 50. IPSEC - Schedule settings

Setting	Options
Policy	Choose NONE, FAILOVER or BACKUP

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

## Administration

### Identification

Setup the router name, hostname and domain name here.

Figure 59. Identification settings

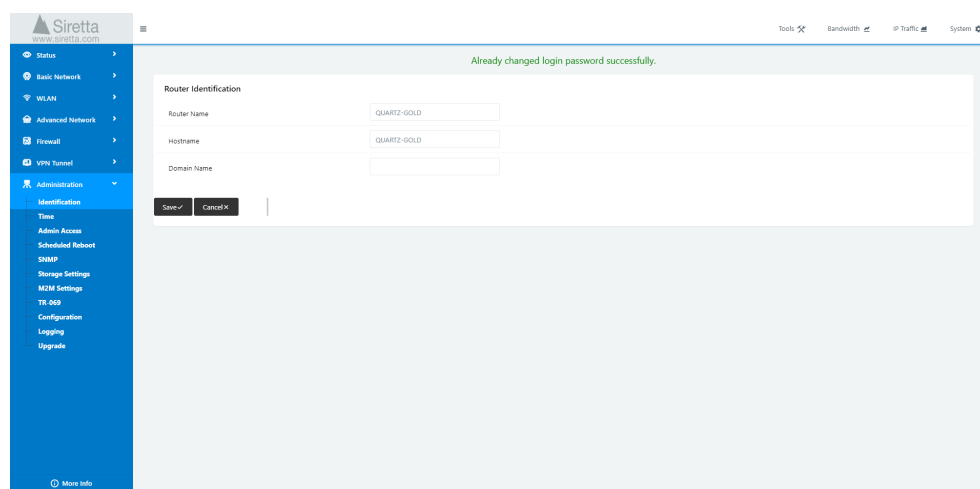


Table 51. Identification settings

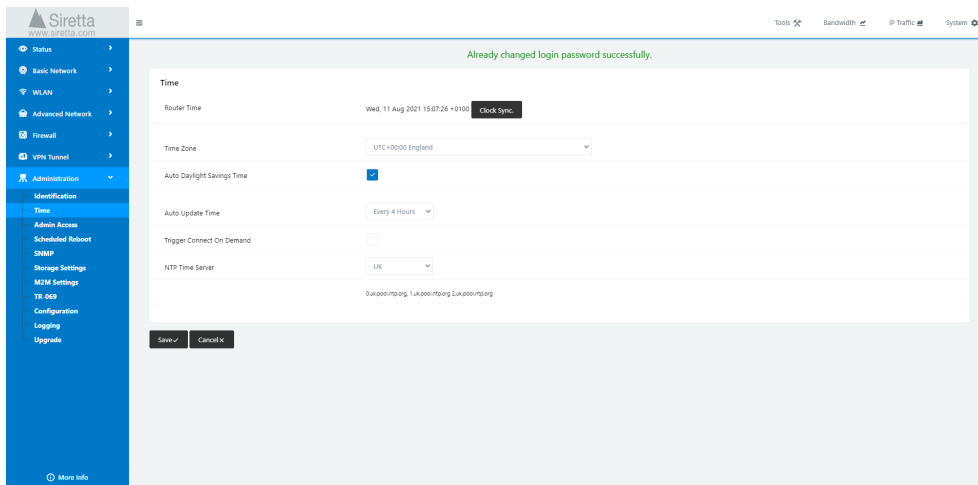
Setting	Options
Router Name	Enter an identifying name for the router
Hostname	Enter required hostname
Domain name	Enter domain name used by the WAN (if used, usually left blank)

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

### Time

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

Figure 60. Time settings



Already changed login password successfully.

**Time**

Router Time: Wed, 11 Aug 2021 15:07:26 +0100 Clock Sync

Time Zone: UTC+00:00 England

Auto Daylight Savings Time: ☒

Auto Update Time: Every 4 Hours

Trigger Connect On Demand: ☐

NTP Time Server: UK  
duk.poo.rtp.org, luk.poo.rtp.org, luk.poo.rtp.org

Save Cancel X

Table 52. Time settings

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 <a href="https://www.iana.org/time-zones">https://www.iana.org/time-zones</a>
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 enable connect on demand
NTP Server	Choose NTP server from list or enter your own custom server

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 configuration settings here. There are two account types: 'Admin' which has unlimited access and 'User' which has read only access.

