

USER GUIDE

SABRE™ RANGER 5000

Version : 1.0 (draft)

Date : 11 Sep 2017

USER GUIDE

Contents

| | |
|--|----|
| Copyright | 3 |
| Warranty | 3 |
| Trademarks | 3 |
| Regulatory Information | 3 |
| 1. Introduction | 6 |
| 2. Quick Reference | 7 |
| 3. Install the Sim Card | 8 |
| 4. Connect the Cables and Wires | 10 |
| 5. Optional Accessories | 18 |
| 6. Fix Optional Mounting Bracket to Sabre™ Ranger 5000 | 19 |
| 7. Mount the Terminal on a Pole | 20 |
| 8. Terminal Grounding | 22 |
| 9. Point the Antenna | 23 |
| 10. Navigate to the Web Console | 25 |
| 11. Web Console | 29 |
| 11.1 Data | 31 |
| 11.1.1 Data Profile | 31 |
| 11.1.2 Firewall | 32 |
| 11.1.3 Port Forwarding | 35 |
| 11.1.4 Data Settings | 36 |
| 11.2 SMS | 37 |
| 11.2.1 Compose | 37 |
| 11.2.2 Inbox | 38 |
| 11.2.3 Sent | 39 |
| 11.2.4 Draft | 39 |
| 11.3 Settings | 40 |
| 11.3.1 Accounts | 40 |
| 11.3.2 Ethernet | 41 |
| 11.3.3 Security | 42 |
| 11.3.4 Terminal Settings | 43 |
| 11.3.4.1 Reboot Terminal | 43 |
| 11.3.4.2 Factory Reset | 43 |
| 11.3.4.3 Firmware Upgrade | 44 |
| 11.3.4.4 Remote Access | 45 |
| 11.3.4.4 Power Saving | 46 |
| 11.3.4.5 CIPHERING | 47 |
| 11.3.4.6 Facility Lock | 47 |
| 11.3.4.7 IP Watchdog | 48 |
| 11.3.4.8 I/O Configurations | 49 |
| 11.3.4.9 Backup/Restore | 53 |
| 11.3.4.10 Web | 54 |
| 11.3.4.11 Antenna Pointing Buzzer | 54 |
| 11.3.4.12 GNSS Selection | 55 |
| 11.3.5 Terminal Info | 56 |
| 11.3.6 SMS Configurations | 57 |
| 11.3.7 Language | 57 |
| 11.3.8 Support | 57 |
| 11.3.9 About | 57 |
| 12. Web Console in Safe Mode | 58 |
| 13. Appendix A: Terminal Block Pin Assignment | 60 |
| 14. Appendix B: Conduit & Accessories | 62 |
| 15. Appendix C: Technical Summary | 63 |
| 16. Appendix D: Backup Configuration Reference Table | 65 |

USER GUIDE

Copyright

© Copyright 2017 Addvalue Innovation Pte Ltd

All rights reserved. This publication and its contents are proprietary to Addvalue Innovation Pte Ltd. No part of this publication may be reproduced in any form or by any means without the written permission of Addvalue Innovation Pte Ltd., 8 Tai Seng Link, Level 5 (Wing 2) Singapore 534158.

Warranty

Addvalue Innovation Pte Ltd has made every effort to ensure the correctness and completeness of the material in this document. Addvalue Innovation Pte Ltd shall not be liable for errors contained herein. The information in this document is subject to change without notice. Addvalue Innovation Pte Ltd makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

All trademarks, marks, names, or product names referenced in this publication are the property of their respective owners. Addvalue Innovation Pte Ltd neither endorses nor otherwise sponsors any such products or services referred to herein. SABRE™ RANGER 5000 is a trademark of Addvalue Innovation Pte Ltd.

Microsoft, Windows, Windows NT, Windows 2000, Windows XP, and Windows 7 are registered trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

INMARSAT is a trademark of the International Mobile Satellite Organization. The Inmarsat LOGO and the trademark BGAN are trademarks of Inmarsat (IP) Company Limited. All trademarks are licensed to Inmarsat Limited.

All other company and product names may be the registered trademarks or trademarks of their respective owners.

Regulatory Information



FEDERAL COMMUNICATION COMMISSION NOTICE

FCC Identifier: XXX-XXXXXXX

USE CONDITIONS:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

USER GUIDE

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IMPORTANT NOTE: EXPOSURE TO RADIO FREQUENCY RADIATION

This Device complies with FCC & IC radiation exposure limits set forth for an uncontrolled environment. The Antenna used for this transmitter must be installed to provide a separation distance of at least 100cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC CAUTION:

Any Changes or modifications not expressly approved by the manufacturer could void the user's authority, which is granted by FCC to operate this satellite terminal, SABRE™ RANGER 5000.

INDUSTRY CANADA STATEMENT**ICC Identifier: XXXXX-XXXXXXXX**

This device complies with Radio standard specification RSS -170 of Industry Canada Rules.

The operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: RADIATION EXPOSURE STATEMENT

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This antenna used for this transmitter must be installed to provide a separation distance of at least 100cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

USER GUIDE

CE RED DECLARATION OF CONFORMITY

The **CE RED Declaration of Conformity** for the Sabre™ Ranger 5000 terminal will be added on this page after completing the upgrade process of the CE RED tests.

Mobile Earth Stations (MES) 1668 – 1670 MHz is under restricted usage under ECC Decision ECC/DEC/ (04)09 for EU Countries. User/Operator shall check with local Radio Spectrum regulator for necessary operating license and restriction usage and protection of Local Radio service.

| | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|
| AT | BE | BG | CZ | DK | EE | FR | DE | IS | IE | IT |
| EL | ES | CY | LV | LI | LT | LU | HU | MT | NL | NO |
| PL | PT | RO | SI | SK | TR | FI | SE | CH | UK | HR |

USER GUIDE

Introduction

The SABRE™ RANGER 5000 is a broadband global area network (BGAN) Class 2 machine-to-machine (M2M) satellite terminal. It has a ruggedised mechanical enclosure designed to be “touch once and left” in all types of weather conditions.

The terminal operates on either the Inmarsat standard BGAN or the M2M service. It offers global coverage and is fit for SCADA applications to gather real-time data from remote unmanned locations. The firmware is specially designed to provide reliable and stable BGAN connectivity continuously for long period of time without user intervention.

It is fully compatible with the Remote Terminal Manager (RTM) or Inmarsat M2M platform, which allows the user to graphically view the location of the terminal and monitor the terminal status.

The terminal can also be configured remotely using SMS commands. The PDP context of the SABRE™ RANGER 5000 can be activated or deactivated via SMS. The rebooting process can also be initiated via SMS. In addition, the terminal logs can be retrieved remotely for debugging purpose.

You can use either the rugged mounting bracket (optional accessory) of the Sabre™ Ranger 5000 (See figure 1 below.) or a VESA MIS-D bracket to mount the SABRE™ RANGER 5000 terminal.



Figure 1

USER GUIDE

2. Quick Reference

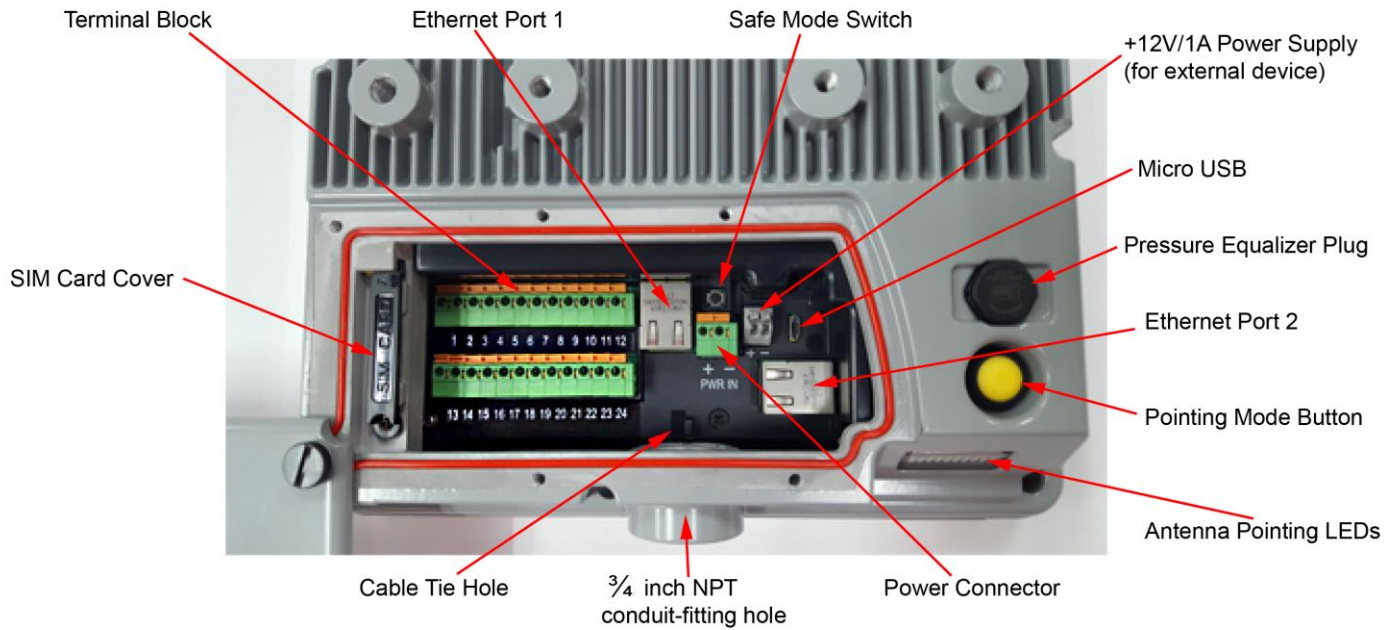


Figure 2

The SABRE™ RANGER 5000 has a NPT $\frac{3}{4}$ inch hole for installing a conduit-fitting or a cable gland on the bottom part of the casing to route all the wires.

USER GUIDE

3. Install the Sim Card

1. Release the five black screws from the protective cover and loosen the “Rotation Point” screw. See figure 3.



Figure 3

2. Rotate the protective cover in a clockwise direction.
3. Open the SIM card cover and rotate in a clockwise direction. See figure 4.



Figure 4

USER GUIDE

4. Slot the SIM card into the SIM card holder in the orientation as shown on figure 5.



Figure 5

5. Insert the SIM card until it 'clicks' into place.
6. Rotate and move the SIM card cover back in place.

USER GUIDE

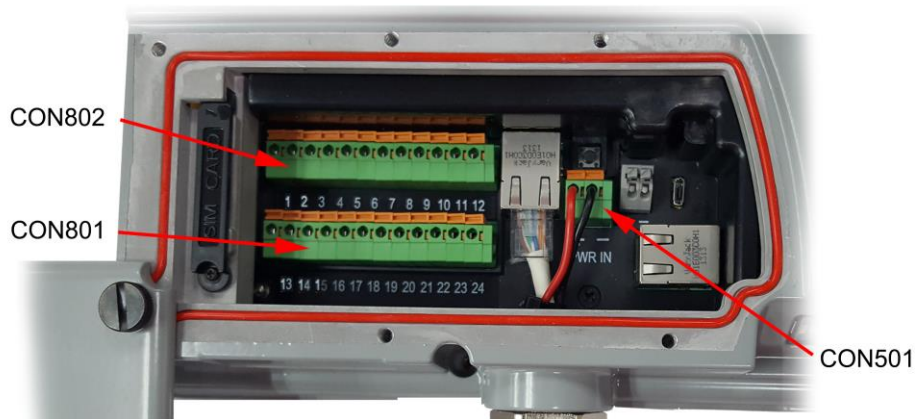
4. Connect the Cables and Wires

The SABRE™ RANGER 5000 has a NPT ¼ inch hole for installing a conduit-fitting or a cable gland at the bottom part of the casing to connect all the wires. See appendix B for information about the conduit and its accessories.



Figure 6

CON801 and CON802 Terminal Block Assignment



Terminal block pin assignment:

| | | | | | | | | | | | |
|-----|----|----|-----|----|----|-----|------------|-----------|-----|----------|------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| GND | OP | OP | GND | IP | IP | GND | RS232/TX | RS232/CTS | GND | RS232/RX | RS232/RTS |
| | 3 | 4 | | 3 | 4 | | RS485/Z(B) | RS485/B | | RS485/A | RS485/Y(A) |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| TDR | OP | OP | GND | IP | IP | GND | Analog | Local | GND | RS232/ | RS232/ |
| | 1 | 2 | | 1 | 2 | | Input | Wakeup | | RX | TX |

Figure 7

USER GUIDE

Ethernet Connection

- Use a CAT5e cable with the RJ45 plug for the Ethernet cable. Thread the Ethernet cable through the conduit-fitting/Cable gland hole carefully.
- Insert the RJ45 Plug into the Ethernet Port 1 (as indicated below in red rectangle).

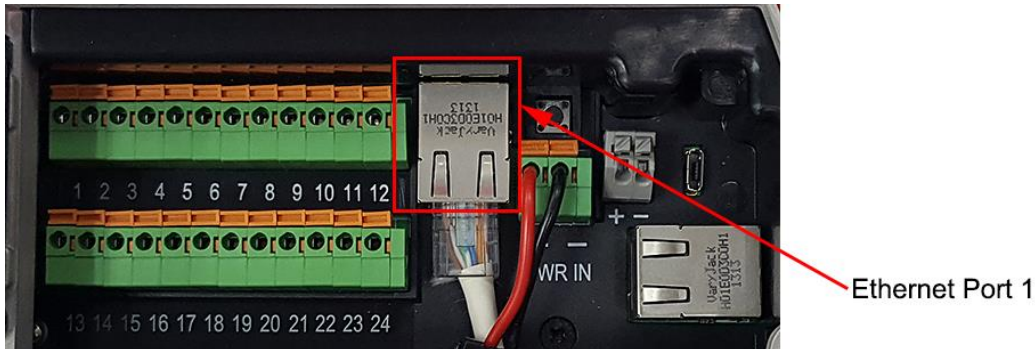


Figure 8

Power Supply input

- Connect a 12VDC nominal power supply to the Power connector, CON501. This Power supply input supports a range of voltages from 10.8 to 32Volts. The terminal requires 20W when transmitting and 6W when receiving.
- Use two AWG16 wires for power connection if the cable length is not more than 10m. Otherwise, use AWG14 wires for a cable that can be lengthened up to 100m.
- Insert the red wire into the terminal block with (+) marking, the black wire into the terminal block with (-) marking. Press and hold the orange tab on the terminal block while inserting the wire into the hole.

NOTE: The sample wires below are used for reference. You may use different colour wires that met the electrical specifications.

