



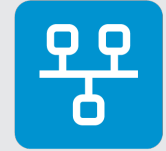
Enabling Industrial IoT



## QUARTZ-COMPACT

3G & 4G Single LAN Industrial Router Range

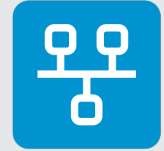
Software Manual  
Rev 1.2



# Table of Contents

	Page
<b>Introduction</b>	<b>3</b>
<b>About Siretta</b>	<b>4</b>
<b>General Description</b>	<b>5</b>
<b>Local Configuration</b>	<b>6</b>
<b>Basic Configuration</b>	<b>8</b>
Cellular Network Configuration	9
LAN Settings	11
Dynamic DNS Settings	12
Routing Settings	13
<b>Advanced Network</b>	<b>14</b>
Port Forwarding Settings	14
DMZ Settings	15
Triggered Settings	16
Firewall Settings	17
linkCONNECT Settings	18
UPnp/NAT-PMP Settings	20
Static DHCP Settings	21
<b>VPN Tunnel</b>	<b>22</b>
GRE Settings	22
VPN Client Settings	23

<b>Administration</b>	<b>25</b>
Identification Settings	25
Time Settings	26
Admin Access Settings	27
Schedule Reboot Settings	28
SNMP Settings	29
M2M Settings	30
System Log Settings	31
Upgrade Settings	32
System Reboot	32
<b>Debugging</b>	<b>33</b>
Logs Settings	33
Ping Settings	33
<b>Restore Factory Settings</b>	<b>34</b>
Via Web Interface	34
Via Router	35
<b>Appendix (For optional GPS feature ONLY)</b>	<b>36</b>
<b>Disclaimer</b>	<b>37</b>
<b>Definitions</b>	<b>38</b>



## Introduction

The QUARTZ-COMPACT Series is a range of UMTS / LTE routers enabling mobile broadband and machine to machine (M2M) industrial communication.

This document is aimed at providing guidance when configuring and using the QUARTZ-COMPACT Series router software.

Configuration of the QUARTZ-COMPACT router can be done via the web using any of the following: Internet Explorer, Firefox, or Chrome. Throughout this document, Internet Explorer 9.0 is used as the example browser.

## 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:

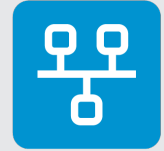
- » Cellular technologies: GSM/GPRS/3G/UMTS/4G/LTE & 5G NR, plus LTE CAT 1, LTE CAT M & LTE CAT NB-IoT
- » Global positioning: GPS/GNSS
- » WLAN/Wi-Fi

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.



## General Description

The Siretta QUARTZ-COMPACT router series is a range of high speed industrial cellular routers in a compact enclosure. The QUARTZ-COMPACT series is offered in 3G / WCDMA/UMTS and 4G / LTE forms giving reliable, secure and high speed wireless connectivity.

The QUARTZ-COMPACT router range has a number of standard options, such as GPS, and 1 x LAN interface. Additionally QUARTZ-COMPACT routers are available, as standard with or without an accessory kit comprising: cellular antennas, PSU and LAN cable.

VPN features can also be configured in the QUARTZ-COMPACT routers, enabling utilization of a virtual private network service through a 3G wireless router designed for the stresses and workload of a modern industrial or commercial environment.

The QUARTZ-COMPACT router series is a high build quality range of routers designed for use in industrial environments needing high performance and a robust hard enclosure as standard. The QUARTZ-COMPACT range is designed for remote management, telemetry, condition monitoring, CCTV, ATMs, vending machine and other M2M applications.

Its compact small size design, enables the QUARTZ-COMPACT router to easily be embedded into other equipment or systems. With the GPS option, the QUARTZ-COMPACT router is ideal for fleet tracking or access management.

## Local Configuration

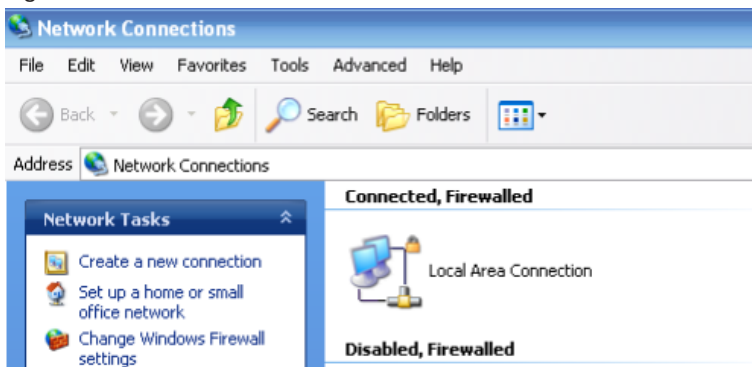
The QUARTZ-COMPACT Series router supports configuration by local Ethernet port, you can specify a static IP or DHCP get IP for your computer.

Default IP address: 192.168.1.1  
subnet mask: 255.255.255.0

Follow the steps below to configure your router locally:

**Step 1.** Click “Start > Control Panel”, find the “Network Connections” icon and double click it to enter. Select “Local Area Connection” corresponding to the network card. (See figure 1 below)

Figure 1. Network connection



**Step 2.** Obtain an IP address automatically or set up IP address as: 192.168.1.xxx

**NOTE** - XXX can be any number between 2~254

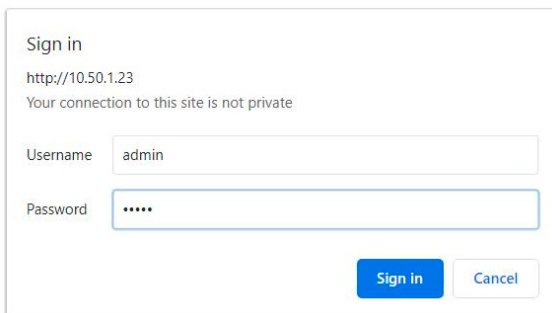
**Step 3.** Open Internet Explorer and visit “<http://192.168.1.1/>”, to enter identify page.