Figure 61. Admin Access settings

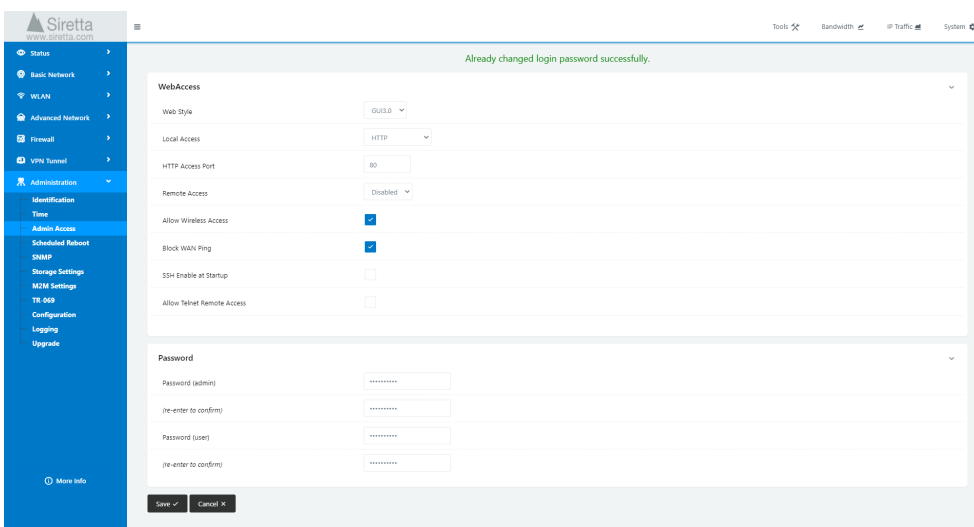


Table 53. Admin Access settings

Setting	Options
Web Style	Choose GUI3.0 or GUI2.0. GUI3.0 is recommended and the view presented in this document. GUI2.0 is the interface style of older QUARTZ routers.
Local Access	Choose Disabled, HTTP, HTTPS or HTTP & HTTPS. Warning: If you select Disabled, make sure that you are prepared to access via Telnet or SSH, otherwise you may have to perform a hardware reset to regain access.
HTTP Access Port	Enter HTTP access port
Remote Access	Choose Disabled, HTTP or HTTPS
Allow Wireless Access	Check to allow admin access via WiFi
Block WAN Ping	Check to block WAN ping

Table 53 (continued). Admin Access settings

Setting	Options
SSH Enable at Startup	Check to enable SSH at 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