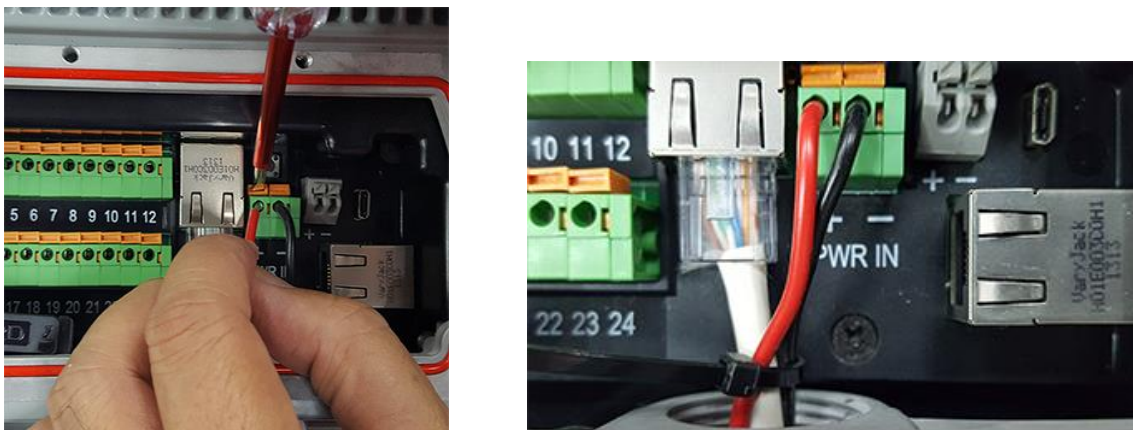


Figure 9

USER GUIDE

RS232 port – debug port

This port is intended for capturing the debug log. The cable length is limited to 10 metres. Use Belden cable no. 9533 or equivalent.

- Connect the wires as shown below.

NOTE: The sample wires below are used for reference. You may use different colour wires that met the electrical specifications.

| | | |
|------------|---|-------------------------------|
| Black wire | → | terminal block 22 (GND) |
| Red wire | → | terminal block 24 (RS232-TX) |
| White wire | → | terminal block 23 (RS232-RX). |



Figure 10

RS232/RS485 – user port

This is a user configurable port. The user can configure this port to be any of the following:

- RS232
- RS485 – full duplex
- RS485 – half duplex

RS232

Use Belden cable no. 9533 or equivalent for 3-wire RS232 (RX, TX, GND) or Belden cable no. 9535 or equivalent for 5-wire RS232 (RX, TX, RTS, CTS, GND). Cable length is limited to 10 metres.

- Connect the wires as shown below.

NOTE: The sample wires below are used for reference. You may use different colour wires that met the electrical specifications.

| | | |
|------------|---|------------------------------|
| Black wire | → | terminal block 10 (GND) |
| Red wire | → | terminal block 8 (RS232-TX) |
| White wire | → | terminal block 11 (RS232-RX) |

NOTE: If you use the Belden cable no. 9535 for 5-wire RS232 (RX, TX, RTS, CTS, GND), refer to figure 7 for the wire connections to the terminal block.

USER GUIDE



Figure 11

Digital Input and Output; Terminal Data Ready (TDR) Output; Local Wake up Input

Use Belden cable no. 9535 or similar non-paired shielded cable for these connections. The number of wires in the cable can vary depending on the user requirements.

Digital output

There are 4 digital outputs configured as Low side drivers. These outputs are connected to pin 14(OP1) and pin 15(OP2) of CON801 and pin 2(OP3) and pin 3(OP4) of CON802. A low side driver will pull the signal to ground when active. An output can sink up to 400mA of current.

Low Side Driver

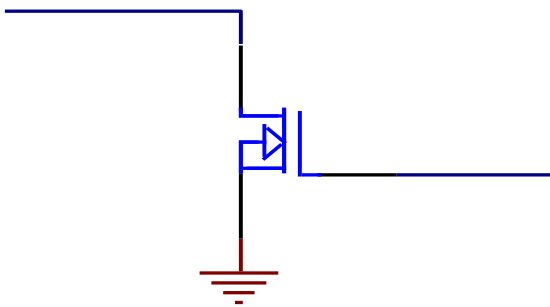


Figure 12

Digital input

There are 4 digital inputs. They are connected to pin 17 (IP1) and pin 18(IP2) of CON801 and pin 5(IP3) and pin 6(IP4) of CON802. These inputs accept a signal of 0V to +32VDC. These inputs have a weak pull-down of approximately 300K ohms. A pull-up to +5VDC may be used to drive these inputs. The input buffer inverts the input logic level. The minimum input voltage to be declared is higher than, 2.6V. The maximum input voltage to be declared is lower than, 1.0V. The digital input ground is connected to pin 4 (GND), pin 7(GND) or pin 16(GND).

USER GUIDE

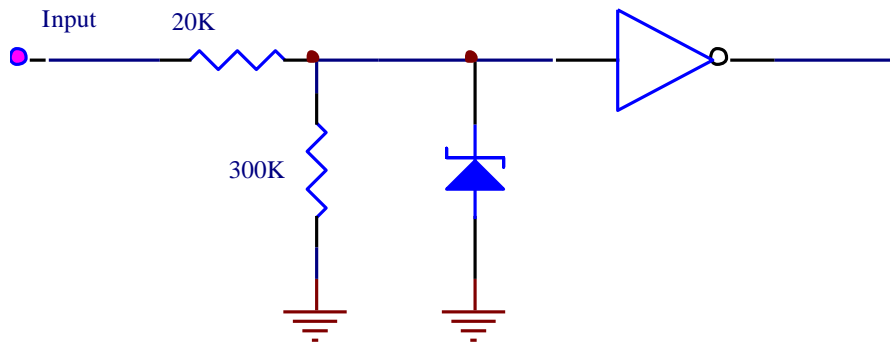


Figure 13

Local Wake up input

This is a digital input. The local wakeup input is connected to pin 21 (Wake-up) of CON801. The signal ground is connected to pin 22 (GND) of CON801. The electrical specifications of this input are the same as the specifications of the Digital input.

Terminal Data Ready (TDR) output

This is a digital output. The TDR output is connected to pin 13 (TDR) of CON801. The signal ground is connected to pin 1 (GND) of CON802. The electrical specifications of this port are the same as the specifications of the Digital output.

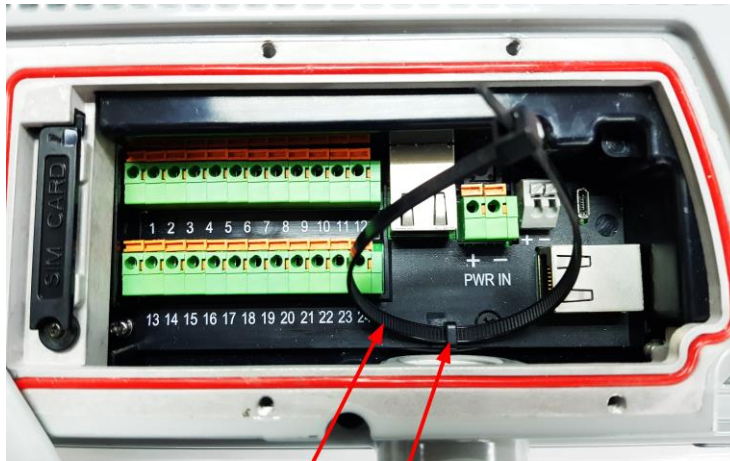
Analogue voltage input

Use Belden cable no. 9841 or equivalent. The analogue input is connected to pin 20 (Analog-input) of CON801. This input will accept a signal of 0V to 32VDC. The analogue signal ground is connected to pin 19 (GND) of CON801.

USER GUIDE

Secure the cables and wires with a cable tie

1. Gather all the connected cables and wires.
2. Loop the cable tie into the cable tie hole in the terminal before fastening to secure the wires in place so that they will not slip off its connectors.
See figure 14 – * wires are not displayed to show the cable tie hole.



Cable Tie

Cable Tie Hole

Figure 14

3. Secure the wires together with a cable tie.



Cable Tie

Figure 15

USER GUIDE

4. Secure the conduit tightly to the adaptor to prevent water from getting into the conduit and the terminal.



Figure 16

USER GUIDE

Secure the protective cover

1. Rotate the protective cover anti-clockwise to the closed position.
2. Tighten the six black screws including the “rotation point” screw with a flat blade screw driver.

NOTE: For ingress protection, it is important to ensure the screws are tightened to a torque value of 0.57 Nm (5.0 in-lbs), approximately 2 ½ to 3 turns for each screw.

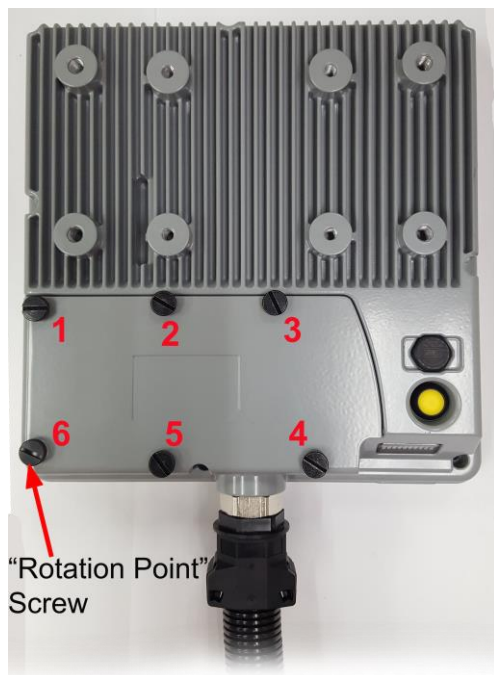


Figure 17

USER GUIDE

5. Optional Accessories

Mounting Bracket

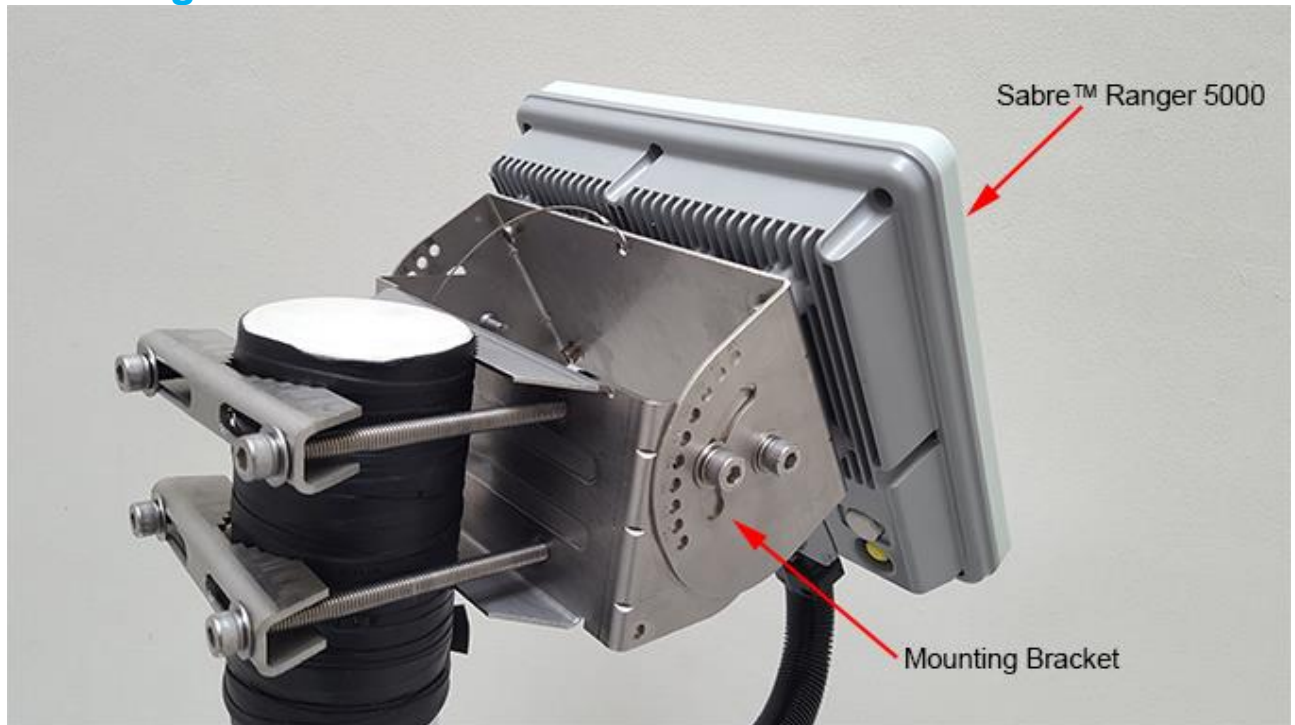


Figure 18

Parts List

| ITEM | DESCRIPTION | QTY |
|------|---|-----|
| 01 | Socket Head Cap Screws, M8 x 120mm, Full thread | 4 |
| 02 | Flat Washers, M8 | 12 |
| 03 | Saddle Clamps | 2 |
| 04 | Bracket Wall (185 x 90 x 100)mm | 1 |
| 05 | Split Washers, M8 | 4 |
| 06 | Socket Head Cap Screws, M8 x 14mm | 8 |
| 07 | Bracket Body (189 x 110 x 90)mm | 1 |

USER GUIDE

6. Fix Optional Mounting Bracket to Sabre™ Ranger 5000

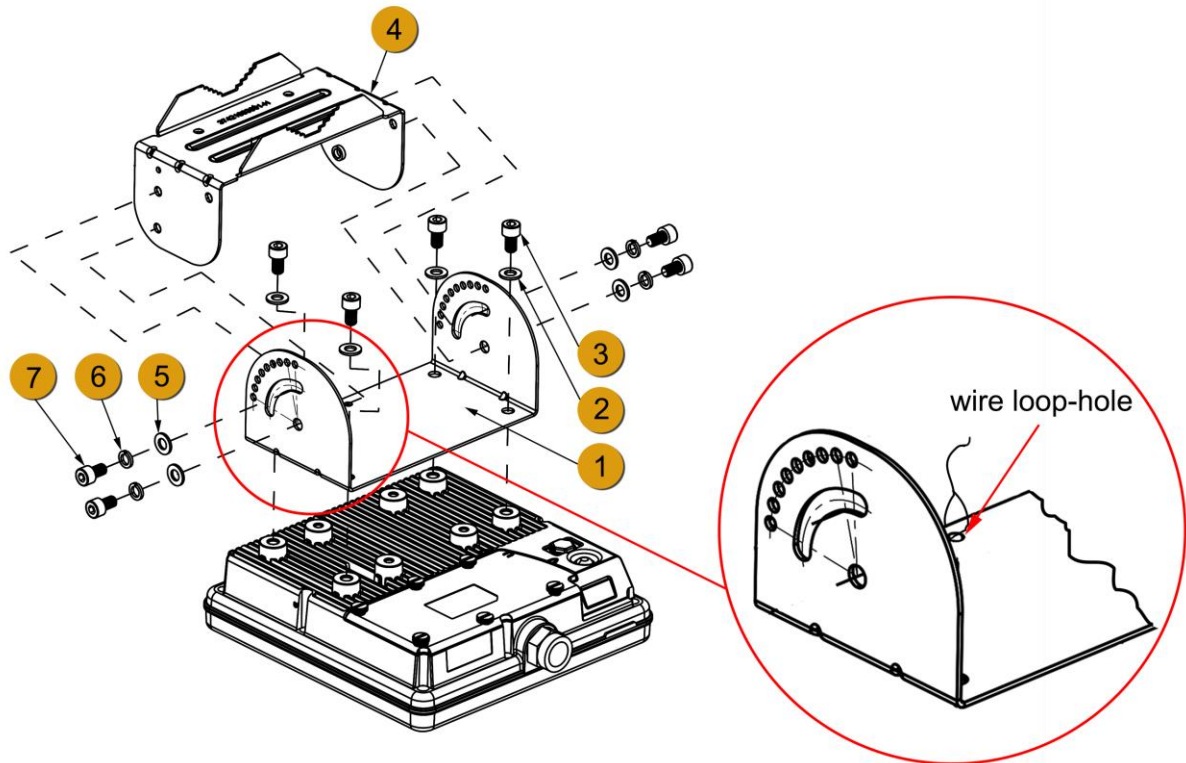


Figure 19

1. See figure 19 above. Place Sabre™ Ranger 5000 terminal with its front face on a flat surface.
2. Attach ① the bracket body on the rear of Sabre™ Ranger 5000 terminal.