**Step 4.** User should use the default user name and password when logging in for the first time.

**Username:** admin

**Password:** admin

Figure 2. User identify interface



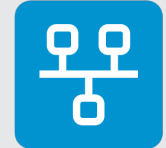
Sign in

http://10.50.1.23

Your connection to this site is not private

Username

Password



## QUARTZ-COMPACT

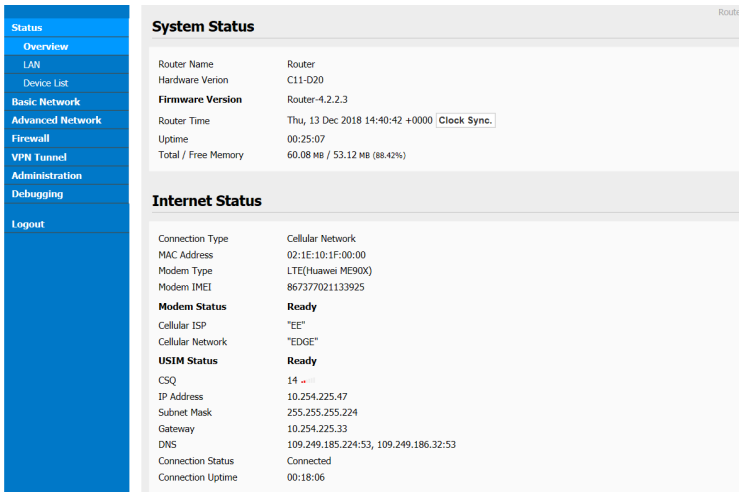
### Software Manual

## Basic Configuration

Different software versions have different web configuration interfaces, in this example we use version 2.6.0.

After visiting the web interface, you can check the current status of the router or modify the router configuration via the web interface. Below is the interface displaying the routers standard settings.

Figure 3. Router status GUI



The screenshot displays the Router status GUI. On the left is a blue sidebar menu with options: Status, Overview, LAN, Device List, Basic Network, Advanced Network, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main content area is titled 'Router' and contains two sections: 'System Status' and 'Internet Status'.

**System Status**

Router Name	Router
Hardware Verion	C11-D20
<b>Firmware Version</b>	Router-4.2.2.3
Router Time	Thu, 13 Dec 2018 14:40:42 +0000 <a href="#">Clock Sync.</a>
Uptime	00:25:07
Total / Free Memory	60.08 MB / 53.12 MB (88.42%)

**Internet Status**

Connection Type	Cellular Network
MAC Address	02:1E:10:1F:00:00
Modem Type	LTE(Huawei ME909)
Modem IMEI	867377021133925
<b>Modem Status</b>	<b>Ready</b>
Cellular ISP	"EE"
Cellular Network	"EDGE"
<b>USIM Status</b>	<b>Ready</b>
CSQ	14
IP Address	10.254.225.47
Subnet Mask	255.255.255.224
Gateway	10.254.225.33
DNS	109.249.185.224:53, 109.249.186.32:53
Connection Status	Connected
Connection Uptime	00:18:06



## Cellular Network Configuration

**Step 1.** Select “Basic Network > Cellular” here you can modify cellular and SIM parameters according to your application.

Figure 4. Cellular settings

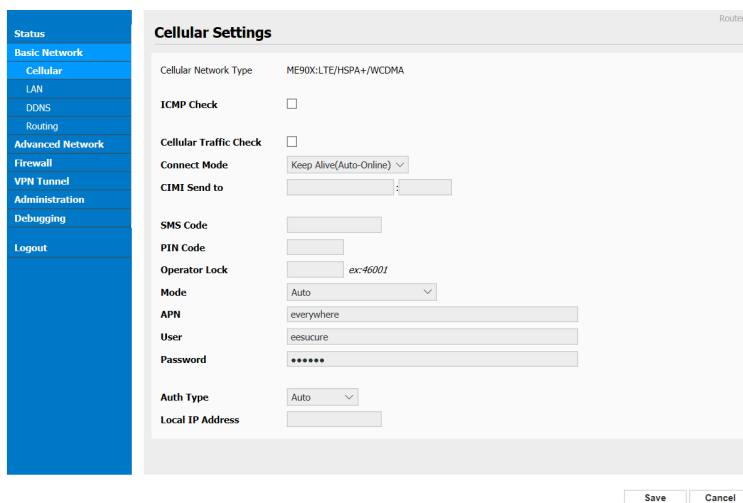


Table 1. Cellular instruction

Parameter	Instruction
ICMP check	To enable or disable ICMP check rules. Enable the ICMP check and setup a reachable IP address as destination IP. Once ICMP check failed, router will switch SIM card.
CSQ limit	
SMS password	
PIN code	Input SIM card PIN code if SIM is setup PIN by ISP
Cellular mode	
APN	APN provided by local ISP, usually CDMA/EVDO network do not need this parameter
User	SIM card username is provided by ISP

Table 1 (continued). Cellular instruction

Parameter	Instruction
Password	SIM card password is provided by ISP
Auth. type	
Use local IP addr.	

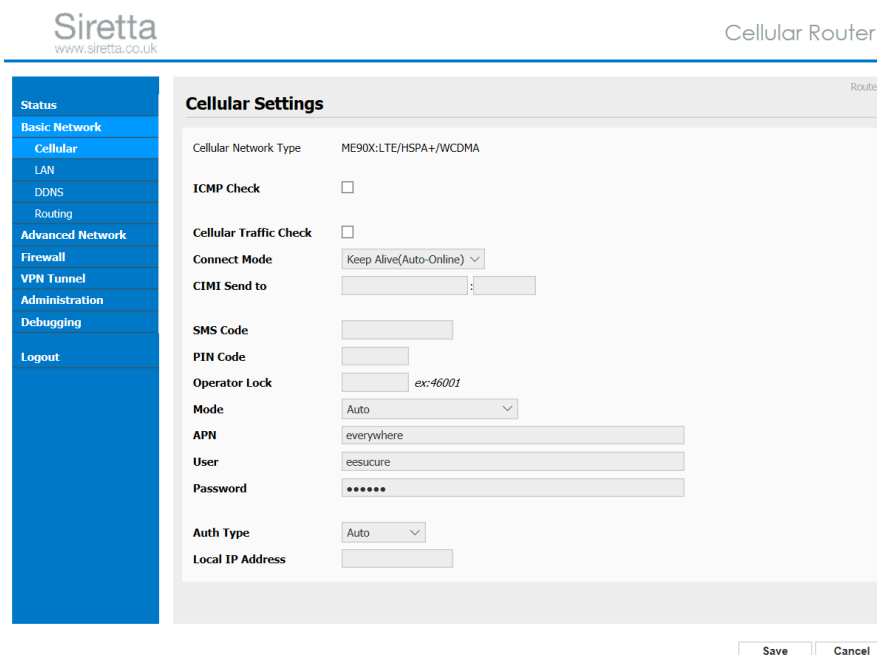
**After all settings have been configured, click the “Save” icon.**

### ICMP Check

Enabling ICMP on the router will automatically check whether the defined IP address is reachable every 60s. If the IP address is unreachable and ICMP check is timed out at the first check, it will make two further attempts at 3s intervals. If the IP address is still unreachable after the third attempt the router will implement the configured fail action.