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

### Scheduled Reboot

Figure 62. Scheduled Reboot settings

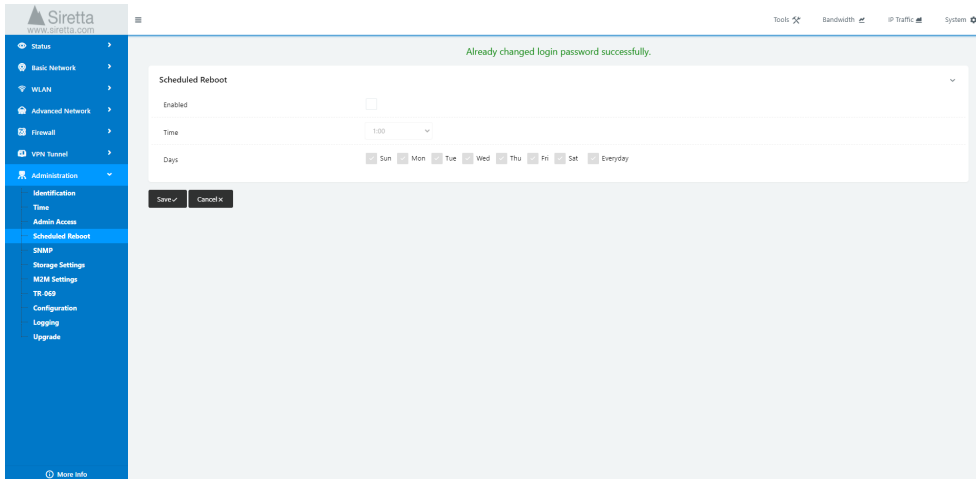


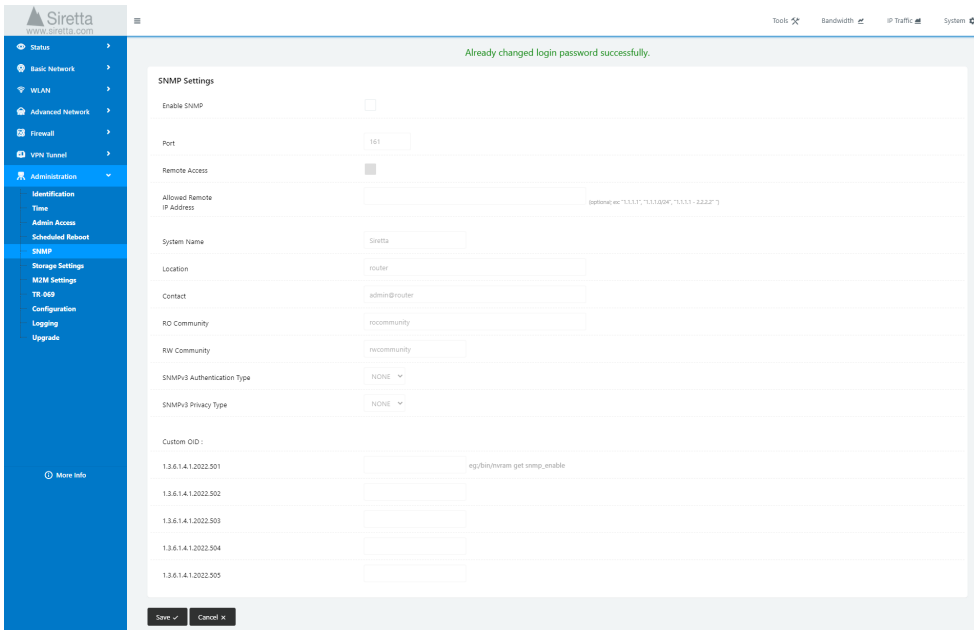
Table 54. Scheduled Reboot settings

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

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

### SNMP

Figure 63. SNMP settings



Already changed login password successfully.

**SNMP Settings**

Enable SNMP ☐

Port

Remote Access ☐

Allowed Remote IP Address

System Name

Location

Contact

RO Community

RW Community

SNMPv3 Authentication Type

SNMPv3 Privacy Type

Custom OID :

1.3.6.1.4.1.2022.501

1.3.6.1.4.1.2022.502

1.3.6.1.4.1.2022.503

1.3.6.1.4.1.2022.504

1.3.6.1.4.1.2022.505

Table 55. SNMP settings

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 remote 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



Table 55 (continued). SNMP settings

Setting	Options
SNMPv3 Authentication Type	Choose NONE, MD5 or SHA
SNMPv3 Privacy Type	Choose NONE, DES or AES
Custom OID	Enter up to 5 custom OIDs (optional)

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 and appended to the file sms.list.

Figure 64. Storage settings

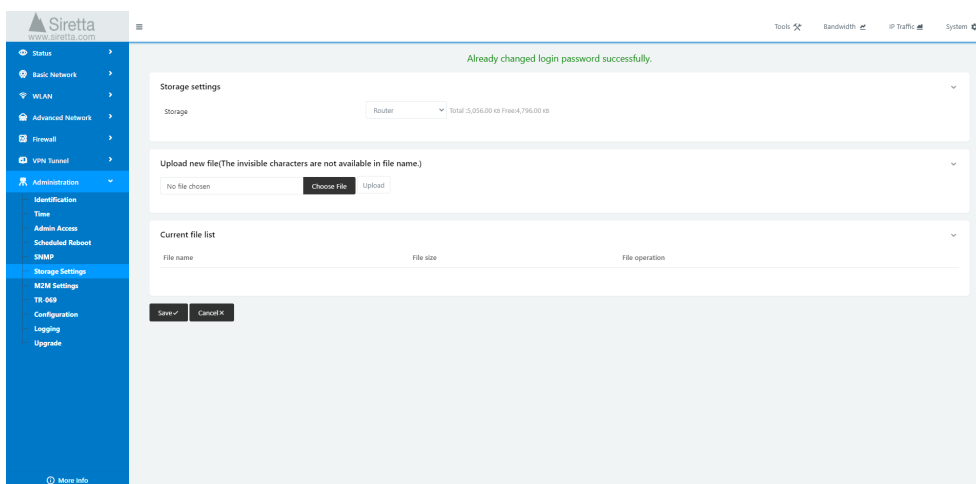


Table 56. Storage settings

Setting	Options
Storage	Always choose router. Removable devices are not supported.
Upload new file	Choose a file and click the upload button to upload it. <b>File names must never include spaces.</b>
Current File List	List of files stored on the QUARTZ-GOLD. Click the icons to the right of the file names to download or delete them.