NOTE: There are five holes at the base of the bracket body. The wire loop-hole as shown on the enlarged view should be placed along the upper edge of the terminal. See figure 19 and its enlarged view.

3. Align the four holes, and fasten ① to Sabre™ Ranger 5000 terminal using the washers (4x) ② and the socket head cap screws (M8 x 14mm - 4x) ③ with a hex L-key.
4. Align the bracket wall ④ to the bracket body ①. See figure 19. Notice the upper holes on the bracket wall align to the slots on the bracket wall and the lower holes align to the holes below the slots of the bracket body.
5. Use the washers (4x) ⑤, the split washers (4x) ⑥ and the socket head screws (M8 x 14mm - 4x) ⑦ to assemble ④ to ①.

NOTE: Do not fully tighten the screws to assemble ④ to ① with a hex L-key, fasten the screws finger tight only as you need to adjust its actual position according to the satellite location later.

USER GUIDE

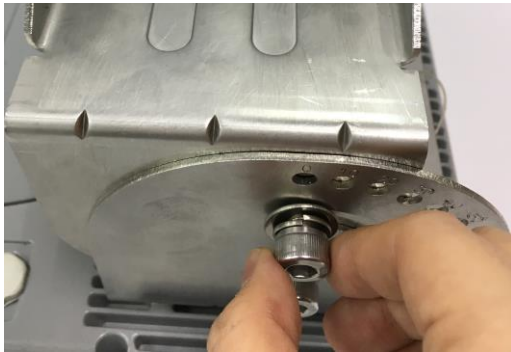


Figure 20

7. Mount the Terminal on a Pole

Before mounting the terminal, ensure that the azimuth is correct by using a compass. For example: North has an azimuth of 0°, East 90°, South 180° and West 270°.

1. Locate a vertical pole or column to mount the SABRE™ RANGER 5000 terminal.

NOTE: The mounting bracket is designed to be mounted on a 1 to 3 inch diameter pole.

2. Mount the pre-assembled terminal to the pole.

TIP: If you have a long conduit of 10 metres or more, use the additional hole on the mounting bracket with a cable tie to hold the conduit before mounting the terminal to a pole. See figure 21 below.



Figure 21

3. Use the supplied washers, socket head cap screws (M8 x 120mm), and the saddle clamps to mount the pre-assembled terminal on the pole.

USER GUIDE

4. Secure the saddle clamps on the pole by first turning in the screws and washers at the position **1** and **2**, and then turn in the screws and washers at the position **3** and **4** for easy installation. See figure 22.

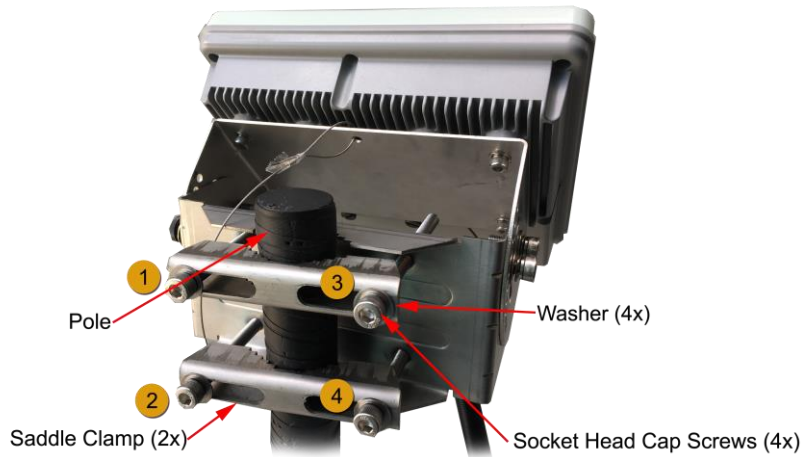
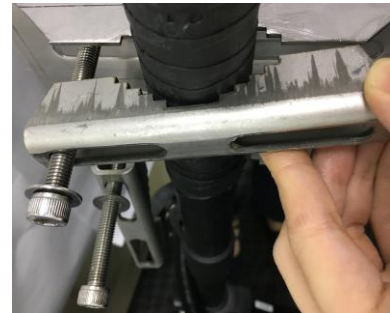


Figure 22

5. Tighten the screws to secure the SABRE™ RANGER 5000 terminal to the pole.



6. Secure the conduit to the pole by using several cable ties.

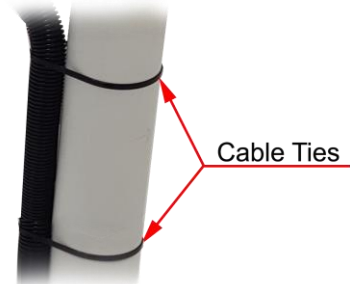


Figure 23

USER GUIDE

8. Terminal Grounding

Protective Earth Grounding

The chassis of the SABRE™ RANGER 5000 terminal must be firmly connected to the earth ground by using a short and low impedance wire.

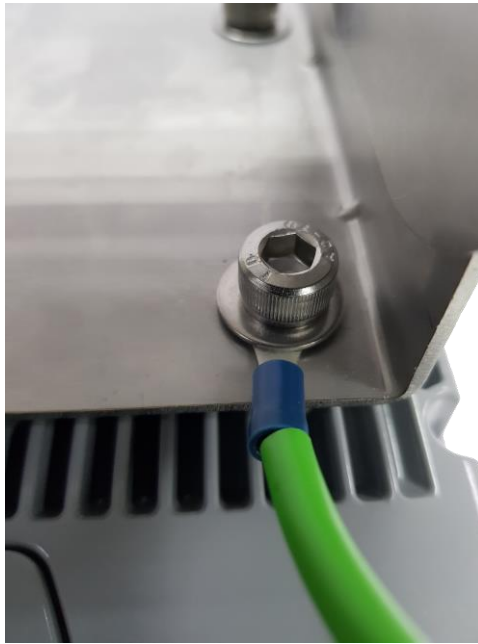


Figure 24

1. Unscrew one of the four mounting screws at the back of the terminal.
2. Insert the earth grounding wire lug in between the mounting bracket and the washer, and then tighten the screw.

NOTE: Please seek professional local advice for earth grounding.

USER GUIDE

9. Point the Antenna

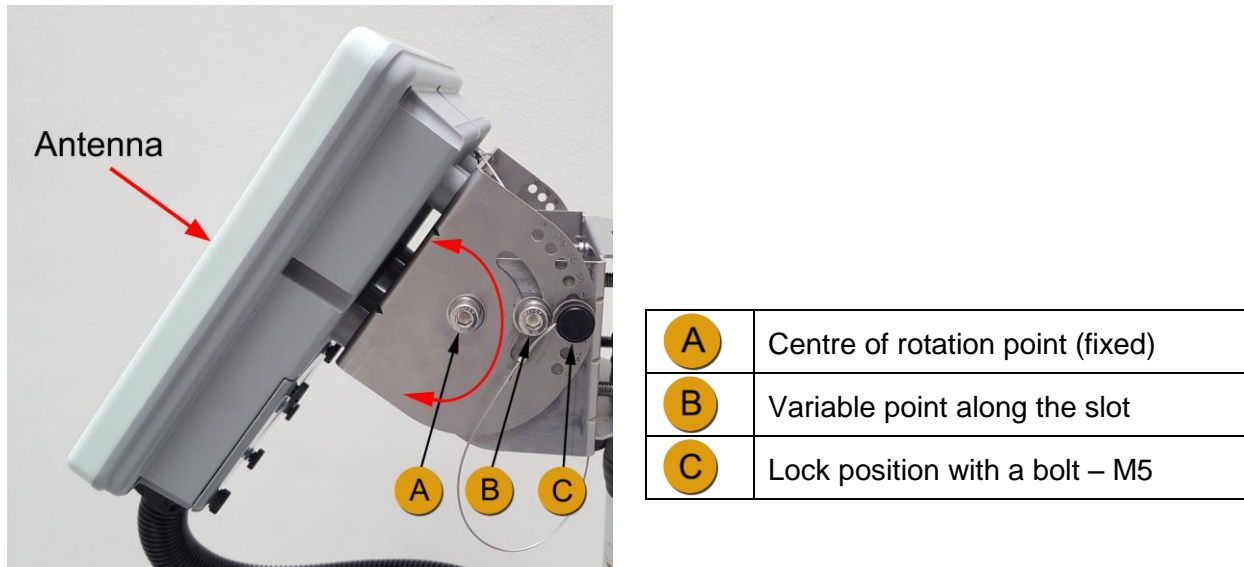


Figure 25

1. Place the terminal outdoor with no obstruction from trees, buildings, hills or any external objects and power up the terminal.
2. Check the elevation and azimuth on the terminal firmware. The terminal firmware displays the pre-calculated elevation and azimuth once the GPS location is acquired.

NOTE: The information can be found in the Web console on the Home page. Refer to the section on Navigate to the Web Console for more details. Azimuth and Elevation are angles used to define the apparent position of an object in the sky, relative to a specific observation point. In this case, we are the observers on earth.

3. Adjust the required elevation angle by tilting the bracket body attached to the terminal along the slot. Notice that you can adjust the angle of elevation in steps of 5°. The angle markings at both sides of the bracket body have an offset of 5°. See figure 26 below. The terminal is at a vertical position at the angle of 0° and at a horizontal position at the angle of 90°.

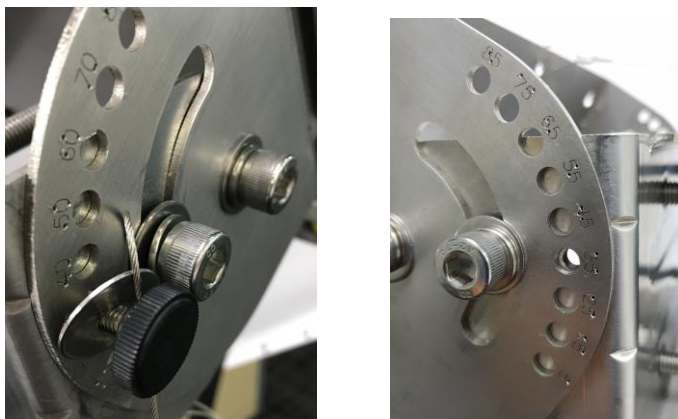


Figure 26

USER GUIDE

4. Insert the M5 bolt to lock the required position and tighten it to secure the angle of elevation. See figure 27.

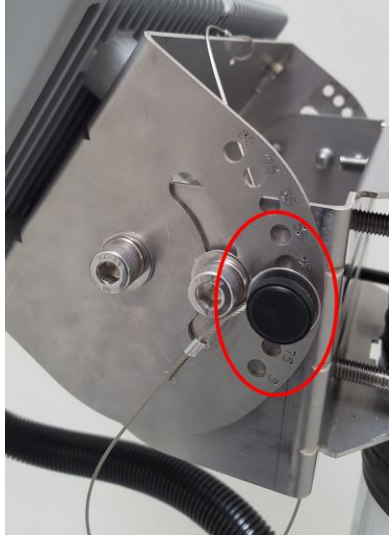


Figure 27

USER GUIDE

10. Navigate to the Web Console

1. The SABRE™ RANGER 5000 terminal should be installed at an outdoor location with the correct **Azimuth**. The terminal needs to be pointed towards the satellite to ensure its connection to the satellite network. Turn ON the power supply to the terminal and connect the Ethernet cable to your laptop/PC.

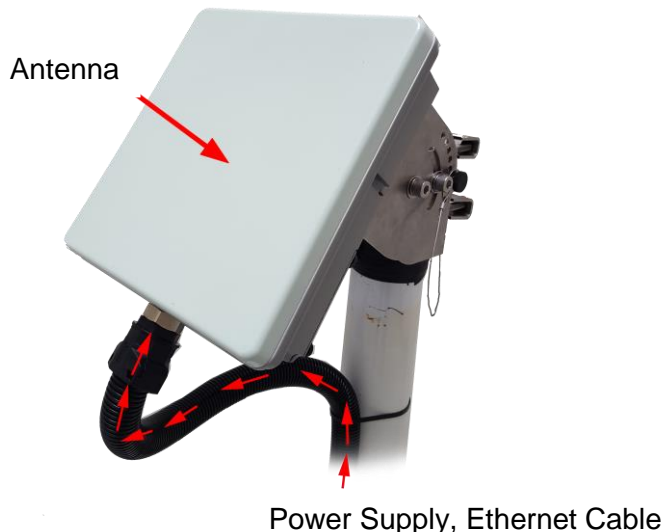


Figure 28

2. When the terminal is powered up, all the Antenna Pointing LEDs will flash briefly and goes off. This indicates the terminal is ON.
3. After a short while, the terminal will go into Auto network registration mode. This is indicated by synchronous flashing of all the LEDs. Press and hold Pointing Mode button for more than 3 seconds to disable the Auto network registration mode and go to the manual network registration mode.

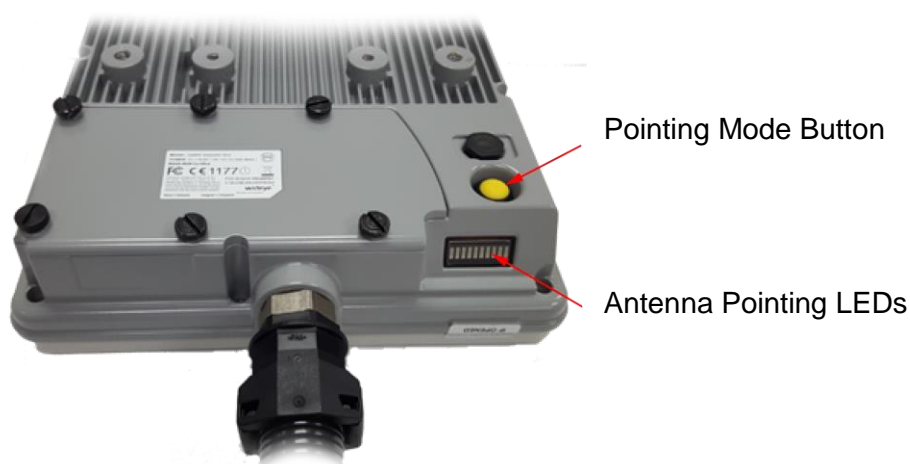
























Figure 29

USER GUIDE

Manual Network Registration

1. The Antenna Pointing LEDs indicate the received Global Beam signal strength. Slowly adjust the **Elevation** of the terminal until the maximum number of LEDs illuminate. See the table below for the number of LEDs lighting up vs the Global beam signal strength.
2. Another way to do the antenna pointing is to use the audio assisted pointing mode. In this mode, a buzzer will emit an audio tone with its pitch changing according to the strength of the global beam signal. The buzzer is disabled by default. To enable the buzzer, navigate to **Settings > Terminal Settings > Antenna Pointing buzzer**. Click **Apply** for the new setting to take effect.
3. After the antenna is correctly pointed to the satellite, press the Pointing Mode button once to exit the pointing mode and start the network registration process.