The Check IP is a public IP or company server IP address.

Figure 5. ICMP



The screenshot shows the Siretta Cellular Router configuration interface. On the left is a navigation menu with options: Status, Basic Network, Cellular (selected), LAN, DDNS, Routing, Advanced Network, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main panel is titled 'Cellular Settings' and contains the following fields:

- Cellular Network Type: ME90X/LTE/HSPA+/WCDMA
- ICMP Check: ☐
- Cellular Traffic Check: ☐
- Connect Mode: Keep Alive(Auto-Online) (dropdown)
- CIMI Send to: [text input] : [text input]
- SMS Code: [text input]
- PIN Code: [text input]
- Operator Lock: [text input] ex:46001
- Mode: Auto (dropdown)
- APN: everywhere
- User: eesecure
- Password: [password input]
- Auth Type: Auto (dropdown)
- Local IP Address: [text input]

At the bottom right of the settings panel are 'Save' and 'Cancel' buttons.

## LAN Settings

Step 1. Select “Basic Network > LAN” to enter LAN settings page.

Figure 6. LAN setting GUI

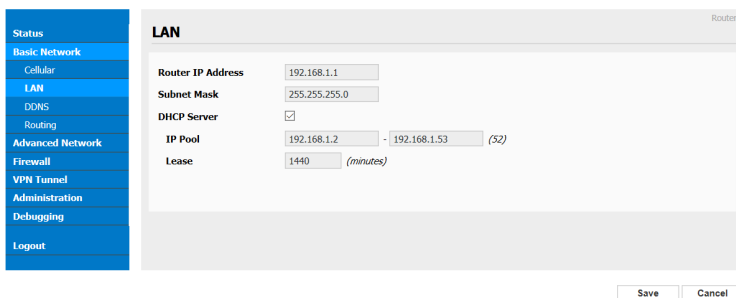


Table 2. LAN settings instruction

Parameter	Instruction
Router IP address	Router IP address, default IP is 192.168.1.1
Subnet mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enabled it will show the IP address range and lease options
IP address range	IP address range within LAN
Lease	The valid time

**After all settings have been configured, click the “Save” icon.**

## Dynamic DNS Settings

Step 1. Select “Basic Network > DDNS” to enter the DDNS settings page.

Figure 9. Dynamic DNSS settings

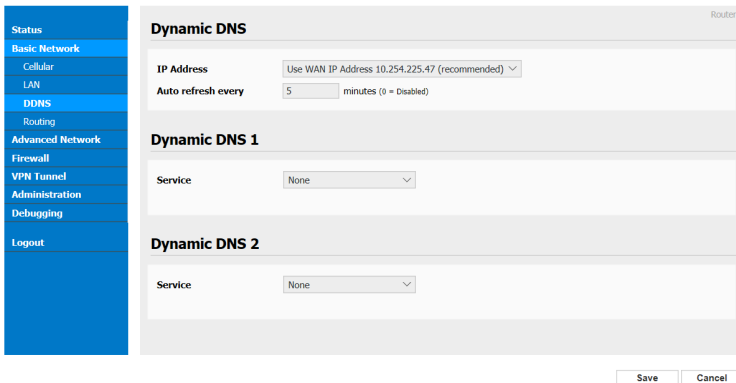


Table 3. DDNS settings instruction

Parameter	Instruction
IP address	Use default IP 0.0.0.0. For customized protocol, please contact Siretta representative.
Auto refresh time	Set the interval refresh of the DDNS client to 240s or above
Service provider	Select the DDNS service provider listed

**After all settings have been configured, click the “Save” icon.**

## Routing Settings

Step 1. Select “Basic Network > Routing” to enter the Routing settings page.

Figure 10. Routing settings

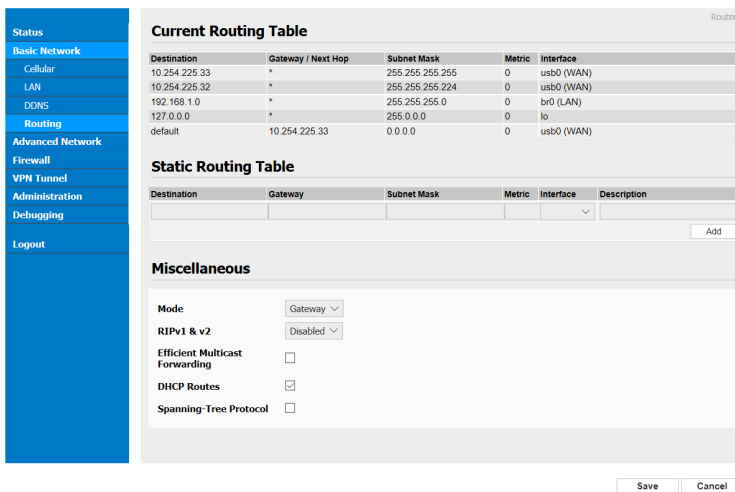


Table 4. Routing settings instruction

Parameter	Instruction
Destination	Router can reach the destination IP address
Gateway	Next hop IP address which the router will reach
Subnet Mask	Subnet mask for destination IP address
Metric	Metrics are used to determine whether one particular route should be chosen over another
Interface	Interface from router to gateway
Description	Describe routing name

**After all settings have been configured, click the “Save” icon.**

# Advanced Network

## Port Forwarding Settings

**Step 1.** Select “Advanced Network > Port Forwarding” to enter the port forwarding settings. You can modify the router name, host name and domain name according to the application requirement.

Figure 14. Port forwarding settings

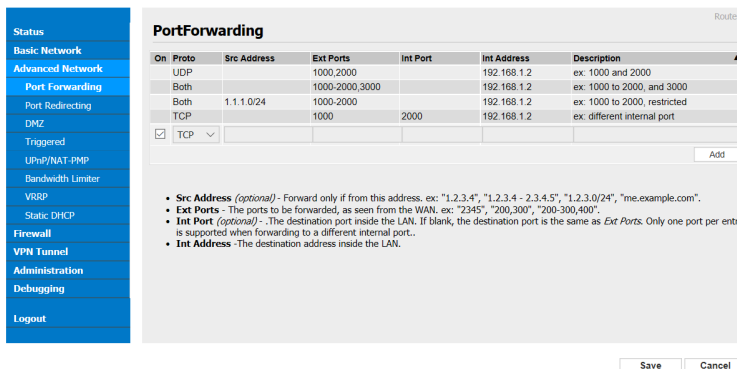


Table 7. Port forwarding settings instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Src. Address	Source IP address. Forward only if from this address.
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.
Int. Port	Internal port. 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	Internal Address. Destination address inside the LAN.
Description	Remark the rule

**After all settings have been configured, click the “Save” icon.**

## DMZ Settings

Step 1. Select “Advanced Network > DMZ” to enter the DMZ settings.