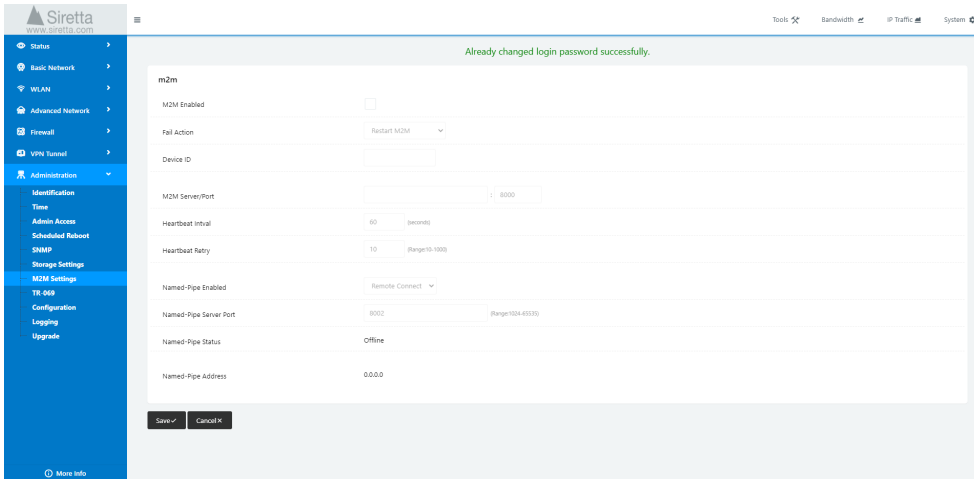
After making all required changes, click 'Save' to apply them.

### M2M Settings

Siretta offer a M2M portal to allow you to view and manage many routers from a cloud-based portal. Configure the settings to connect the QUARTZ-GOLD to this portal here.

**NOTE:** This is currently in Beta – please contact support for settings if you wish to try this out.

Figure 65. M2M settings



### TR-069

Configure TR-069 client for remote management settings here.