NOTE:  indicates flashing green LED and  indicates steady green LED.

| LEDs Signal | Global Beam Signal Strength (dB) |
|---|----------------------------------|
|   | 0 – 40 |
|   | 41 – 47 |
|    | 48 |
|   | 49 |
|    | 50 |
|   | 51 |
|    | 52 |
|   | 53 |
|   | 54 |
|  | 55 and above |

USER GUIDE

NOTE:

When the Antenna is pointing away from the satellite, the received signal strength is weaker. This is indicated by, lighting up a fewer number of LEDs and a low pitch audio tone. When the Antenna moves towards the satellite, the signal strength will gradually increase. This is indicated by lighting up more LEDs and gradually increasing pitch of the audio tone.

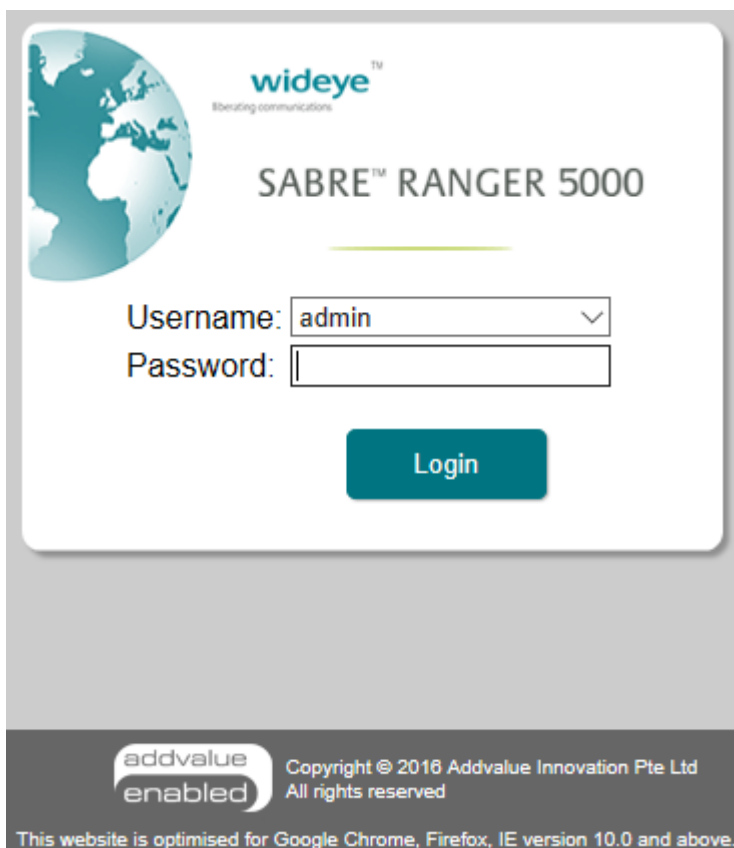
4. You may also verify the signal strength through the Web Console.

i) Open any web browser and type **http://RANGER5000** or **http://192.168.1.35** on the address bar.

ii) The default credentials are:

Username: **admin**

Password: **1234**



wideye™
liberating communications

SABRE™ RANGER 5000

Username:

Password:

Login

addvalue enabled
Copyright © 2016 Addvalue Innovation Pte Ltd
All rights reserved

This website is optimised for Google Chrome, Firefox, IE version 10.0 and above.

Figure 30

NOTE:

Web Console will remind the user to change the password for the first time login for security purposes. A minimum of 6 characters are required for the new password.

USER GUIDE

iii) You can see the following details:

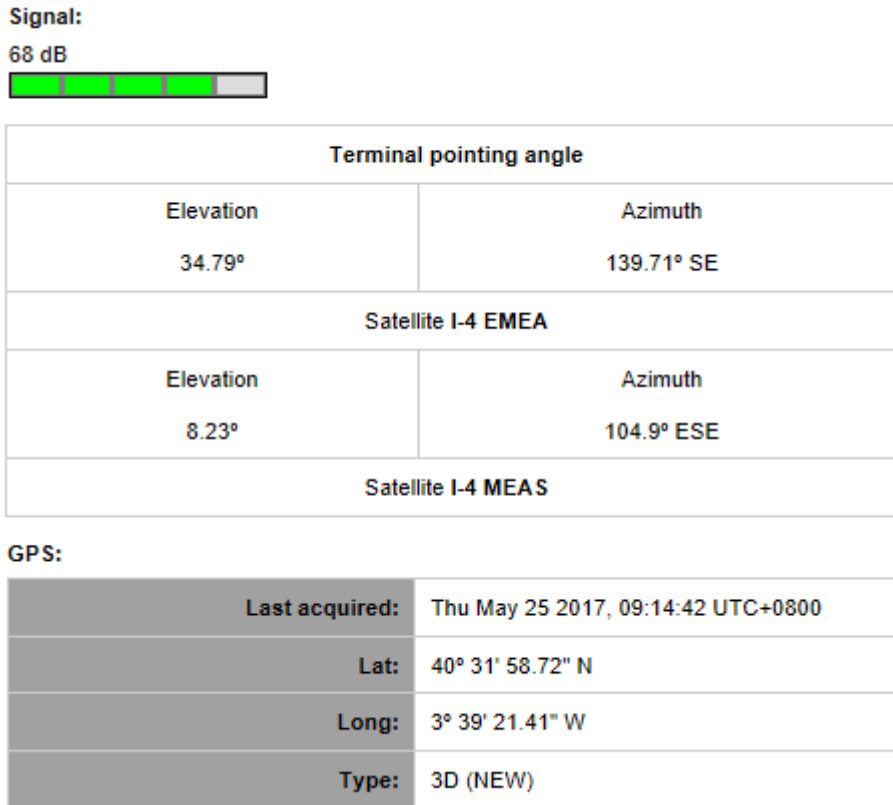


Figure 31

1. After the terminal is properly pointed, press and hold the Pointing Mode Button once to trigger the network registration.
2. The Antenna Pointing LEDs flash in sequence during the network registration.

NOTE:

The SABRE™ RANGER 5000 terminal activates a data connection automatically by default.

Auto Network Registration

When the terminal is powered up while it is already pointed to the satellite, it will register to the network automatically.

The LEDs will flash from right to left. When the network registration is successfully completed, all the LEDs will flash twice and turn off.

USER GUIDE

11. Web Console

After login to the Web Console, navigate to **Home > Menu** to view the menu page.

MENU OVERVIEW

| Data | SMS | Settings | Logout |
|---|---|---|--------|
| <u>Data Profile</u> - Primary Profiles - Secondary Profiles <u>Firewall</u> -Setup -HTTP Filters <u>Port Forwarding</u> <u>Data Settings</u> | <u>Compose</u> <u>Inbox</u> <u>Sent</u> <u>Draft</u> | <u>Accounts</u> <u>Ethernet</u> -Ethernet - Ethernet Settings - DHCP - MAC Filtering <u>Security</u> - Terminal PIN - SIM PIN <u>Terminal Settings</u> - Reboot Terminal - Factory Reset - Firmware Upgrade - Remote Access - Power Saving - Ciphering - Facility Lock - IP Watchdog - I/O Configurations - Backup/Restore - Web - Antenna Pointing Buzzer - GNSS Selection <u>Terminal Info</u> - Information - Logs - Data Log <u>SMS Configurations</u> - Information - Remote Control <u>Language</u> <u>Support</u> <u>About</u> | |

USER GUIDE

STATUS OF TERMINAL

The Home page provides the status information of the terminal, pointing information and allows a data connection to be established.

Navigate to Home page for the terminal status.

The screenshot shows the 'Home' page of the terminal's web console. It displays the following information:

- Status:**
 - Registered to network: Yes
 - Data connection active: No (with an 'Activate Data Connection' button)
- Signal:** 69 dB (with a signal strength bar)
- GPS:**
 - Last acquired: Tue May 24 2016, 17:16:34 UTC+0800
 - Lat: 40° 31' 58.72" N
 - Long: 3° 39' 21.41" W
 - Type: 3D (NEW)
- Temperature:** Normal

At the bottom, a message reads: "Registered to Network but no active data connection exists. Please activate a data connection before doing any data transfer."

| | |
|-------------|--|
| Status | Indicates registration and data connection status. |
| Signal | Indicates terminal received signal strength. |
| GPS | Indicates GPS information. |
| Temperature | Indicates current operating temperature status. |

Figure 32

Click “**Activate Data Connection**” or “**Deactivate Data Connection**” in order to activate or deactivate data connection.

NOTE:

Signal strength must be 42dB or above for the terminal to successfully connect or register to the network.

Signal strength can be improved by pointing more accurately.

If the signal strength level indicated in the web console is low under a registered condition, you can slowly adjust the terminal’s elevation, azimuth angles and monitor the signal strength displayed in web console.

USER GUIDE

11.1 Data

11.1.1 Data Profile

Navigate to **Menu > Data > Data Profile** in order to modify the connection type.

The connection profile defines the connection type.

You can select from a list of profiles to be the default primary profile and connection type.

Figure 33

Click “Edit” to modify the data profile.

You can create your customized primary profile.

Figure 34

NOTE:

Please note that the 'Static IP Address APN Username' and 'Static IP Address APN password' stated are not for Web Console login purposes.

These are provided by your Service Provider if your network required a static IP address subscription.

Leave it blank if you do not have such subscription

USER GUIDE

Profile Name

Change the profile name as desired.

Access Point Name (APN)

By default, the APN from your SIM card is selected.

Follow these steps to change the Access Point Name (APN):

- i. Select User Defined.
- ii. Enter the new APN in the field space provided (e.g. STRATOS.BGAN.INMARSAT.COM).
- iii. Enter the username and password (these details should be supplied by your service provider) if required.

Static IP Address APN

By default, a Dynamic IP Address is selected.

To use a Static IP Address:

- i. Select Static IP Address and enter the APN address and password in the space provided.

11.1.2 Firewall

The firewall function is disabled by default. Navigate to the firewall setup page to enable it.

Navigate to **Menu > Data > Firewall > Setup** to change the Firewall protection profile setup.

Figure 35

Follow these steps to change the firewall setup.

- i. Click **Edit** to modify the predefined profile settings.

You can edit the profile name and predefined rules to allow or reject incoming packets.

Figure 36

USER GUIDE

Navigate to **Menu > Data > Firewall > Setup > Edit**

Incoming Rule

i. Under Incoming Rule tab, click **Add** to add new rules.

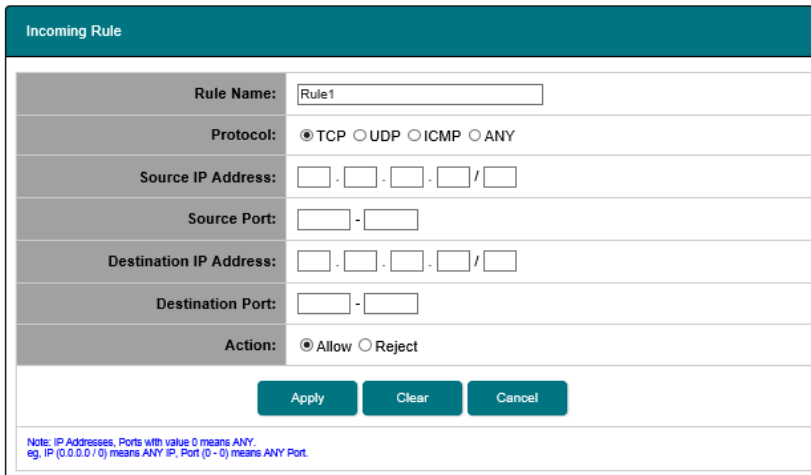


Figure 37

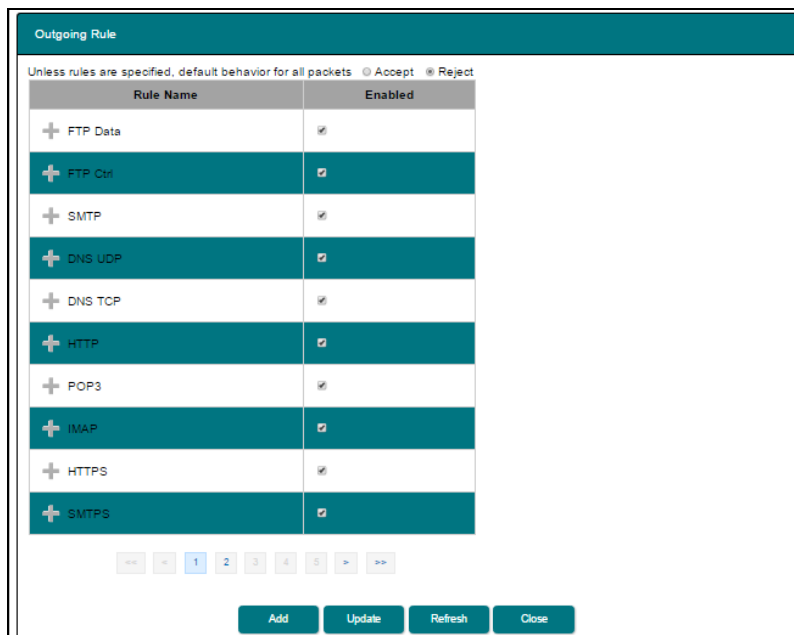
ii. Enter your desired rule name and fill in the necessary information.

iii. Select **Action: Reject** to reject the incoming packet.

iv. Click **Apply** to save the new incoming rules.

Outgoing Rule

i. Under Outgoing Rule tab, click the '+' symbol besides the rule name to edit the existing rules. or click **Add** to add new rules.



| Rule Name | Enabled |
|------------|-------------------------------------|
| + FTP Data | <input checked="" type="checkbox"/> |
| + FTP Ctr | <input checked="" type="checkbox"/> |
| + SMTP | <input checked="" type="checkbox"/> |
| + DNS UDP | <input checked="" type="checkbox"/> |
| + DNS TCP | <input checked="" type="checkbox"/> |
| + HTTP | <input checked="" type="checkbox"/> |
| + POP3 | <input checked="" type="checkbox"/> |
| + IMAP | <input checked="" type="checkbox"/> |
| + HTTPS | <input checked="" type="checkbox"/> |
| + SMTPS | <input checked="" type="checkbox"/> |

Figure 38

USER GUIDE

- ii. Similar to incoming rule, you can create your desired rule name and fill in the necessary information.
- iii. Click **Apply** to save the new outgoing rules.

HOSTNAME FILTERING

To stop the users from accessing certain websites through the internet, you can configure the filtering settings in your SABRE™ RANGER 5000 terminal.

Navigate to **Menu > Data > Firewall > HTTP Filters** to enable the filtering based on the hostname or the keywords.

Follow these steps to apply hostname filtering:

- i. Select **Enabled**.