Figure 15. DMZ settings

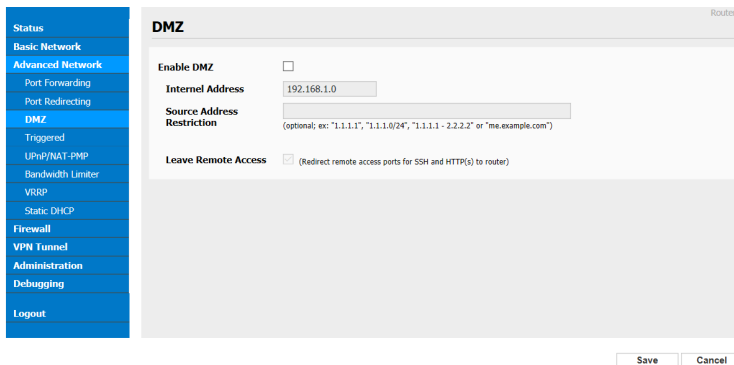


Table 8. DMZ settings instruction

Parameter	Instruction
Destination Address	Destination address inside the LAN
Source Address Restriction	If there is no IP address here, it will allow access to all IP address. If an IP address is defined, access will be allowed to this IP address only.
Leave Remote Access	Leave remote access

After all settings have been configured, click the “Save” icon.

## Triggered Settings

Step 1. Select “Advanced Network > Triggered” to enter the triggered settings.

Figure 16. Triggered settings

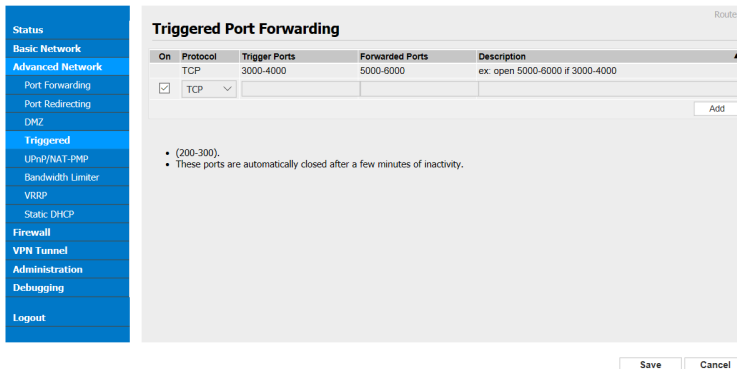


Table 9. Triggered settings instruction

Parameter	Instruction
Protocol	Supports UDP, TCP, both UDP and TCP
Triggered Ports	Trigger ports are the initial LAN to WAN “trigger”
Transferred Ports	Transferred ports are the WAN to LAN ports that are opened if the “trigger” is activated
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic

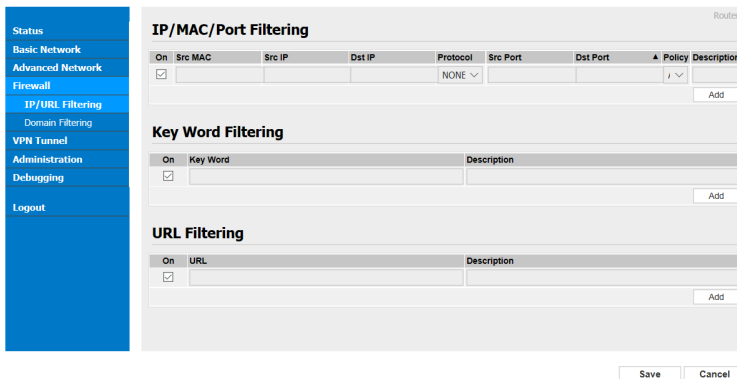
**After all settings have been configured, click the “Save” icon.**



## Firewall Settings

Step 1. Select “Advanced Network > Firewall” to enter the firewall settings.

Figure 17. Firewall settings



**IP/MAC/Port Filtering**

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NONE				

**Key Word Filtering**

On	Key Word	Description
<input checked="" type="checkbox"/>		

**URL Filtering**

On	URL	Description
<input checked="" type="checkbox"/>		

Save Cancel

### linkCONNECT Settings

Step 1. Select “Advanced Network > linkCONNECT” to enter the linkCONNECT settings.

Figure 18. linkCONNECT settings

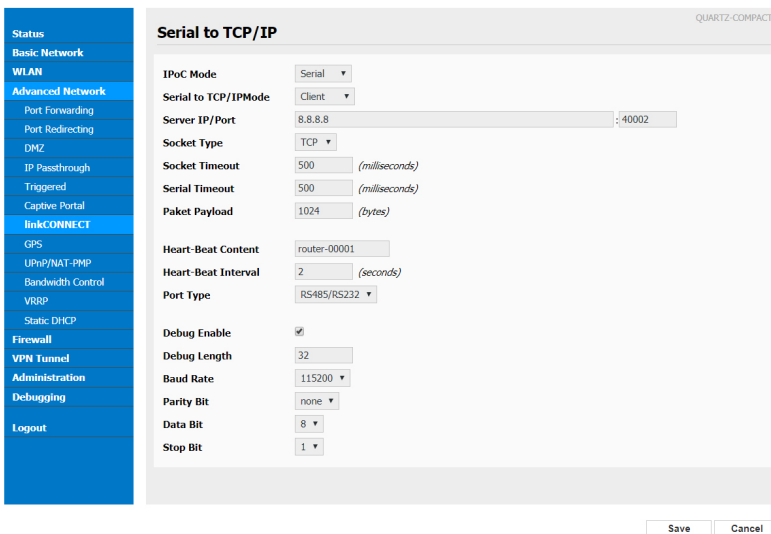
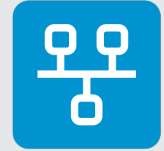


Table 10. linkCONNECT settings instruction

Parameter	Instruction
Serial to TC/IP mode	Disable, Server and Client mode
Server IP/Port	IP address and domain name for Server IP
Socket Type	TCP/UDP protocol
Socket Timeout	Setting time to transmit data to serial port
Serial Timeout	Serial timeout is the waiting time for transmitting a data packet. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.
Heart-beat Content	Send heart beat to the defined server to keep router online. It is convenient to monitor the router from the server.