Figure 66. TR-069 settings

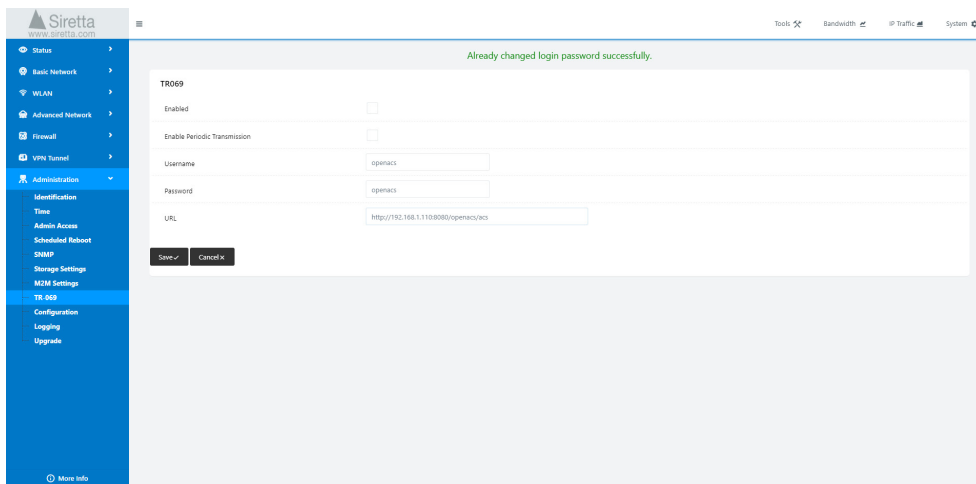


Table 57. TR-069 settings

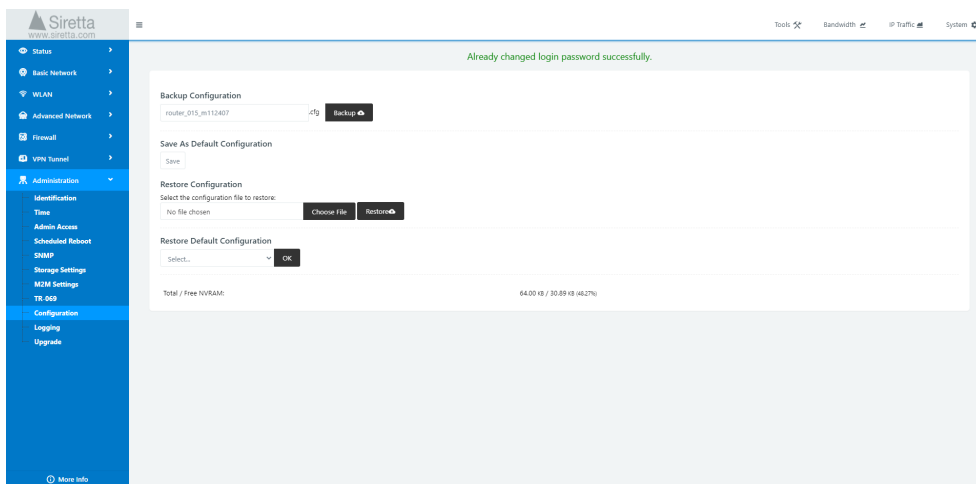
Setting	Options
Enabled	Check to enable TR-069
Enable Periodic Transmission	Check to enable periodic transmission
Username	Username as required for server
Password	Password as required for server
URL	URL and port of server

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

## Configuration

Backup and restore configurations here.

Figure 67. Configuration settings



### 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 whilst configurations are being experimented with and you need to 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.

### Logging

Status messages for debugging purposes can be logged by the QUARTZ-GOLD, 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.

Figure 68. Logging settings

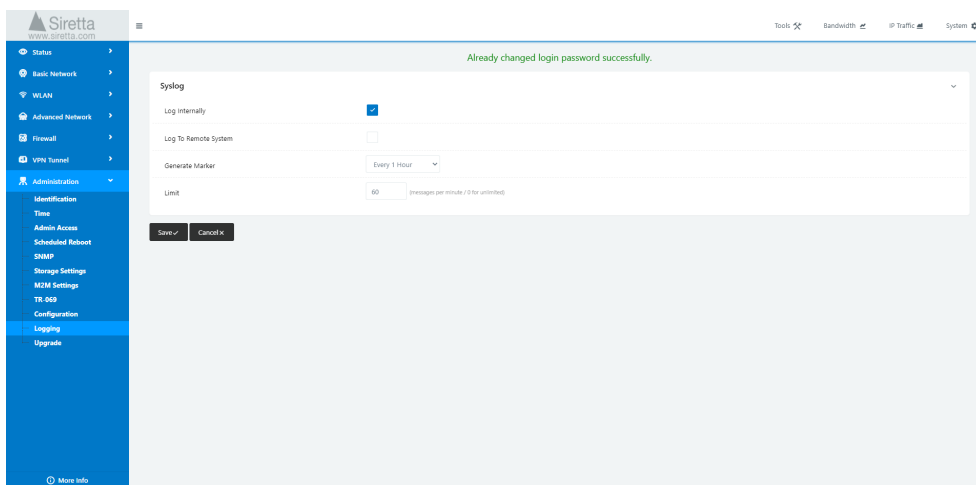


Table 58. Storage settings

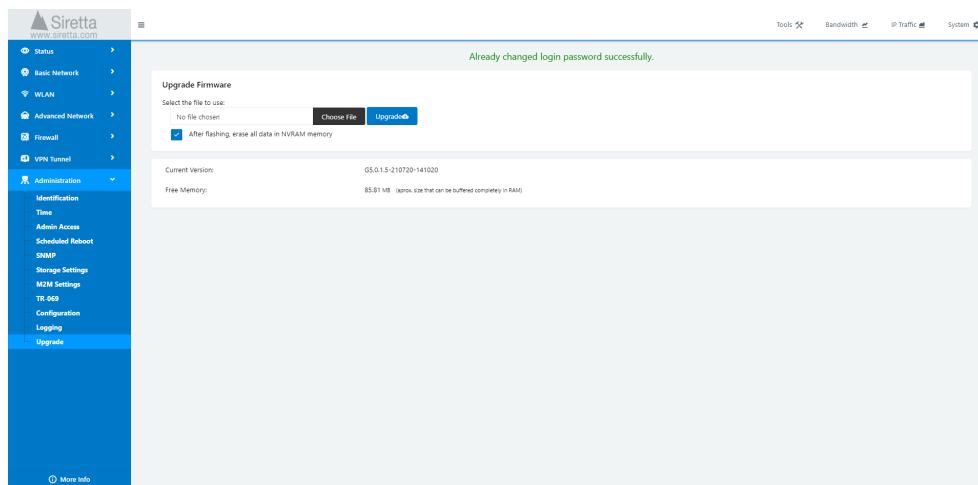
Setting	Options
Log Internally	Check to enable internal logging
Log to remote System	Check to enable external logging (and then enter target IP address and port)
Generate Marker	Choose marker insertion rate from drop down menu
Limit	Enter a limit to the number of messages/minute logged.