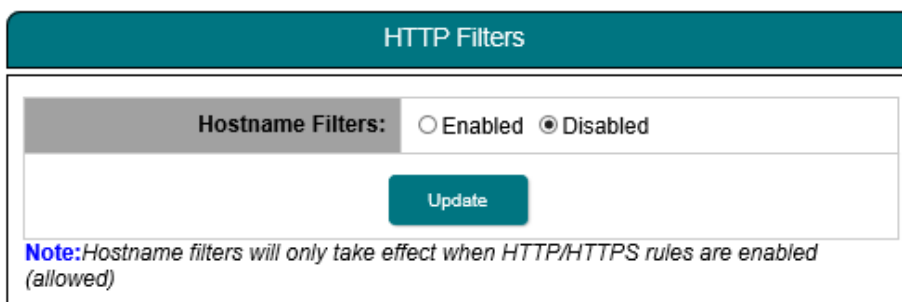


Figure 39

- ii. Click **Update** to modify the settings.
- iii. Under **Hostname/Keywords** tab, click **Add** to add new keywords (e.g. Facebook).

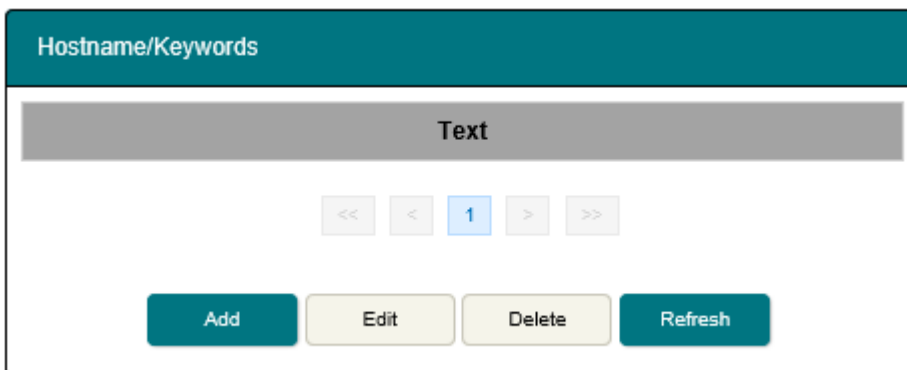


Figure 40

- iv. You can modify existing keywords by selecting the Text from the list.
- v. Click **Edit** to modify or **Delete** to delete the selected keywords.

NOTE:

Hostname filters will only take effect when HTTP/HTTPS rules are enabled under Data> Firewall> Setup. Re-activate your data connection for the new settings to take effect.

USER GUIDE

11.1.3 Port Forwarding

Port forwarding is a feature for a router (multi-user) mode. This feature configures SABRE™ RANGER 5000 to direct the incoming traffic on certain TCP/UDP port to a specific port on a local computer or server through IP address.

Navigate to **Menu > Data > Port Forwarding** to configure new port forwarding rule.

| Incoming Port | Protocol |
|--|----------|
| <div style="display: flex; justify-content: space-around;"> Add Edit Delete Refresh </div> | |

Figure 41

Follow these steps to add a new forwarding rule:

- i. Click **Add**.

| | |
|--|---|
| Incoming Port: | <input type="text"/> - <input type="text"/> |
| Protocol: | TCP ▾ |
| Destination IP Address: | <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> |
| Destination Port: | <input type="text"/> - <input type="text"/> |
| Enabled: | <input type="checkbox"/> |
| <div style="display: flex; justify-content: center; gap: 20px;"> Add Cancel </div> | |

Figure 42

- ii. Enter the **Incoming Port** number range in the provided space.
If only one number, repeat the number in both space, example: 80-80.
- ii. Select the **Protocol** type: TCP (for HTTP) or UDP.
- iv. Enter the **Destination IP address** of your server or the receiving devices in the provided space.
- v. Enter the **Destination Port** number in the provided space.
Example: TCP port 80 for web server.
- vi. Click **Add** to save the settings.

NOTE: Re-activate your data connection for the new settings to take effect.

USER GUIDE

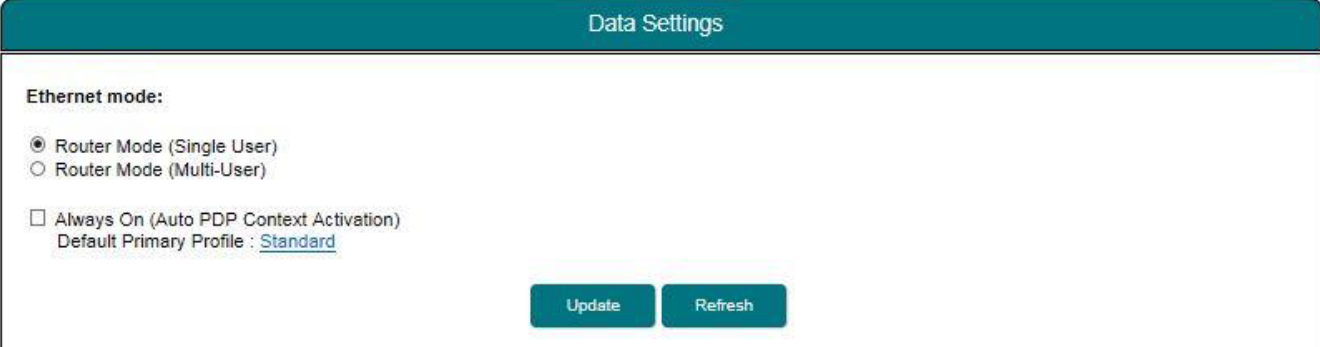
11.1.4 Data Settings

Auto PDP Context Activation is a feature to establish the PDP connection upon power up. It also helps to re-establish the PDP connection due to network deregistration or any reason other than user intervention.

Navigate to **Menu > Data > Data Settings** to configure the data settings to **Always On**.

To enable Auto PDP Context Activation

- i. Click **Always On (Auto PDP Context Activation)**.
- ii. Click **Update** for the new configuration to take effect.



Data Settings

Ethernet mode:

Router Mode (Single User)

Router Mode (Multi-User)

Always On (Auto PDP Context Activation)

Default Primary Profile : [Standard](#)

Update

Refresh

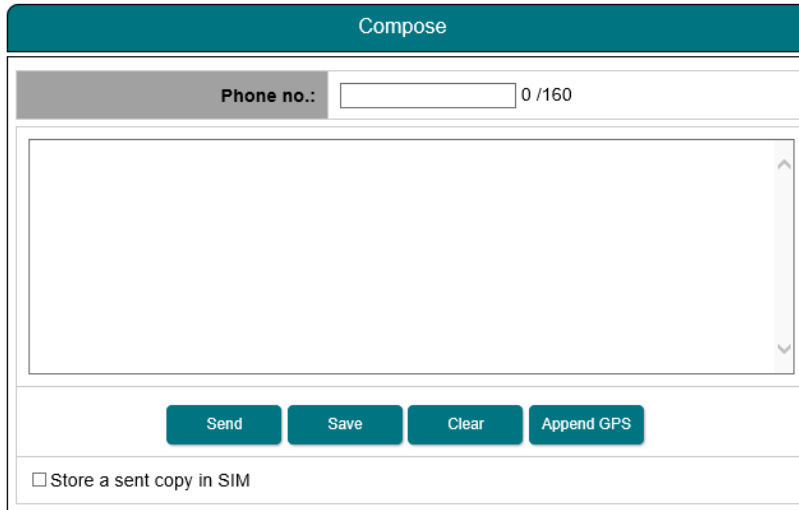
Figure 43

USER GUIDE

11.2 SMS

11.2.1 Compose

Navigate to **Menu >SMS > Compose** to enter compose page.



The screenshot shows the 'Compose' screen for sending an SMS. It features a teal header with the word 'Compose'. Below the header, there is a 'Phone no.:' label followed by a text input field and '0 /160'. A large text editor box is in the center. At the bottom, there are four buttons: 'Send', 'Save', 'Clear', and 'Append GPS'. Below the buttons is a checkbox labeled 'Store a sent copy in SIM'.

Figure 44

- i. Enter the recipient's phone number in the Phone no. box.
Type the message in the text editor box.
- ii. Click **Send** to send the SMS.
- iii. To save an unsent SMS, click **Save** and the unsent SMS will be saved in **Drafts**.
- iv. Check the box if you wish to store a sent SMS on to the SIM card.
- v. Click **Append GPS** to include your GPS location in the SMS.

USER GUIDE

11.2.2 Inbox

Navigate to **SMS > Inbox** to view Received SMSs.

Reply to an SMS from Inbox:

- i. Select the SMS you plan to reply to by selecting the particular SMSs.
- ii. Click **Reply**.
- iii. The inbox console will switch over to **Compose** mode. Enter your reply in the text box.
- iv. Click **Send** to send the SMS.

Forward an SMS from the Inbox:

- i. Select the SMS you plan to forward and click **Forward**.
- ii. The inbox console will switch over to **Compose** mode. Enter your reply in text box.
- iii. Click **Send** to send the SMS.

Delete an SMS from the Inbox:

- i. Select the SMS you plan to delete and click **Delete**.
- ii. A single SMS or multiple SMSs can be deleted based on the selection.
- iii. Click **OK** to confirm the deletion, or **Cancel** to abort.

To Refresh the Inbox list:

- i. Click **Refresh** and the list will be refreshed.

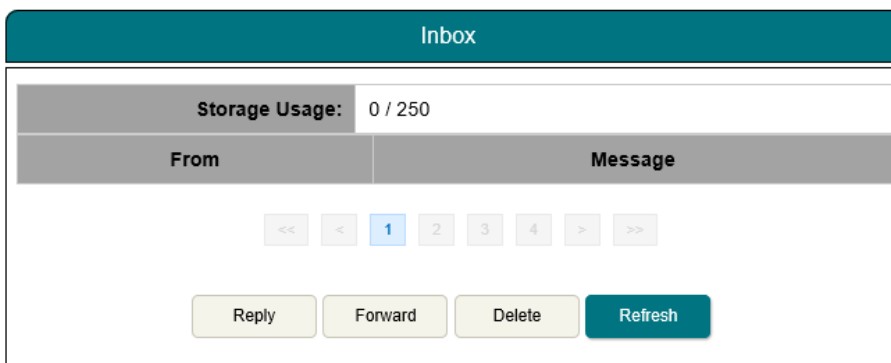


Figure 45

USER GUIDE

11.2.3 Sent

Navigate to **SMS > Sent** to view Sent SMS.

Forward a sent SMS:

- i. Select the SMS you plan to forward and click **Forward**.
- ii. The Sent console will switch over to the Compose mode.
- iii. Enter the recipient's number in the Phone No. field.
- iv. Click **Send**.
- v. The SMS will be sent to the recipient.

Delete a sent SMS:

- i. Select the SMS you plan to delete.
- ii. Click **Delete**.
- iii. Click **OK** to confirm the deletion, or **Cancel** to abort.

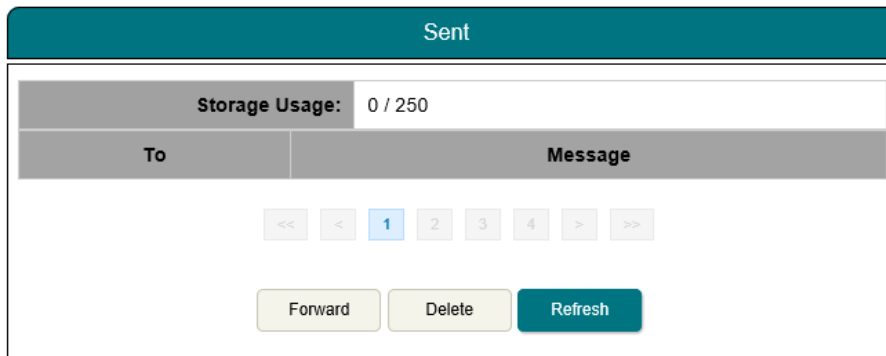


Figure 46

11.2.4 Draft

Stored SMSs are saved inside the draft folder.

Navigate to **SMS > Draft** to view Draft SMSs.

Send a draft SMS:

- i. Select the draft SMS you plan to send and click **Send**.
- ii. The SMS will be sent to the recipient.

Forward a draft SMS to other recipient:

- i. Select the draft SMS you plan to send and click **Send**.
- ii. Click **Forward**.
- iii. The draft console will switch over to the Compose console.
- iv. Enter the recipient's number in the Phone No. field.
- v. Click **Send**.
- vi. The SMS will be sent to the recipient.

Delete a draft:

- i. Select the draft SMS you plan to send.
- ii. Click **Delete**.
- iii. Click **OK** to confirm the deletion, or **Cancel** to abort.

Refresh the draft list:

- i. Click **Refresh** and the list will be refreshed.

USER GUIDE

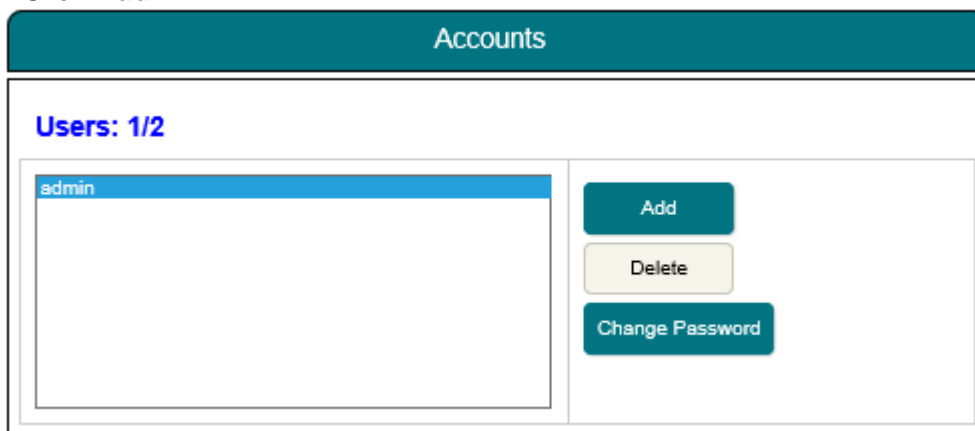
11.3 Settings

11.3.1 Accounts

Navigate to **Menu > Settings > Accounts** to create or edit an account for Web Console access. By default, the password for admin is **1234**. You are recommended to change the admin password for security reasons. Only one User and one Admin account are allowed.

Add a user account:

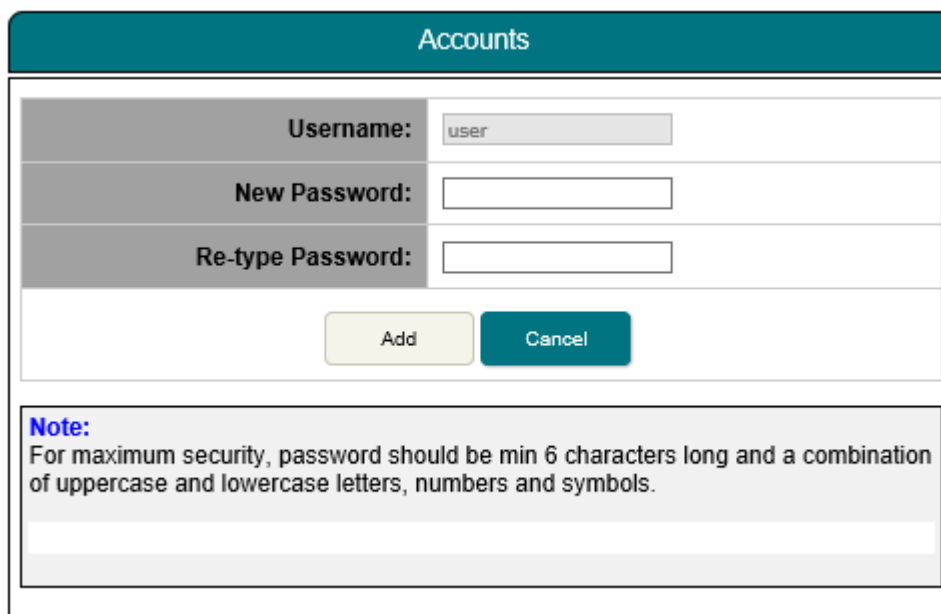
i. Click **Add**.