## QUARTZ-COMPACT

Software Manual

Table 10 (continued). linkCONNECT settings instruction

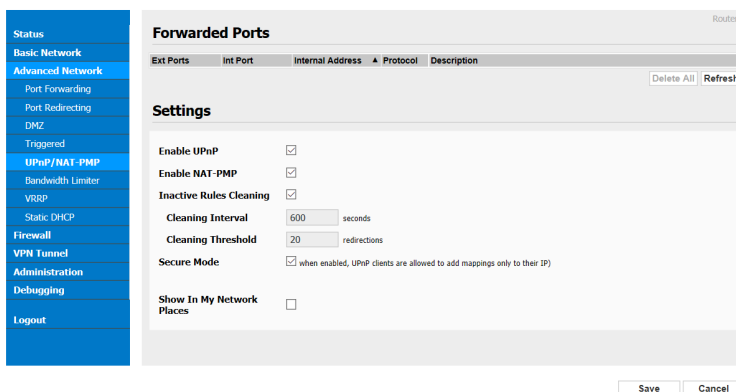
Parameter	Instruction
Heart beat Interval	Heart beat interval time
Baud Rate	112100 as default
Parity Bit	None as default
Data Bit	8bit as default
Stop Bit	1bit as default

**After all settings have been configured, click the “Save” icon.**

## UPnp/NAT-PMP Settings

Step 1. Select “Advanced Network > Upnp/NAT-PMP” to enter the Upnp/NAT-PMP settings.

Figure 19. Upnp/NAT-PMP settings



The screenshot shows the 'UPnP/NAT-PMP' settings page. The left sidebar contains a navigation menu with the following items: Status, Basic Network, Advanced Network (selected), Port Forwarding, Port Redirecting, DMZ, Triggered, UPnP/NAT-PMP (selected), Bandwidth Limiter, VRRP, Static DHCP, Firewall, VPN Tunnel, Administration, Debugging, and Logout. The main content area is titled 'Forwarded Ports' and 'Settings'. The 'Settings' section includes the following options:

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

At the bottom of the settings area are 'Save' and 'Cancel' buttons.

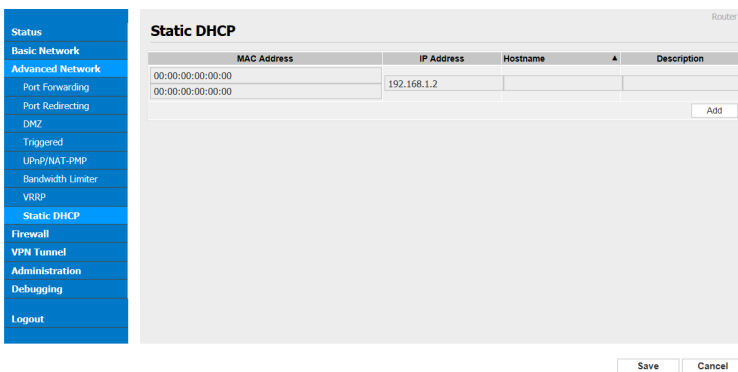
After all settings have been configured, click the “Save” icon.

**NOTE** - linkCONNECT and GPS are not available simultaneously on QUARTZ-COMPACT

### Static DHCP Settings

Step 1. Select “Advanced Network > Static DHCP” to enter the static DHCP settings.

Figure 20. Static DHCP settings



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

Save Cancel

After all settings have been configured, click the “Save” icon.

# VPN Tunnel

## GRE Settings

Step 1. Select “VPN Tunnel > GRE” to enter the GRE settings.

Figure 21. GRE settings

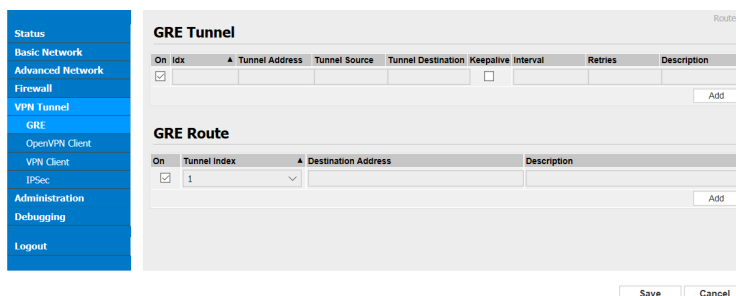


Table 11. GRE settings instruction

Parameter	Instruction
Remote IP Address	GRE peer IP address. Usually a public IP address.
Local IP Address	Local IP address for LAN
Tunnel Local IP Address	GRE Tunnel local IP address which is a virtual IP address
Remote LAN IP Address	GRE Tunnel remote IP address which is a virtual IP address
ICMP Check IP Address	Checks the IP address is reachable. If ICMP check is failed, GRE will be established again.

**After all settings have been configured, click the “Save” icon.**

## VPN Client Settings

Step 1. Select “VPN Tunnel > VPN Client” to enter the VPN client settings.

Figure 20. VPN client settings

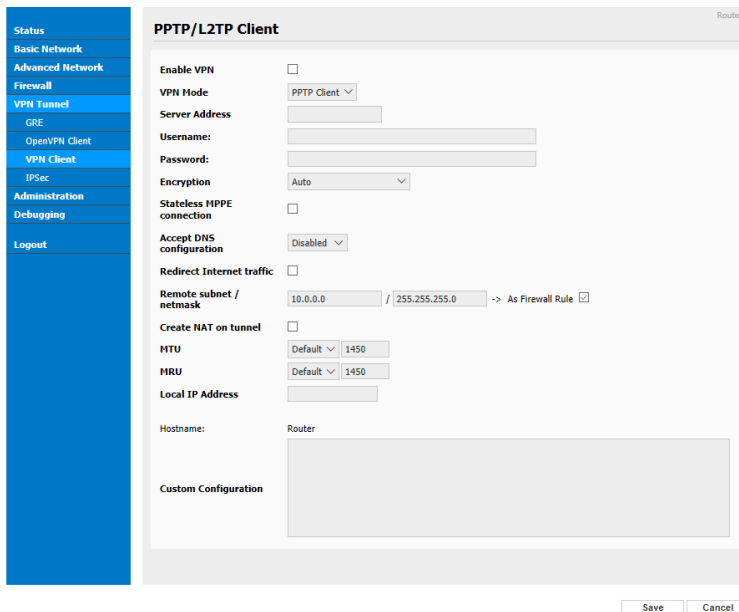


Table 12. VPN client settings instruction

Parameter	Instruction
VPN Mode	VPN Mode for PPTP and L2TP
Server Address	VPN Server IP address
User name	As the configuration requested
Password	As the configuration requested
Encryption	As the configuration requested
Stateless MPPE	As the configuration requested
Accept DNS	As the configuration requested

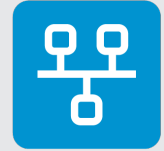


Table 12 (continued). VPN client settings instruction

Parameter	Instruction
Remote Subnet	As the configuration requested
Create NAT on Tunnel	As the configuration requested



# Administration

## Identification Settings

**Step 1.** Select “Administrator > Identification” to enter the router identification settings. Here you can modify the router name, host name and domain name according to your requirements.

