HUGHES
An EchoStar Company

EchoStar Mobile™

Hughes 4500
User Guide

H62751
Revision B
May 20, 2020

11717 Exploration Lane, Germantown, MD 20876

Phone (301) 428-5500 Fax (301) 428-1868/2830

Contents

Understanding safety alert messages

Safety alert messages call attention to potential safety hazards and tell you how to avoid them. These messages are identified by the signal words DANGER, WARNING, CAUTION, or NOTICE, as illustrated below. To avoid possible property damage, personal injury, or in some cases possible death, read and comply with all safety alert messages.

Messages concerning personal injury

The signal words DANGER, WARNING, and CAUTION indicate hazards that could result in personal injury or in some cases death, as explained below. Each of these signal words indicates the severity of the potential hazard.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury.

Messages concerning property damage

A NOTICE concerns property damage only.

NOTICE

NOTICE is used for advisory messages concerning possible property damage, product damage or malfunction, data loss, or other unwanted results—but *not* personal injury.

Safety symbols

The generic safety alert symbol

calls attention to a potential personal injury hazard. It appears next to the DANGER, WARNING, and CAUTION signal words as part of the signal word label. Other symbols may appear next to DANGER, WARNING, or CAUTION to indicate a specific type of hazard (for example, fire or electric shock). If other hazard symbols are used in this document, they are identified in this section.

Additional symbols

This document uses the following hazard symbols:

Warning: Potential Radio Frequency (RF) hazard. Where you see this alert symbol and WARNING heading, strictly follow the warning instructions to avoid injury to eyes or other personal injury.

Warning: Where you see this alert symbol and WARNING heading, strictly follow the warning instructions to avoid personal injury.

Danger: Electric shock hazard: Where you see this alert symbol and DANGER heading, strictly follow the warning instructions to avoid electric shock injury or death.

Warnings for satellite terminal

CAUTION

Do Not Stand near by the Antenna: This device emits radio frequency energy. To avoid injury, do not place head or other body parts in front of the satellite antenna when system is operational. Maintain one meter distance or more from the terminal while active is the warning.

General: Handle your Satellite Terminal with care. The unit is weather resistant per IEC 60529 IP67; however, do not submerge the unit. Avoid exposing your Satellite Terminal to extreme hot or cold temperatures outside the range -25° C to +65° C.

Avoid placing the Terminal close to cigarettes, open flames or any source of heat.

Changes or modifications to the Terminal not expressly approved by Hughes Network Systems could void your authority to operate this equipment.

Only use a soft damp cloth to clean the Terminal.

To avoid impaired Terminal performance, please ensure the unit's antenna is not damaged or covered with foreign material like paint or labeling.

When inserting the SIM, do not bend it or damage the contacts in any way. When connecting the interface cables, do not use excessive force.

In the Vicinity of Blasting Work and in Explosive Environments: Never use the Satellite Terminal where blasting work is in progress. Observe all restrictions and follow any regulations or rules. Areas with a potentially explosive environment are often, but not always, clearly marked. Do not use the Terminal while at a petrol filling station. Do not use near fuel or chemicals.

Qualified Service: Do not attempt to disassemble your Satellite Terminal. The unit does not contain consumer-serviceable components. Only qualified service personnel may install or repair equipment.

Accessories: Use Hughes approved accessories only. Use of non-approved accessories may result in loss of performance, damage to the Satellite Terminal, fire, electric shock or injury.

Connecting Devices: Never connect incompatible devices to the Satellite Terminal. When connecting the Satellite Terminal to any other device, read the device's User Manual for detailed safety instructions.

⚠ CAUTION

Pacemakers: The various brands and models of cardiac pacemakers available exhibit a wide range of immunity levels to radio signals. Therefore, people who wear a cardiac pacemaker and who want to use a Satellite Terminal should seek the advice of their cardiologist. If, as a pacemaker user, you are still concerned about interaction with the Satellite Terminal, we suggest you follow these guidelines:

- Maintain a distance of one meter from the main antenna front and sides and your pacemaker
- Refer to your pacemaker product literature for information on your particular device

If you have any reason to suspect that interference is taking place, turn off your Satellite Terminal immediately.

⚠ CAUTION

Hearing Aids: Most new models of hearing aids are immune to radio frequency interference from Satellite Terminals that are more than 2 meters away. Many types of older hearing aids may be susceptible to interference, making it very difficult to use them near a Terminal. Should interference be experienced, maintain additional separation between you and the Satellite Terminal.