The screenshot shows the 'Accounts' management page. At the top, there is a teal header with the word 'Accounts'. Below the header, it says 'Users: 1/2'. There is a table with one row containing the username 'admin'. To the right of the table are three buttons: 'Add' (teal), 'Delete' (light grey), and 'Change Password' (teal).

Figure 47

ii. Enter **New Password** and **Re-type Password**.



The screenshot shows the 'Accounts' management page with the 'Add' form open. The form has three input fields: 'Username:' with the value 'user', 'New Password:', and 'Re-type Password:'. Below the fields are two buttons: 'Add' (light grey) and 'Cancel' (teal). At the bottom, there is a 'Note:' section with the text: 'For maximum security, password should be min 6 characters long and a combination of uppercase and lowercase letters, numbers and symbols.'

Figure 48

iii. Click **Add**.

USER GUIDE

11.3.2 Ethernet

Navigate to **Menu > Settings > Ethernet > MAC Filtering** to set the allowed MAC address and the access rights.

The MAC address is a number that uniquely identifies any device connected to a network. The MAC address of your device will be shown on the page.

MAC Filtering Reject List:

- i. Select **Enabled** to enable this feature.
- ii. Select **Reject List** to block the devices to access the terminal.
- iii. Enter the MAC address into the provided space and click **Add** to update the list.
- iv. Click **Update** to make the new settings take effect.

| MAC Filtering | |
|--|---|
| MAC Filtering: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Use: | <input checked="" type="radio"/> Reject List <input type="radio"/> Allowed List |
| <input type="button" value="Update"/> <input type="button" value="Refresh"/> | |
| Reject List | |
| 11:22:33:44:55:66 | Delete |
| <input type="text"/> | Add |
| <input type="button" value="Delete All"/> | |
| *Your MAC Address: 98:76:54:32:10:12 | |

Figure 49

MAC Filtering Allowed List:

- i. Select **Enabled** to enable this feature.
- ii. Select **Allowed List** to allow the devices to access the terminal.
- iii. Enter the MAC address into the provided space and click **Add** to update the list.
- iv. Click **Update** to make the new settings take effect.

| MAC Filtering | |
|--|---|
| MAC Filtering: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Use: | <input type="radio"/> Reject List <input checked="" type="radio"/> Allowed List |
| <input type="button" value="Update"/> <input type="button" value="Refresh"/> | |
| Allowed List | |
| 66:55:44:33:22:11 | Delete |
| <input type="text"/> | Add |
| <input type="button" value="Delete All"/> | |
| *Your MAC Address: 98:76:54:32:10:12 | |

Figure 50

USER GUIDE

11.3.3 Security

TERMINAL PIN

Once the Terminal PIN is activated, the terminal will prompt for the password every time when you reboot it.

Navigate to **Menu > Settings > Security > Terminal PIN** to enable Terminal PIN.

- i. Select **Enabled** to enable Terminal PIN.
- ii. Select **Disabled** if you do not need to enable Terminal to SIM.
- iii. Enter the PIN number in the space provided and click **Update PIN**.

Figure 51

NOTE: The same password is used for the Factory Reset PIN

SIM PIN

If the security feature is enabled, a prompt requests you to enter the SIM PIN each time you power up your SABRE™ RANGER 5000 terminal.

This helps prevent unauthorised use of your SIM. Disable this feature to skip the PIN entry process.

Navigate to **Menu > Settings > Security > SIM PIN** to enable the SIM PIN.

- i. Select **Enabled** to set the SIM PIN.
- ii. Select **Disabled** if you do not need to set the SIM PIN.
- iii. Enter the PIN number in the space provided and click **Apply**.

Figure 52

NOTE:

The SIM PIN depends on the SIM card. Consult your service provider if necessary.

USER GUIDE

11.3.4 Terminal Settings

11.3.4.1 Reboot Terminal

Navigate to **Menu > Settings > Terminal Settings > Reboot Terminal** to reboot the terminal.

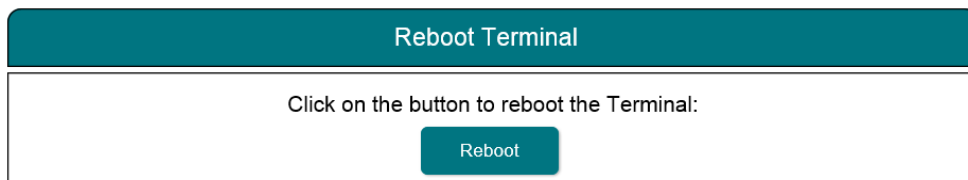


Figure 53

11.3.4.2 Factory Reset

Navigate to **Menu > Settings > Terminal Settings > Factory Reset** to factory reset the terminal. Enter security code for factory reset (Default: 0000).

NOTE:

By default, the security code is 0000. Once you change the Terminal PIN, the Factory Reset password is changed to match the Terminal PIN.

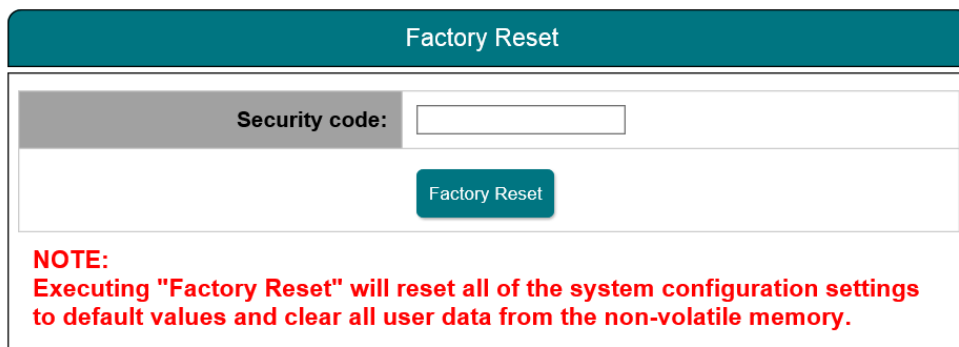


Figure 54

USER GUIDE

11.3.4.3 Firmware Upgrade

Firmware upgrade allows you to update the terminal with the latest operating software.

The terminal has to be in Safe Mode for firmware upgrading.

Navigate to **Menu > Settings > Terminal Settings> Firmware Upgrade** to perform a firmware upgrade.

Your terminal will reboot in Safe Mode once you click the Firmware Upgrade button.

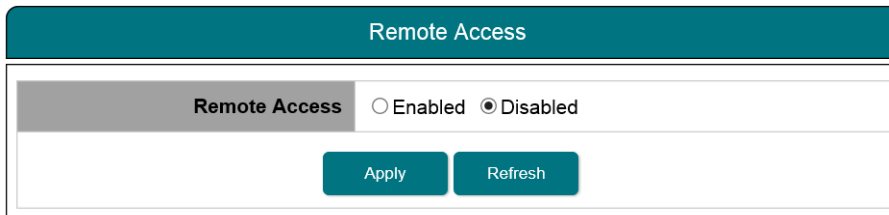


Figure 55

USER GUIDE

11.3.4.4 Remote Access

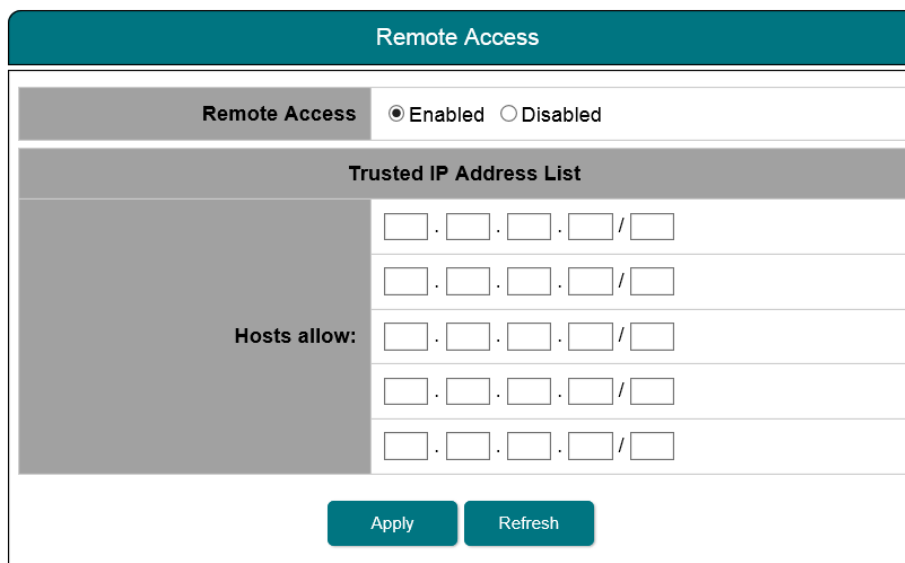
User can control the SABRE™ RANGER 5000 through Web Console remote access. Navigate to **Menu > Settings > Terminal Settings > Remote Access** to enable the Web Console remote access.



The screenshot shows the 'Remote Access' configuration page. At the top, there is a teal header with the text 'Remote Access'. Below the header, there is a section with a grey background and the text 'Remote Access' followed by two radio buttons: 'Enabled' (unselected) and 'Disabled' (selected). At the bottom of this section, there are two teal buttons: 'Apply' and 'Refresh'.

Figure 56

- i. Select **Enabled** to enable the remote access feature.
- ii. Select **Disabled** if you do not need the feature.
- iii. Click **Apply** for the new configuration to take effect.
- iv. Enter the allowed Global IP address of the devices.



The screenshot shows the 'Remote Access' configuration page with 'Enabled' selected. Below the radio buttons, there is a section with a grey background and the text 'Trusted IP Address List'. Underneath this, there is a label 'Hosts allow:' followed by five rows of IP address input fields, each in the format '□.□.□.□/□'. At the bottom of the page, there are two teal buttons: 'Apply' and 'Refresh'.

Figure 57

USER GUIDE

11.3.4.4 Power Saving

The screenshot displays the 'Power Saving' configuration page for the SABRE™ RANGER 5000. The page includes a navigation menu with 'Home', 'Settings', 'Terminal Settings', and 'Power Saving'. The main content area is titled 'Power Saving' and contains the following settings:

- Power Option:**
 - Default
 - Smart Ethernet
- Ethernet Settings:**
 - Ethernet Off
 - Ethernet On Demand
- Hibernation Settings:**
 - Hibernation
 - Wake-On PIN
 - Wake-On LAN
 - Schedules Wake-Up
- Hibernation Wake-Up Schedules:**
 - Schedule: Daily
 - Hours: 00 Hr(s)
 - Durations: 00 Min(s)
 - State: Enabled Disabled
 - Set button
- Hibernation Wake-Up Schedules Table:**

| Hours (HH) | Durations (Min) |
|---------------------------------------|-----------------|
| <input type="checkbox"/> 0 | 0 Min(s) |
| <input checked="" type="checkbox"/> 1 | 0 Min(s) |

Figure 58

USER GUIDE

11.3.4.5 Ciphering

Any data transmitted through the terminal will be encrypted under ciphering mode. User can enable this feature for added security.

Navigate to **Menu > Settings > Terminal Settings> Ciphering** to enable the Ciphering feature.

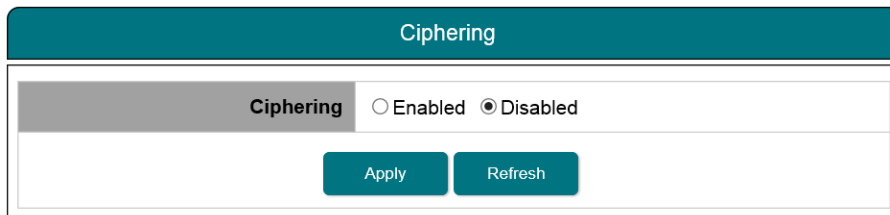


Figure 59

- i. Select **Enabled** to enable the ciphering feature.
- ii. Select **Disabled** if you do not need the feature.
- iii. Click **Apply** for the new configuration to take effect.

11.3.4.6 Facility Lock

Navigate to **Menu > Settings > Terminal Settings> Facility Lock** to enable the Facility Lock feature.

By default Facility lock is disabled



Figure 60

- i. Select **Enabled** to enable the facility lock feature.
- ii. Select **Disabled** if you do not need the feature.
- iii. Click **Apply** for the new **configuration** to take effect upon the next reboot.

USER GUIDE

11.3.4.7 IP Watchdog

IP Watchdog is a fail-safe feature that enables the SABRE™ RANGER 5000 to keep the IP connection alive. This can prevent the loss of IP connection due to unexpected causes and help the terminal to acquire the IP connection again.

There are two types of watchdog mechanism:

1. Periodic Reboot

The reboot is based on the pre-configured time period regardless of the connection status.

2. Ping based Watchdog

After all the pre-configured IP addresses failed to ping, the terminal will perform system reboot automatically. The Ping based Watchdog can only be activated when it is set in Multi-user router mode with active PDP context. User can define 3 sets of IP addresses. Based on the time intervals and numbers of tries, the terminal can verify whether the connection is still available. As long as the terminal is able to ping any of the IP addresses, the watchdog will not trigger a system reboot.

NOTE: In Single-user Router mode, the terminal will automatically disable Ping based Watchdog feature.

Navigate to **Menu > Settings > Terminal Settings > IP Watchdog** to enable the IP Watchdog feature.

Periodic Reboot

- i. Select **Enabled** to enable the Periodic Reboot feature.
- ii. Select **Disabled** if you do not need the feature.
- iii. Enter the duration for the terminal to trigger a periodic reboot.
- iv. Click **Apply** for the new configuration to take effect

Ping based Watchdog

- i. Select **Enabled** to enable the Ping based Reboot.
- ii. Select **Disabled** if you do not need the feature.
- iii. Enter the IP addresses with the number of retries (from 0 to 255).
- iv. Enter the test intervals (from 5 to 1440) minutes
- v. Click Update for the new configuration to take effect
- vi. Tick “No ping request if IP traffic is detected within the ping interval” to save the data usage.

Figure 61

USER GUIDE

11.3.4.8 I/O Configurations

The SABRE™ RANGER 5000 terminal incorporates an embedded serial device server (Serial to IP). With the Serial to IP capability, the data collected from the RS232 serial device can be retrieved locally through the local LAN or remotely through the Internet.

A serial device server can transfer the data between a computer serial (COM) port and an Ethernet LAN port.

It is recommended for connecting your RS232 serial device to an IP-based Ethernet LAN. The serial device server can support up to 4 simultaneous connections, which allows multiple clients to collect data from the same serial device concurrently.

Navigate to **Menu > Settings > Terminal Settings> I/O Configurations** to enable the serial device server.

Device Serial Server

- i. Select **Enabled** to enable the server.
- ii. Select **Disabled** to disable the server.