Figure 21. Router identification settings

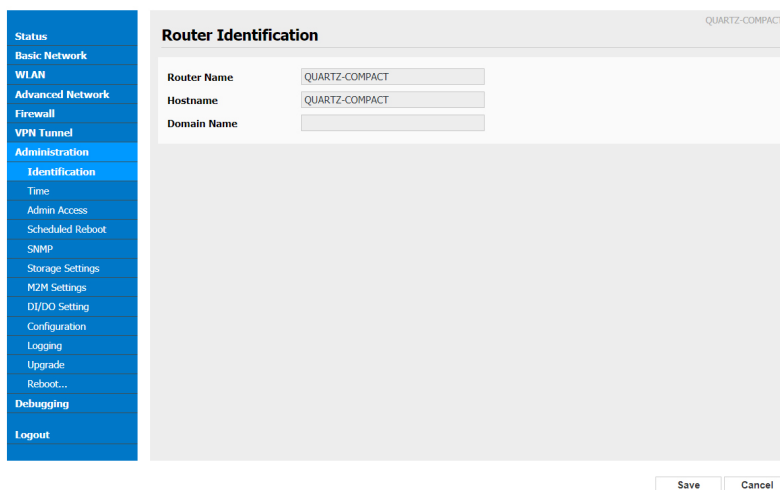


Table 13. Router identification settings instruction

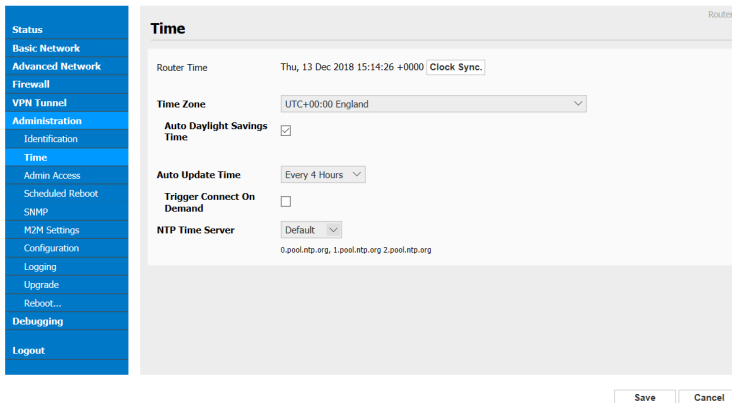
Parameter	Instruction
Router Name	Default is router. Can be customised, maximum 32 characters.
Host Name	Default is router. Can be customised, maximum 32 characters.
Domain Name	Default is empty. Can be customised, maximum 32 characters. This is the domain name for the WAN, it will only need to be configured in WAN applications.

**After all settings have been configured, click the “Save” icon.**

## Time Settings

Step 1. Select “Administrator > Time” to enter the time settings.

Figure 22. Time settings



After all settings have been configured, click the “Save” icon.

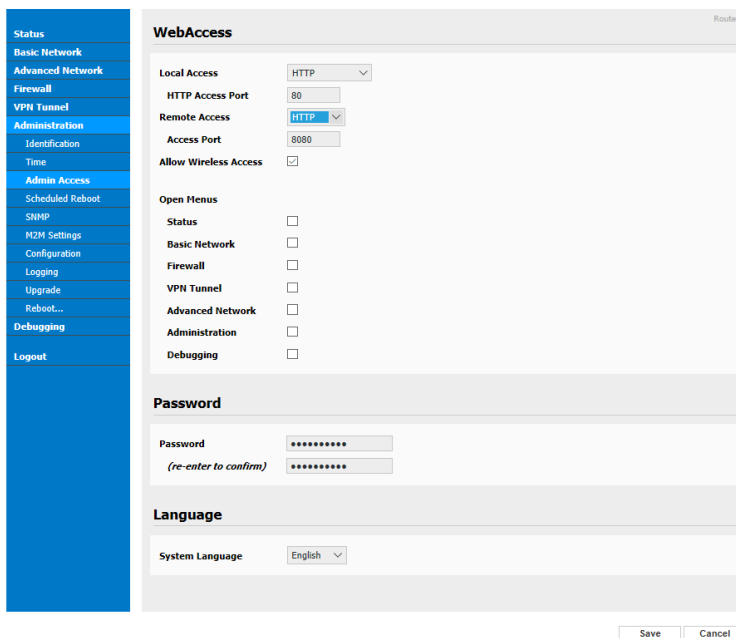
**NOTE** - If the device is online but time update fails, try another NTP time server.

### Admin Access Settings

Step 1. Select “Administrator > Admin Access” to enter the admin settings. Here, you can configure the basic web parameters enabling it to be more convenient for your usage.

**NOTE** - The password is the router system account password.

Figure 23. Admin settings



**WebAccess**

Local Access: HTTP (dropdown), HTTP Access Port: 80 (text box)

Remote Access: HTTP (dropdown), Access Port: 8080 (text box)

Allow Wireless Access: ☒

**Open Menus**

- Status: ☐
- Basic Network: ☐
- Firewall: ☐
- VPN Tunnel: ☐
- Advanced Network: ☐
- Administration: ☐
- Debugging: ☐

**Password**

Password: [masked], (re-enter to confirm): [masked]

**Language**

System Language: English (dropdown)

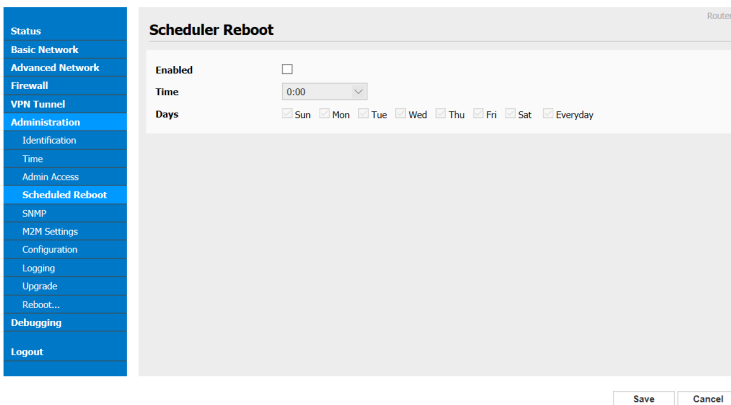
Save Cancel

After all settings have been configured, click the “Save” icon.