⚠ CAUTION

Electrical Storms: Operation of the Satellite Terminal during electrical storms may result in severe personal injury or death.

Equipment users

User must be a skilled person. Designated users should not be exposed to conditions that could cause pain or injury, nor intentionally caused said conditions.

Chapter 1

Introduction

Overview

The Hughes 4500 Terminal provides reliable satellite connectivity over the EchoStar Mobile GMR-1 3G satellite network. The Hughes 4500 Terminal comes in a very small form factor and it allows the user to send and receive IP packets via Ethernet.

Figure 1: Hughes 4500 Terminal

About this user guide

This user guide contains the most up-to-date information available on this product on the date it was generated. It is focused on the specific information needed to operate the Hughes 4500 terminal and to connect to the EchoStar Mobile Satellite network. If you are a first time user, you will be guided through the procedure for powering up your terminal, obtaining a GPS fix, connecting your computer to the terminal and registering with the network. You are then ready to start using data services.

Package contents

When you unpack the Hughes 4500 Portable Terminal kit package, you will find the following:

- Hughes 4500 Terminal
- Quick Start User Guide

Your Service Provider will supply you with a UMTS Subscriber Identification Module (USIM) and its PIN, and Satellite Terminal configuration instructions – you will need these to access the satellite network.

Minimum system requirements for laptop/PC

These are the minimum computer system requirements for successful interface with the Satellite Terminal:

- Internet Browser: Microsoft Internet Explorer (IE11 or later), Mozilla Firefox, Chrome, or Safari
- PC Support for Ethernet
- PC Support for USB

System Requirements to support maintenance port

To support the maintenance port, intended as the USB port, the following Operating System (OS) have been tested and they do not require the installation of any USB drivers:

- Microsoft Windows 7
- Microsoft Windows 10

Additional Hardware

Please refer to the Hughes catalog and pricelist for the purchase of any optional additional hardware items.

Table 1: Additional Hardware Items from the Hughes catalog

Item	Part Number	Specifications
Magnetic Mounting Kit	3501354-0001	High quality corrosion resistant plate with two circular magnets attached, ideal for vehicular installations
Fixed Mounting Bracket	3501353-0001	High quality corrosion resistant angle bracket ideal for vertical installations
Power & Data Cable, blunt wire, 5m	3501314-0002	Blunt wire including the mating barrel connector to the 4500 Terminal
Power & Data Cable, blunt wire, 10m	3501314-0003	Blunt wire including the mating barrel connector to the 4500 Terminal
Power & Data Cable, cig lighter plug & RJ45 socket, 5m	3501314-0004	Ideal for temporary vehicular installations
Mating Power & Data Connector, bare	9509554-0001	For custom cable installations
Custom Power & Data Cable, 8.5mm OD, 100m	9509573-0001	For custom cable installations

Chapter 2

Using the Hughes 4500

Before getting started

NOTICE

Install the USIM into the terminal unit before powering up the unit.

Figure 2: Inserting the USIM card

Quick start

The Hughes 4500 terminal must first obtain a GPS fix by positioning it with an open view of the sky. The GPS fix is acquired by the time the terminal is fully booted up. This time is typically specified at 30 sec.

Connecting the terminal to the computer

You can connect your computer to the Hughes 4500 with one or more of the following interfaces:

- Ethernet
- Micro-USB

Connecting by Ethernet

To connect the Hughes 4500 terminal to a device using Ethernet:

- Connect a standard Ethernet cable to the Ethernet signals of the barrel connector.

Connecting by USB

The common installation access port for Installers is the Micro-USB port. To connect the Hughes 4500 terminal to a device using USB:

- Connect a standard Micro-USB cable to the Micro-USB signals of the barrel connector.

NOTICE

The USB port can be only used for configuration. It cannot be used for user data connections over the satellite link.

Chapter 3

Using the Web UI

Accessing the Web UI

The Hughes 4500 includes an internal Web User Interface (Web UI). To access the Web UI, open your favourite web browser and type in the internal IP address of the terminal. If you are using a:

- Ethernet port, type this Ethernet IP address: http://192.168.128.100
- USB port, type this Maintenance IP address: http://169.254.1.1

The Web UI opens up to the **Terminal Status** page. Along the top of all Web UI pages are icons representing the categories of available subpages; **Home, Connections, Settings, Usage** and **Support**.

Home page

The Home page shows the current terminal status and allows user to set up the initial data connection.

On the left side of the page is the **Status** bar. These items are updated automatically when the status of any item changes.