TCP/IP Settings

1. Time Configuration

TCP alive check time is the inactivity timeout (min) used to disconnect an idle TCP connection. By default, it is configured as 10 minutes.

- | | | |
|------------------|---|---|
| 0 minute | : | TCP connection will not be disconnected due to an idle TCP connection. |
| 1 to 99 minutes: | | Based on the TCP alive check time, the terminal will deactivate the TCP connection if no TCP activity within the configured period. After the connection is closed, the terminal will be standby for another host's TCP connection. |

TCP keep alive time is the time to keep the connection active in between the terminal and the remote PC. By default, it is configured as 0 minute.

If the user sets the keep alive time as 1 minute, the terminal will send an empty packet every 1 minute to ensure that the connection of the remote PC is still active.

Inactivity time is the reference idle time for a TCP connection to deactivate due to an idle serial data connection. By default, it is set as 0 minute.

- | | | |
|------------------|---|--|
| 0 minute | : | TCP connection will not be impacted by an idle serial data connection. |
| 1 to 99 minutes: | | Based on the inactivity time, the terminal will deactivate the TCP connection if no serial data activity within the configured period. After the connection is closed, the terminal will be standby for another host's TCP connection. |

USER GUIDE

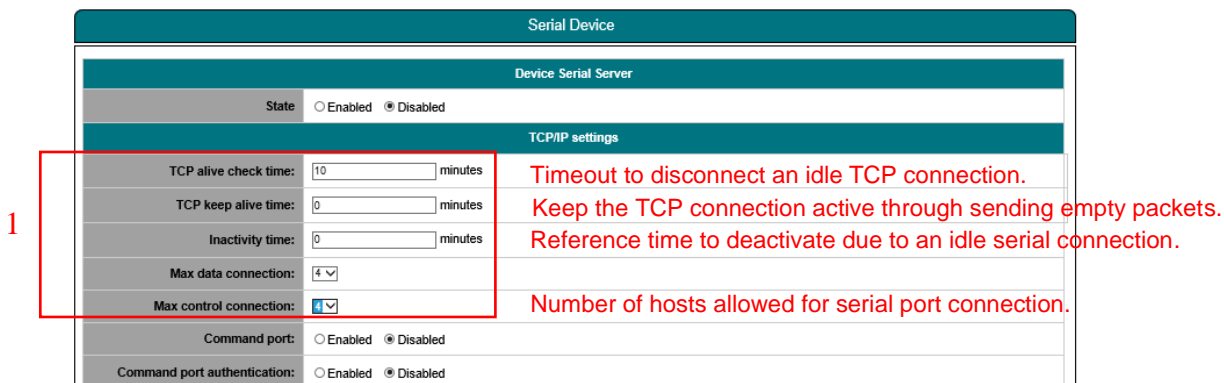


Figure 62

1. **Max connection** is used when the user needs to receive data from different hosts simultaneously.

By default the terminal only allows 1 connection at a time.

Max. connection 1: only one host to the specific serial port.
 Max. connection 2 to 4: Terminal allows 2 to 4 TCP connections to open the serial port simultaneously.

- i. Select **Enabled** to enable the Periodic Reboot.
- ii. Select **Disabled** if you do not need the feature.
- iii. Enter the IP addresses with the number of retries.
- iv. Enter the test intervals.
- v. Click **Apply** for the new configuration to take effect.

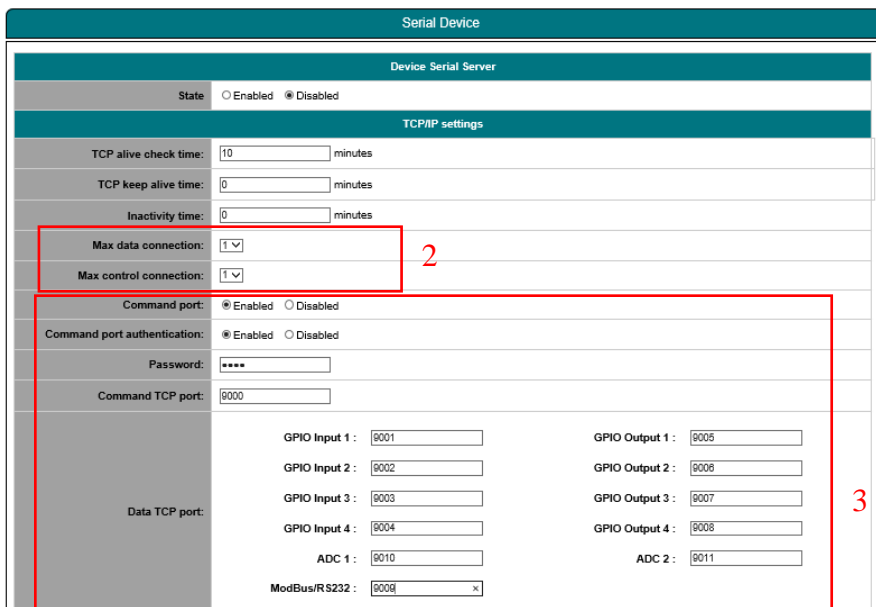


Figure 63

USER GUIDE

2. **Command Port** is used when the users need to retrieve data from the serial cable. It can be done through locally or remotely.
 - i. Select **Enabled** for **Command Port** and **Command Port Authentication** to enable this feature.
 - ii. By default, the password for command port is **1234**. Users are recommended to change the password for security purpose.

Command TCP port:

Control port for data transmission (example: 9000).
Standby for the host to prevent any conflict with other applications.

Data TCP port:

Acts as the TCP port that the data actually transmits through this port.
After establishing the connection, data can be transmitted in both directions, from PC to port 9001 and from port 9001 to PC.

User can define up to 4 GPIO input and output ports.

GPIO input can be a switch or sensor which can provide information to the terminal.
GPIO output can be a LED which can display the output.

ADC is used for voltage measurement.

ADC 1 - Internal supply voltage of the terminal.

ADC 2 - External supply voltage to the terminal.

Can be used to monitor the input voltage of a solar panel or an external battery.

3. **Serial Port Settings**

From the drop down menu, select the respective baud rates (from **4800** to **115200**).

The screenshot shows a web interface for 'Serial settings'. At the top, there's a teal header with the text 'Serial settings'. Below it, a 'Baudrate:' label is followed by a dropdown menu showing '4800'. A red box highlights this dropdown, and a red '4' is placed to its right. Below this is another teal header for 'Remote Control'. Underneath, there are two sections: 'Hosts allow:' and 'Hosts deny:'. Each section has five rows of IP address input fields, each consisting of four boxes for the octets and a slash for the port. At the bottom of the form, there is a note: 'Note: The deny list takes precedence over the allow lists.' and two buttons labeled 'Update' and 'Refresh'.

Figure 64

USER GUIDE

4. Remote Control of Serial Port Interface

For remote access, users need to know the Global IP address of the terminal. This information can be retrieved through Data Logs.

By default, the terminal accepts all the IP addresses.

Host Allow

IP address range (IP/CIDR) of the computer allowed for remote access.

Host Deny

IP address range (IP/CIDR) of the computer rejected for remote access.

USER GUIDE

11.3.4.9 Backup/Restore

Configuration settings can be saved and kept as a reference for the future.

To understand which configurations are included in the backup list, refer to [Appendix D: Backup Configuration Reference Table](#).

Navigate to **Menu > Settings > Terminal Settings > Backup/Restore** to save or restore the configuration settings.

Backup configuration settings

- i. Click Backup.
- ii. The settings will be saved as a document.

Restore configuration settings

- i. Browse the file location of previous backup file.
- ii. Click Restore.
- iii. Navigate to **Menu > Settings > Terminal Settings > Reboot Terminal** and click “Reboot terminal” to reboot the terminal for the new settings to take effect.

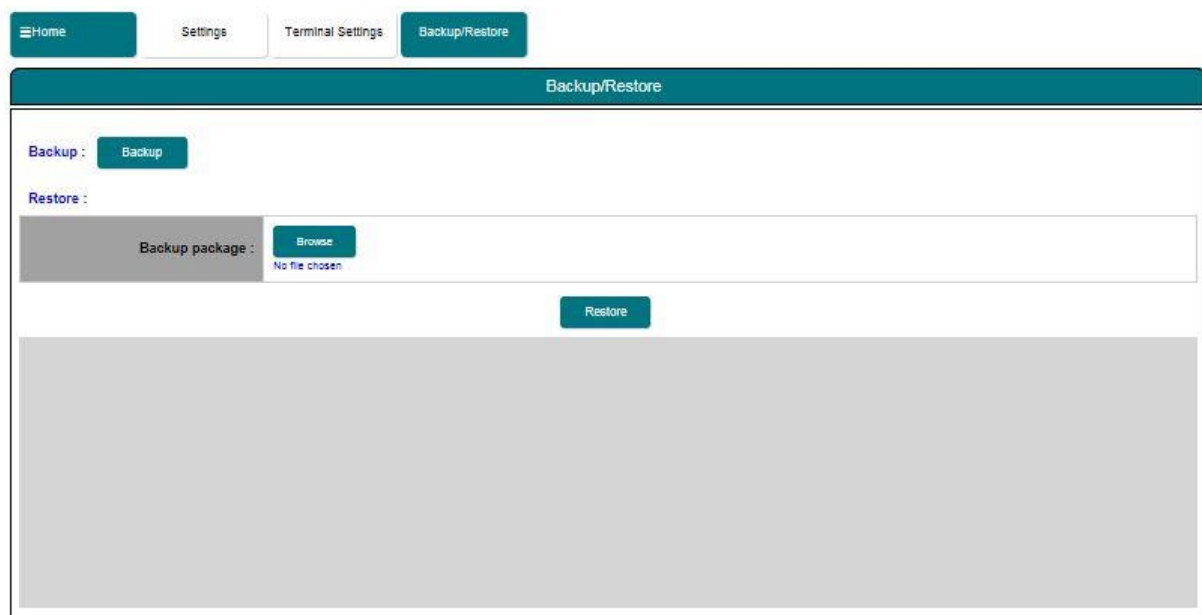


Figure 65

USER GUIDE

11.3.4.10 Web

For security purpose, user can change the port of the Web Console.

Navigate to **Menu > Settings > Terminal Settings> Web** to change the internet browsing port. By default, the port is 80.

- i. Enter the new port number. It can be any number from 1 to 65535.
- ii. Click **Update** for the setting to take effect.
- iii. Navigate to **Menu > Settings > Terminal Settings> Reboot Terminal** and click “Reboot terminal” to reboot the terminal for the new settings to take effect.

NOTE: After set the port number (e.g. 20), <http://192.168.1.35:20> is the address to login the Web Console.

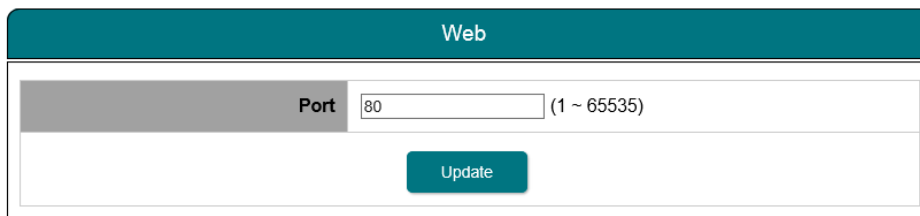


Figure 66

11.3.4.11 Antenna Pointing Buzzer

Navigate to **Menu > Settings > Terminal Settings> Antenna Pointing Buzzer** to enable Audio Assisted Pointing Mode. By default, the antenna pointing buzzer is disabled.

- i. Select **Enabled** to enable the antenna pointing buzzer.
- ii. Click **Update** for the setting to take effect.

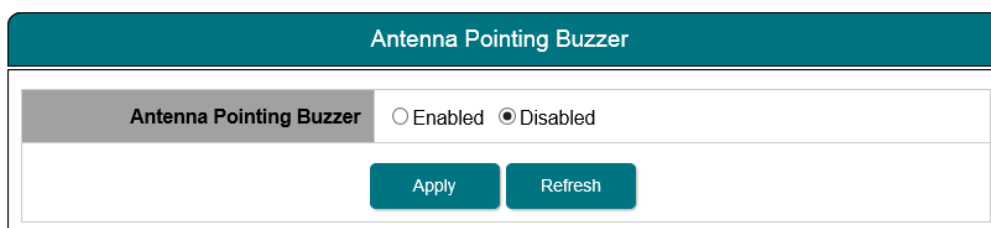


Figure 67

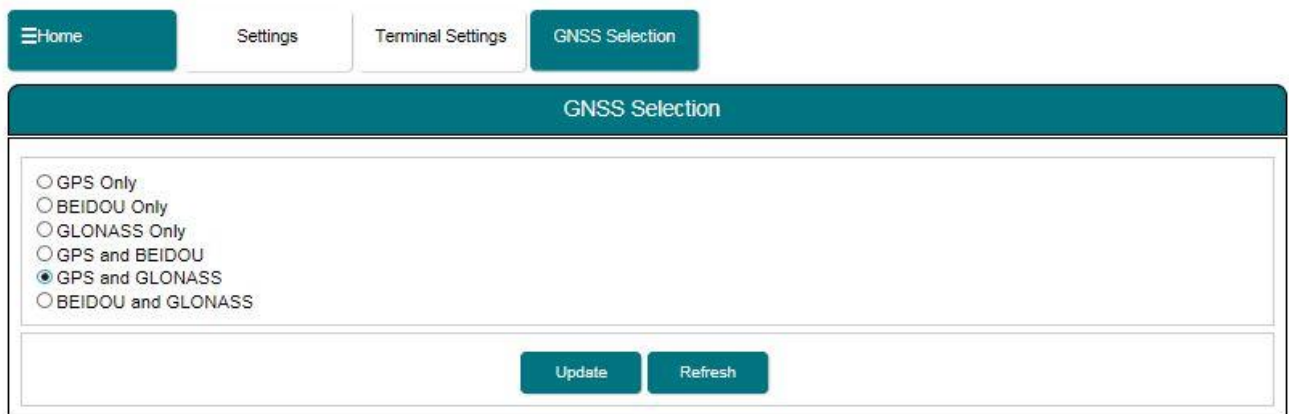
USER GUIDE

11.3.4.12 GNSS Selection

Navigate to **Menu > Settings > Terminal Settings > GNSS Selection**

- i. Select your GNSS option.
- ii. Click **Update** for the setting and reboot to take effect.

Factory default: GPS and GLONASS



Home Settings Terminal Settings GNSS Selection

GNSS Selection

GPS Only
 BEIDOU Only
 GLONASS Only
 GPS and BEIDOU
 GPS and GLONASS
 BEIDOU and GLONASS

Update Refresh

Figure 68

USER GUIDE

11.3.5 Terminal Info

Navigate to **Menu > Settings > Terminal Info > Information** in order to check for the detail of the terminal. You may need to supply this information when contacting your service provider.

Logs

Navigate to **Menu > Settings > Terminal Info > Logs** to view the Event Log or Error Log of the terminal. Click **Export all Logs** in order to export the logs.

Data Log

Navigate to **Menu > Settings > Terminal Info > Data Log** to view the data usage of the terminal. Click **Export all Logs** in order to export the logs.

From data log, user can check for the public IP address of the terminal.