## Schedule Reboot Settings

Step 1. Select “Administrator > Scheduled Reboot” to enter the reboot settings.

Figure 24. Reboot settings

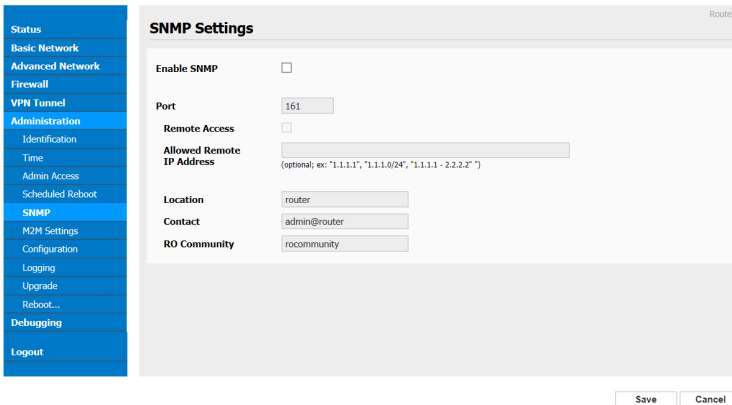


After all settings have been configured, click the “Save” icon.

## SNMP Settings

Step 1. Select “Administrator > SNMP” to enter the SNMP settings.

Figure 25. SNMP settings



**SNMP Settings**

Router

Enable SNMP ☐

Port

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")

Location

Contact

RO Community

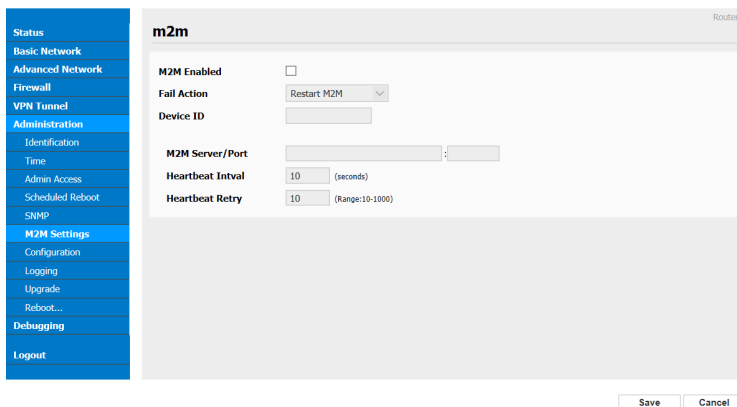
Save Cancel

After all settings have been configured, click the “Save” icon.

## M2M Access Settings

Step 1. Select “Administrator > M2M Settings” to enter the SNMP settings.

Figure 26. M2M access settings

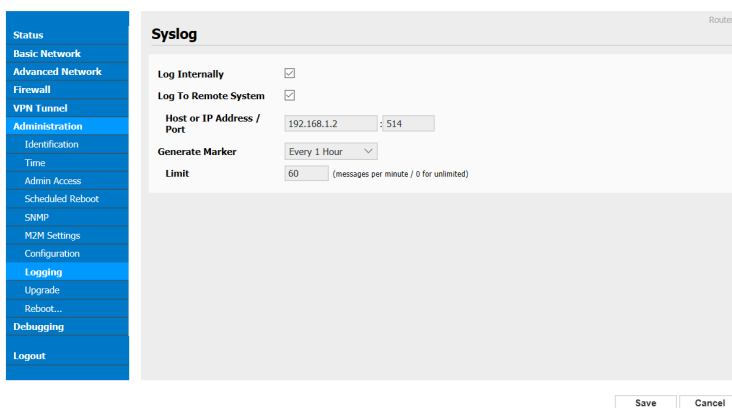


After all settings have been configured, click the “Save” icon.

## System Log Settings

Step 1. Select “Administrator > Logging” to enter the logging settings. Here you can select the save path for any backed up configurations. (Local or remote server)

Figure 31. Log settings



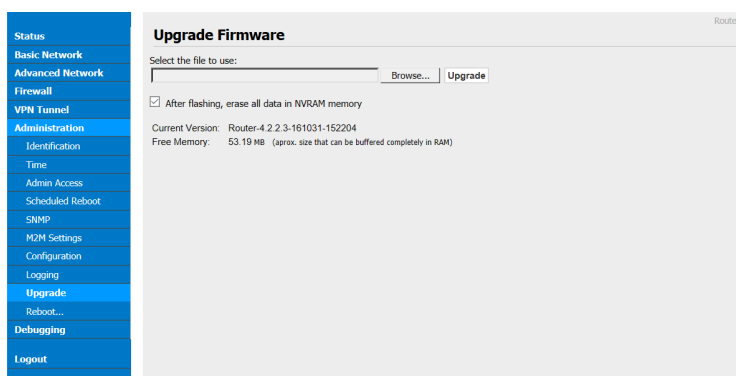
After all settings have been configured, click the “Save” icon.

## Upgrade Settings

Step 1. Select “Administrator > Upgrade” to enter the upgrade firmware settings.

**NOTE** - When upgrading the firmware, do not remove power.

Figure 32. Upgrade firmware settings



After all settings have been configured, click the “Save” icon.

## System Reboot

Step 1. Select “Administrator > Reboot” to reboot the router. A popup will appear, prompting ‘YES’ or ‘NO’ to continue with the reboot.

Step 2: If you select ‘YES’, the system will reboot. All relevant firmware upgrades will be effective after the reboot.

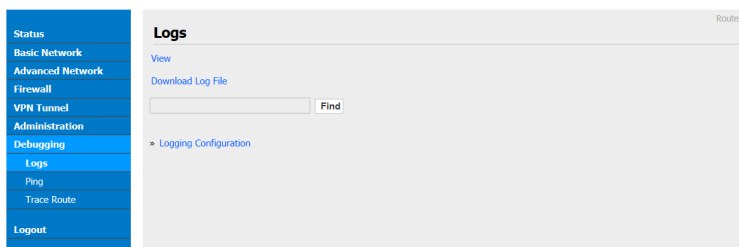


# Debugging

## Logs Settings

Step 1. Select “Debugging > Logs” to enter the log settings.