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

### Upgrade

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

Figure 69. Upgrade settings



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 you would like to preserve the configuration settings currently in the router. By default, the 'After flashing, erase all data in NVRAM memory' option is checked – you may wish to uncheck this.

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

Some firmware versions may alter the factory default settings. If possible, it is always wise to factory reset the QUARTZ-GOLD after a firmware update. This can be done either via the web interface of the router (Administration > Configuration, Restore Default Configuration), or by holding the reset pin in for at least 30 seconds after the router has been powered up and booted.

This upgrade page is where you can get the full firmware detail which is the version with date and time stamp.

# Copyright Information

## Copyright Declaration

© 2021 Siretta Ltd, all rights reserved

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without the written permission of Siretta Ltd.

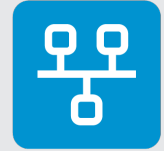
## Trademarks

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.

Wireshark is a registered trademark of the Wireshark Foundation.

All other trademarks are the property of their respective owners.





## Disclaimer

The information contained in this document is proprietary to Siretta Ltd. Siretta has made every effort to ensure that the accuracy of the information contained within this document is accurate. Siretta 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 by the use of this information.

Siretta does not take responsibility for any application developed using the router characterized in this document and notes that any application of this router 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.

All rights reserved.

© 2022 Siretta Ltd

## Definitions

Term	Definition		
4G	4th Generation Mobile Telecommunications	OSPF	Open Shortest Path First
APN	Access Point Name	PLMN	Public Land Mobile Network
ARP	Address Resolution Protocol	PPP	Point-to-Point
CIMI	Cloud Infrastructure Management Interface	PPPoE	Point-to-Point over Ethernet
CLI	Command Line Interface	PPTP	Point-to-Point Tunneling Protocol
DDNS	Dynamic Domain Name Systeem	QOS	Quality of Service
DHCP	Dynamic Host Configuration Protocol	Rx	Receive
DNS	Domain Name System	RTT	Round Trip Time
ECM	Enterprise Content Management	SIM	Subscriber Identity Module
GPS	Global Positioning System	SMS	Short Messaging Service
GRE	Generic Routing Encapsulation	SNMP	Simple Network Management Protocol
GUI	Graphical User Interface	SSID	Service Set Identifier
HTTP	Hypertext Transfer Protocol	T	Transmit
HTTPS	Hypertext Transfer Protocol Secure	TCP	Transmission Control Protocol
ICMP	Internet Control Message Protocol	TR-069	Technical Report 069
IP	Internet Protocol	TTL	Time to Live
IPSEC	Internet Protocol Security	UDP	User Datagram Protocol
L2TP	Layer 2 Tunneling Protocol	UPnP	Universal Plug and Play
LAN	Local Area Network	URL	Uniform Resource Locator
LTE	Long Term Evolution	VLAN	Virtual Local Area Network
M2M	Machine to Machine	VPN	Virtual Private Network
MRU	Maximum Receive Unit	VRRP	Virtual Router Redundancy Protocol
MTU	Maximum Transmission Unit	WAN	Wider Area Network
NAT-PMP	Network Address Translation - Port Mapping Protocol	WEP	Wired Equivalent Privacy
NMEA	National Marine Electronics Association	WLAN	Wireless Local Area Network
NTP	Network Time Protocol	WOL	Wake on LAN
		WPA	Wi-Fi Protected Access



Enabling Industrial IoT

**sales** +44 (0)118 976 9000

**email** [sales@siretta.com](mailto:sales@siretta.com)

**[www.siretta.com](http://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 1.2 - October 2022