1. **Connection:** This field indicates whether you are registered with the EML Network. It also shows if you are registered with the IMS and receive signal strength.
2. **Position:** This field displays the current position status. If the terminal acquired a GPS fix, it will display the Latitude, Longitude, Altitude, the last time the GPS position was updated and the geocoordinates in the Military Grid Reference System. Time displayed is UTC time.
3. **Terminal Properties:** This field indicates miscellaneous status information.

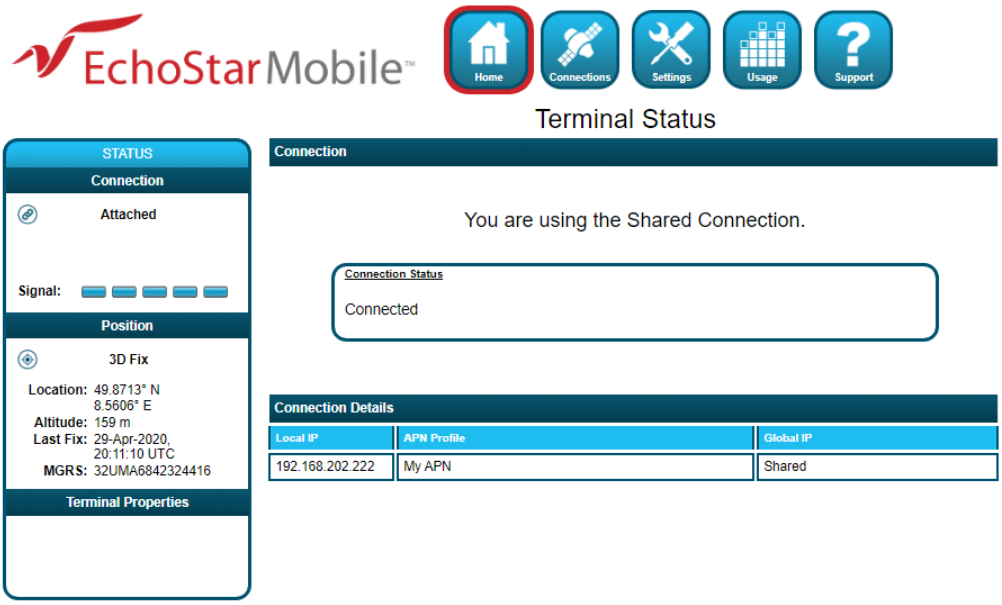

Figure 3: Terminal Status page

Once connected to the network, the Terminal Status page will show that the UT is registered with the network. In the middle of the Terminal Status page it will show that the "Shared Connection" is established along with the TE's local IP address.

For a basic connectivity, the Terminal would work with one signal bar. For more details the user can look at the diagnostics page to see if the signal quality (SQI) is at least 5dB. It is desirable to have 10dB or better.

Connections

The **Connections** page shows the status of the Shared Connection and the two Custom Connections or Dedicated Connections. Each connection shows the Local IP address associated with that connection and the Profile. It also shows the Global IP address for active Custom connections.

- **Shared Connection –** This section shows the Connection status, the global IP address and an Action button to disconnect the connection.
- **Connected Devices Using the Shared Connection –** This section shows the local IP addresses of all devices connected to the Shared Connection.
- **Dedicated Connection 1 and Dedicated Connection 2 –** This section shows the local IP, the APN Profile, the global IP address and an Action button to disconnect the connection.

To start a Custom connection with the network, select one of the APN Profiles from the drop-down menu and then click the Connect button. Once connected, a global IP address will be populated and the Connect button will change to Disconnect.