Figure 33. Log settings

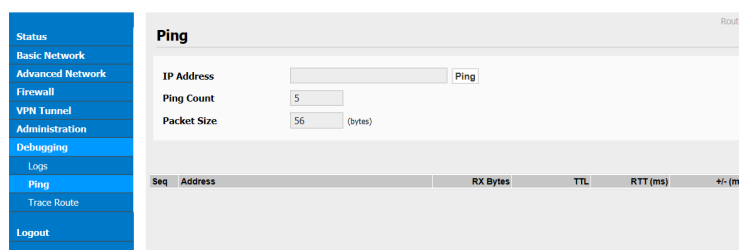


After all settings have been configured, click the “Save” icon.

## Ping Settings

Step 1. Select “Debugging > Ping” to enter the ping settings.

Figure 34. Ping settings



After all settings have been configured, click the “Save” icon.

# Restore Factory Settings

## Via Web Interface

If you want to restore factory settings on your router, this can be done on the web interface by selecting “**Administration > Configuration**”. Select “**Restore Configuration**” this will restore your router to it factory settings.

Figure 35. Restore configuration



The screenshot shows the Siretta web interface. On the left is a navigation menu with options: Status, Basic Network, Advanced Network, Firewall, VPN Tunnel, Administration, Identification, Time, Admin Access, Scheduled Reboot, SNMP, M2M Settings, Configuration, Logging, Upgrade, Reboot..., Debugging, and Logout. The 'Configuration' option is highlighted. The main content area is titled 'Router' and contains three sections: 'Backup Configuration' (with a text field 'Router\_Router-4223\_m17209D', a '.cfg' file type, and a 'Backup' button), 'Restore Configuration' (with a 'Select the configuration file to restore:' label, a 'Browse...' button, and a 'Restore' button), and 'Restore Default Configuration' (with a 'Select...' dropdown and a 'Save' button). A blue arrow points from the 'Restore' button to the text 'Click here to restore factory settings'.

### Via Router

To restore the routers factory settings, press and hold the reset button on the router located near the power connector. Press and hold the reset button for at least 5 seconds, this can be done when the router is either in use or turned on. Reset is successful when the NET light stops blinking. The router will now be restored to factory settings.

Figure 36. Reset button on router

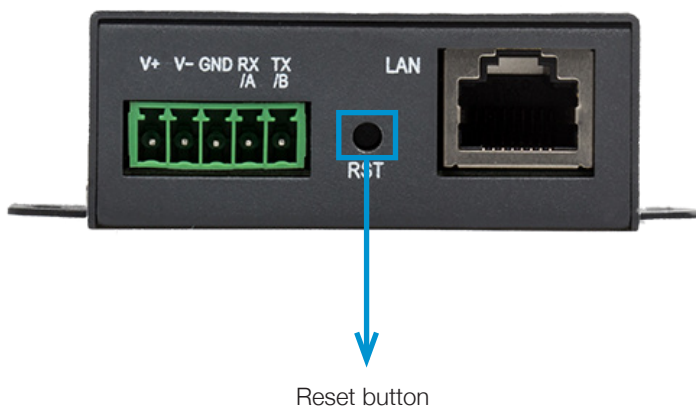


Table 14. Factory settings

Parameter	Default settings
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin

## Appendix (For optional GPS feature only)

Step 1. Select “Advanced Network > GPS” to enter the GPS settings.

Figure 37. GPS settings

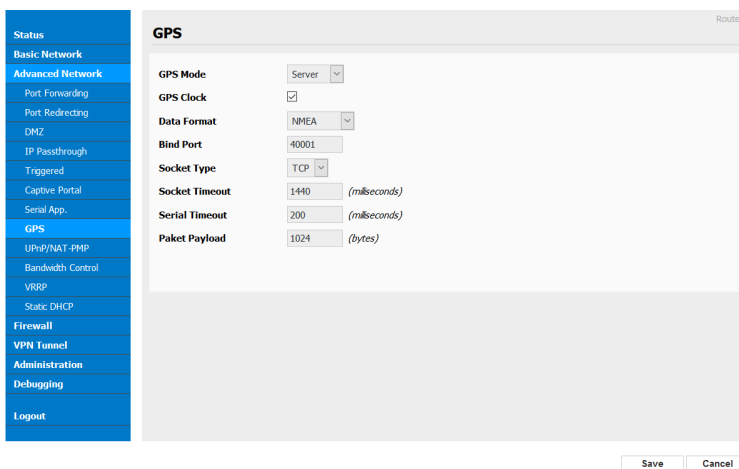


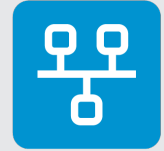
Table 15. GPS settings

Parameter	Instruction
Bind Port	Local port for GPS data.
Socket type	GPS data protocol.
Socket Timeout	The timeout for socket connection. If socket is not established, it will reconnect after the timeout time.
Serial Timeout	The time is defined by serial port buffer. After the time, router will send GPS to server.
Packet Payload	The max packet for GPS data.

**After all settings have been configured, click the “Save” icon.**

**NOTE** - GPS data format: dtu.heartbeat.content,gps\_date, gps\_time, gps\_use, gps\_latitude, gps\_NS, gps\_longitude, gps\_EW, gps\_speed, gps\_degrees, gps\_FS, gps\_HDOP, gps\_MSL

e.g. Router\_00001,083238,120313,12,2230.31563,N,11355.02863,E



## Disclaimer

The information contained in this document is proprietary to Siretta. 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.

© 2019 Siretta Ltd

## Definitions

Term	Definition		
3G	3rd Generation Mobile Telecommunications	SMS	Short Message Service
4G	4th Generation Mobile Telecommunications	SNMP	Simple Network Management Protocol
APN	Access Point Name	TCP	Transmission Control Protocol
DDNS	Dynamic Domain Name System	UDP	User Datagram Protocol
DHCP	Dynamic Host Configuration Protocol	UMTS	Universal Mobile Telecommunications System
DI	Direct Input	UPnP	Universal Plug and Play
DMZ	Demilitarized Zone	VPN	Virtual Private Network
DNS	Domain Name System	WAN	Wide Area Network
DO	Direct Output	WLAN	Wireless Local Area Network
GND	Ground		
GPS	Global Positioning System		
GUI	Graphical User Interface		
I/O	Input/Output		
ICMP	Internet Control Message Protocol		
IP	Internet Protocol		
ISP	Internet Service Provider		
LAN	Local Area Network		
LTE	Long-Term Evolution		
M2M	Machine to Machine		
MPPE	Microsoft Point-to-Point Encryption		
NAT	Network Address Translation		
NTP	Network Time Protocol		
PMP	Port Mapping Protocol		
SIM	Subscriber Identity Module		



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