Example: 161.30.22.119 for the current activated data session (status: in progress).

| Data Log | | | | | | | |
|-----------------|---------------------|--------------|--------------------------|--------------------------------|---------------|-------------------------|----------------|
| Data Log | | | | | | | |
| Connection Type | Date/Time | Duration | Volume (Upload/Download) | Uplink/Downlink Bitrate (kbps) | IP Address | APN (Access Point Name) | Cause |
| Background | 2013/11/21 11:02:55 | 000:05:03:19 | 1.64 MB / 3.32 MB | Dynamic / Dynamic | 161.30.22.119 | bgan.inmarsat.com | In progress... |
| Background | 2013/11/21 10:55:17 | 000:00:03:45 | 18.32 KB / 19.28 KB | Dynamic / Dynamic | 161.30.22.99 | bgan.inmarsat.com | Normal |
| Background | 2013/11/21 10:48:38 | 000:00:05:41 | 3.23 KB / 4.72 KB | Dynamic / Dynamic | 161.30.22.88 | bgan.inmarsat.com | Normal |

Figure 69

USER GUIDE

11.3.6 SMS Configurations

Navigate to **Menu > Settings > SMS Configurations > Remote Control** to configure the SMS remote control features.

By default, it allows all phone number to remotely control your terminal.

- i. Select **Enabled** to enable the SMS remote control feature.
- ii. Select **Allow only listed numbers** to allow only specific numbers.
You can configure up to 5 phone numbers.
- iii. Tick the **ACK SMS remote command** to receive an acknowledgement SMS from the terminal.
This may incur airtime charges depending on the service provider.
- iv. Enter the SMS password for the remote control.
- v. Click **update** for the feature to take effect.

NOTE: Refer to Sabre RANGER 5000 SMS Remote Control Feature User Guide for the SMS command.

Figure 70

11.3.7 Language

Navigate to **Menu > Settings > Terminal Info > Language** to select the desired language.

The default language is English.

English and Chinese Simplified are available for your selection.

11.3.8 Support

Navigate to **Menu > Settings > Terminal Info > Support** to get the contact information of your service provider's support team.

11.3.9 About

Navigate to **Menu > Settings > Terminal Info > About** to get the contact information of the manufacturer.

USER GUIDE

12. Web Console in Safe Mode

Safe Mode is a simple version of the normal Web Console with some basic settings. If you could not access the Web Console in normal way, you can try to access the Web Console in the Safe Mode.

ENABLING SAFE MODE

There are two methods for enabling the Safe Mode.

Method 1: Enter Safe Mode through Web Console (Normal Mode)

- i. With the terminal powered on, connect personal computer to the SABRE™ RANGER 5000 via Ethernet cable.
- ii. Login to Web Console by typing **http://RANGER5000** or **http://192.168.1.35** into the address bar of any web browser.
- iii. Navigate to **Menu > Settings > Terminal Settings> Firmware Upgrade** to perform a firmware upgrade. Your terminal will reboot in Safe Mode once you click the Firmware Upgrade button.
- iv. If Safe Mode is enabled successfully, the Antenna Pointing LEDs are solid green.
- v. Login to the Web Console in safe mode by typing **http://RANGER5000** or **http://192.168.1.35** into the address bar of the web browser again.

Method 2: Enter Safe Mode through physical buttons.

- i. With the terminal off, press and hold 'Safe Mode Switch'.

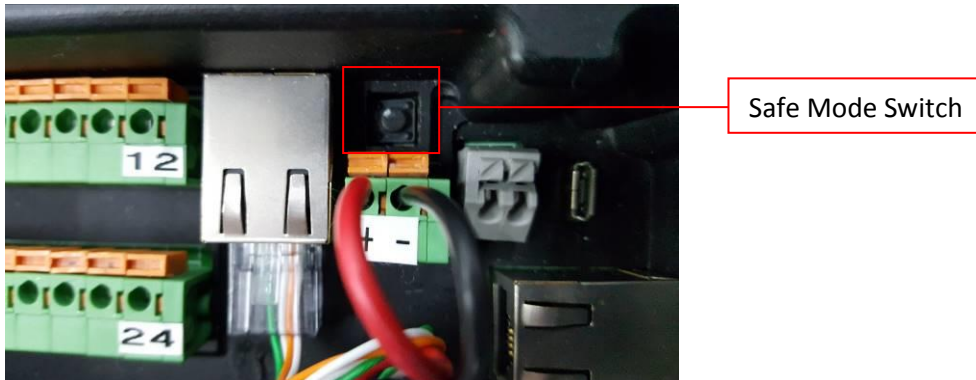


Figure 71

- ii. In parallel, power up the terminal.
- iii. Release 'Safe Mode Button' after 5 seconds.
- iv. If Safe Mode is enabled successfully, the Antenna Pointing LEDs are solid green.
- v. Login to the Web Console in safe mode by typing **http://RANGER5000** or **http://192.168.1.35** into the address bar of any web browser.

NOTE:

The username and password of the Web Console are the same for Normal Mode and Safe Mode.

USER GUIDE

MENU OVERVIEW

SETTINGS

- Reboot
- Factory Reset
- Terminal Info
- Logs
 - Event
 - Error

REBOOT

Navigate **Menu > Settings > Reboot** to reboot and switch the terminal to Normal Mode.

FACTORY RESET

Navigate to **Menu > Settings > Factory Reset** to factory reset the terminal.
Enter security code for factory reset (Default: 0000).

NOTE:

By default, the security code is 0000. Once you change the Terminal PIN, the Factory Reset password is changed to match the Terminal PIN.

TERMINAL INFO

Navigate to **Menu > Settings > Terminal Info** to check for the detail of the terminal.
You may need to supply this information when contacting your service provider.

LOGS

Navigate to **Menu > Settings > Log** to view the Event Log or Error Log of the terminal.
Click **Export all Logs** in order to export the logs.

USER GUIDE

13. Appendix A: Terminal Block Pin Assignment



Terminal block pin assignment:

| | | | | | | | | | | | |
|-----|---------|---------|-----|---------|---------|-----|------------------------|----------------------|-----|---------------------|-------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| GND | OP 3 | OP 4 | GND | IP 3 | IP 4 | GND | RS232/TX RS485/Z(B) | RS232/CTS RS485/B | GND | RS232/RX RS485/A | RS232/RTS RS485/Y(A) |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| TDR | OP 1 | OP 2 | GND | IP 1 | IP 2 | GND | Analog Input | Local Wakeup | GND | RS232/ RX | RS232/ TX |

Figure 72

USER GUIDE

Terminal block pin assignment Table:

| Pin # | Name | Description | Remark |
|-------|-------------------------|------------------------|--|
| 1 | GND | GROUND | |
| 2 | OP 3 | DIGITAL OUTPUT 3 | Max +40V |
| 3 | OP 4 | DIGITAL OUTPUT 4 | Max +40V |
| 4 | GND | GROUND | |
| 5 | IP 3 | DIGITAL INPUT 3 | Max +32V |
| 6 | IP 4 | DIGITAL INPUT 4 | Max +32V |
| 7 | GND | GROUND | |
| 8 | RS232/TX RS485/Z(B) | | Software Configurable RS232/RS485 Factory default to: RS232 |
| 9 | RS232/CTS RS485/B | | Software Configurable RS232/RS485 Factory default to: RS232 |
| 10 | GND | GROUND | |
| 11 | RS232/RX RS485/A | | Software Configurable RS232/RS485 Factory default to: RS232 |
| 12 | RS232/RTS RS485/Y(A) | | Software Configurable RS232/RS485 Factory default to: RS232 |
| 13 | TDR | TERMINAL DATA READY | Open Drain Output Pin Max +40V |
| 14 | OP 1 | DIGITAL OUTPUT 1 | Max +40V |
| 15 | OP 2 | DIGITAL OUTPUT 2 | Max +40V |
| 16 | GND | GROUND | |
| 17 | IP 1 | DIGITAL INPUT 1 | Max +32V |
| 18 | IP 2 | DIGITAL INPUT 2 | Max +32V |
| 19 | GND | GROUND | |
| 20 | Analog Input | | Max +32V |
| 21 | Local Wakeup | | Max +32V |
| 22 | GND | | |
| 23 | RS232/RX | | Debug Log Output only |
| 24 | RS232/TX | | Debug Log Output only |

USER GUIDE

14. Appendix B: Conduit & Accessories

You may use the conduits and accessories listed below in your installation. These are provided for your reference only. Depending on your installation requirements, some or all of these parts may not be suitable for your application.

www.Schlemmer.com

- 1) 1200232 NW23 Black PA6 corrugated pipe ID23.2 X OD28.9 mm
- 2) 3805013 M25 male straight connector, black PA6 c/w gasket IP65
- 3) 7211977 Black PA6 M25 locknut
- 4) 6402212 Nickel Plated Brass Adaptor male NPT 3/4" female M25

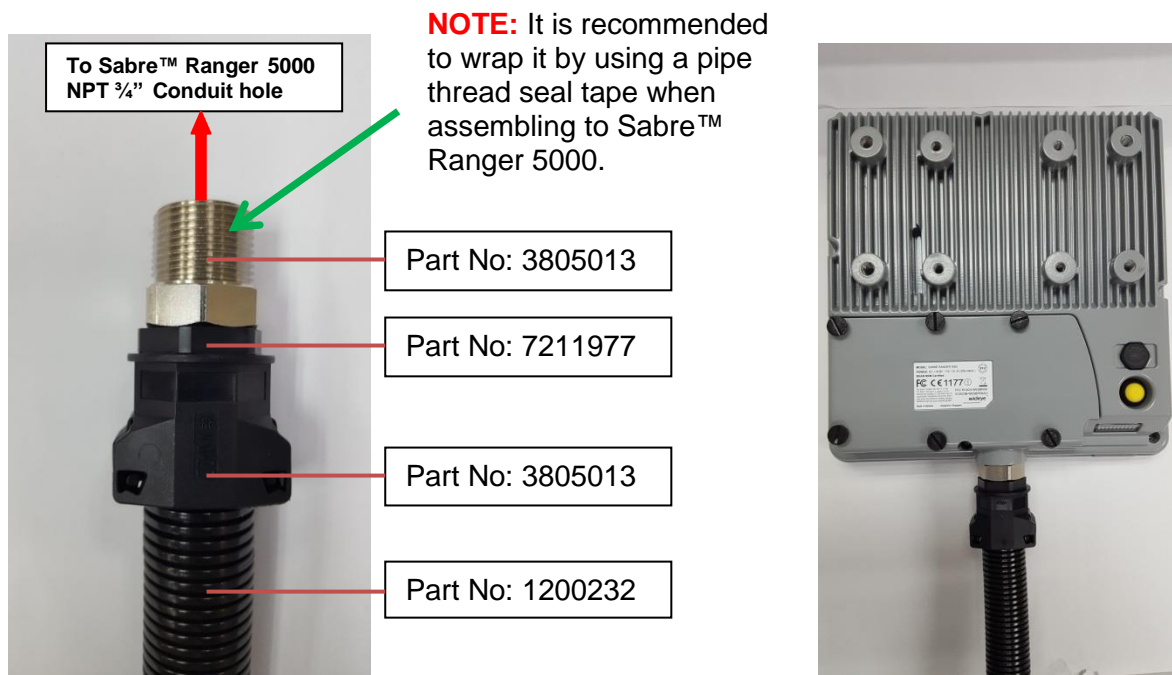


Figure 73

Assembly View

USER GUIDE

15. Appendix C: Technical Summary

Frequency Band

Receive: 1518MHz - 1559MHz

Transmit: 1626.5MHz - 1660.5MHz and 1668 – 1675MHz

Antenna

Type: Built-in patch antenna

GNSS Air Interface

Integrated GPS receiver and antenna

Support: GPS / Beidou / Glonass

Bearer Data Rate

M2M SIM

Standard IP: Up to 448/464kbps (send /receive)

BGAN SIM

Standard IP: up to 448/464kbps (send /receive)

Symmetric Streaming IP: Up to 32, 64,128kbps

Services

Standard IP, Streaming IP (BGAN SIM Only), SMS

Interfaces

2 x RJ45 Ethernet Ports (RJ45)

2 x 12 PIN Terminal Block

1 x RS232 / RS485 with Modbus

1 x RS232 (debug)

4 x GPIO – Output

4 x GPIO – Input

1 x Analog Input Port

1 x Local wakeup - Input

1 x Power Supply Input (2 wires) Terminal Block

1 x DC Output (2 wires) Terminal Block

1 x Antenna Pointing Switch

5 x Antenna Pointing LED

1 x Antenna Pointing Buzzer

1 x Safe mode button

1 x SIM card holder

1 x Micro USB (Reserved)

Firmware Upgrades

Over-the-air or via Ethernet Port

USER GUIDE

Supports 3GPP AT Commands

OS Agnostic (supports access via Web-MMI)

Environmental

| | |
|---------------------|--------------------------|
| Operating Temp: | -40°C to +75°C |
| Operating Humidity: | 95% (Condensing at 40°C) |
| Storage Temp: | -40°C to +80°C |
| Storage Humidity: | 5% to 95% (RH) |
| Water & Dust: | IP66 compliant |

Electrical

| | |
|-----------------|------------------|
| DC input range: | +10.8V to +32V |
| Power (max): | 30W (excluding*) |
| *DC output: | +12V Max 1A |

Power Consumption

| | |
|-------------------------|----------------|
| Receive: | <6 W |
| Transmit: | 20 W (typical) |
| Standby mode: | <1 W |
| Low power standby Mode: | < 50mW |

Weight

~2.5Kg

Dimensions

241(L) x 239(W) x 71(H) mm

Wind loading

Up to 125 mph (200kph) with mounting bracket is supplied by Addvalue Innovation Pte Ltd.

Regulatory Approvals

CE
 FCC
 IC (Industry Canada)
 UL Safety Mark
 NEMA Type 4X
 RoHS
 IP66
 Class 1 Div. 2 Certified
 Inmarsat Type Approval

USER GUIDE

16. Appendix D: Backup Configuration Reference Table

| | |
|--|--|
| <p>Data</p> <p><u>Data Profile</u></p> <ul style="list-style-type: none"> -Firewall <li style="padding-left: 20px;">-Setup <li style="padding-left: 20px;">-HTTP Filters <p><u>Port Forwarding</u></p> <p><u>Data Settings</u></p> | <p>SETTINGS</p> <p><u>Accounts</u></p> <ul style="list-style-type: none"> -Ethernet <ul style="list-style-type: none"> - MAC Filtering -Terminal Settings <ul style="list-style-type: none"> - Remote Access - IP Watchdog - Serial Device (not included yet) - SMS - Remote Control <p><u>Language</u></p> |
|--|--|

Whilst the above information has been prepared by Addvalue Innovation Pte Ltd ("Addvalue") in good faith, and all reasonable efforts have been made to ensure its accuracy, Addvalue makes no warranty or representation as to the accuracy, completeness or fitness for purpose or use of the information. Addvalue shall not be liable for any loss or damage of any kind, including indirect or consequential loss, arising from use of the information and all warranties and conditions, whether express or implied by statute, common law or otherwise, are hereby excluded to the extent permitted by law of Singapore. Addvalue, the Addvalue Enabled logo, Wideye, and the Wideye logo are either trademarks or registered trademarks of Addvalue Technologies Ltd and/or its affiliates in Singapore and/or other countries.