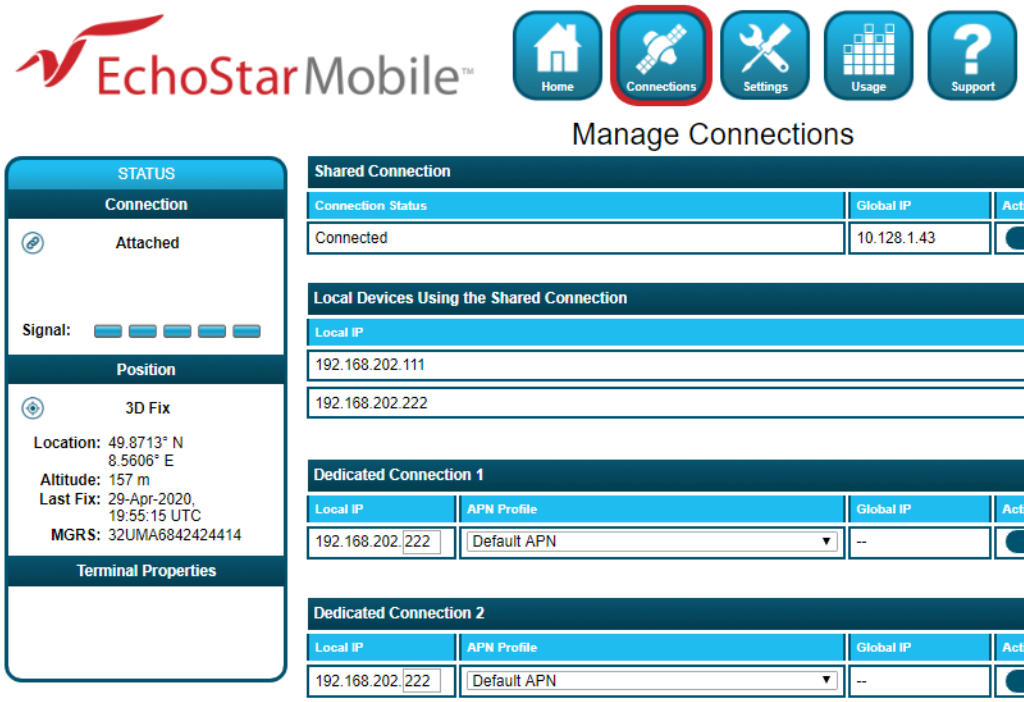

Figure 4: Connection page

Settings page

The Settings page provides a set of subpages for the configuration of various parameters of the terminal:

- **General Setup**
- **IP Address/DHCP**
- **Ethernet Security**
- **Security**
- **APN Profiles**
- **Connection Profiles**
- **Outbound Filters**
- **Port Forwarding**
- **Remote Management**

General setup

This subpage allows the user to configure general parameters of the Hughes 4500 Terminal. A description of each item is as follows:

- **Language –** The user can choose between the different language options by clicking the drop-down arrow, select the language and then click the Apply Changes button.
- **LED Settings –** The user can select between 3 different ways to turn off LED indicators, in normal operating mode. By clicking the drop-down arrow, select the option and then click the Apply Changes button.

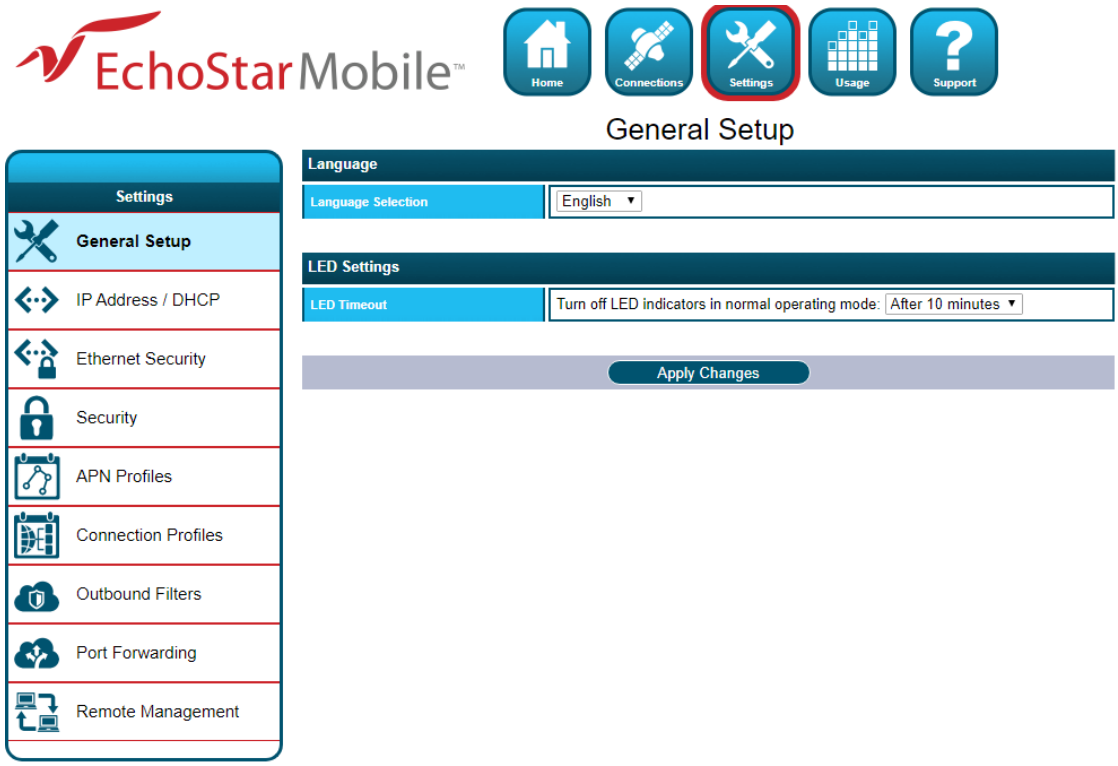

Figure 5: Setting page

IP Address/DHCP Settings

- **Terminal Local IP Address –** This section allows the user to change the local IP address of the terminal from the default Ethernet IP address: **192.168.128.100**. All four octets are available to change. Once the local IP address is changed on this page and applied, the first 3 octets of the DHCP address range will also change automatically.
- **DHCP Server –** Allows the DHCP server in the UT to be turned on or off by checking the Enable box.
- **DHCP Address Range –** This allows the user to set the range of DHCP addresses (from .101 to .199) that are given out by the UT to connected TEs.

  Updates to the Local IP address and DHCP server will **not** take effect until the UT is **rebooted**.

- **DHCP Reservations –** This section allows the user to add an IP address that will permanently be assigned to a particular connected device based upon the detected device's MAC address.

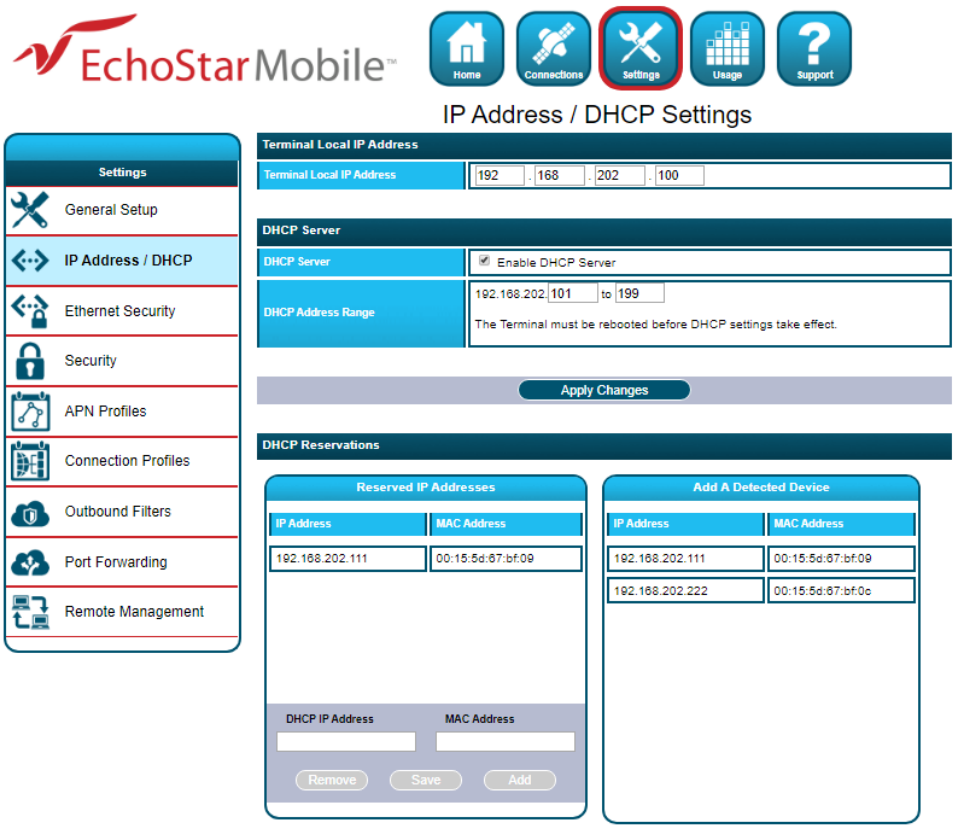

Figure 6: IP Address/ DHCP screen

Ethernet security

The Ethernet Security page allows the user to enable **Ethernet MAC Address Filtering**.

- **Ethernet MAC Address Filtering –** User can select any detected device and add the MAC address to the Allowed MAC Addresses field to the left. The user can also manually add a MAC address in the box at the bottom of the page, then add it to the Allowed MAC Address field.

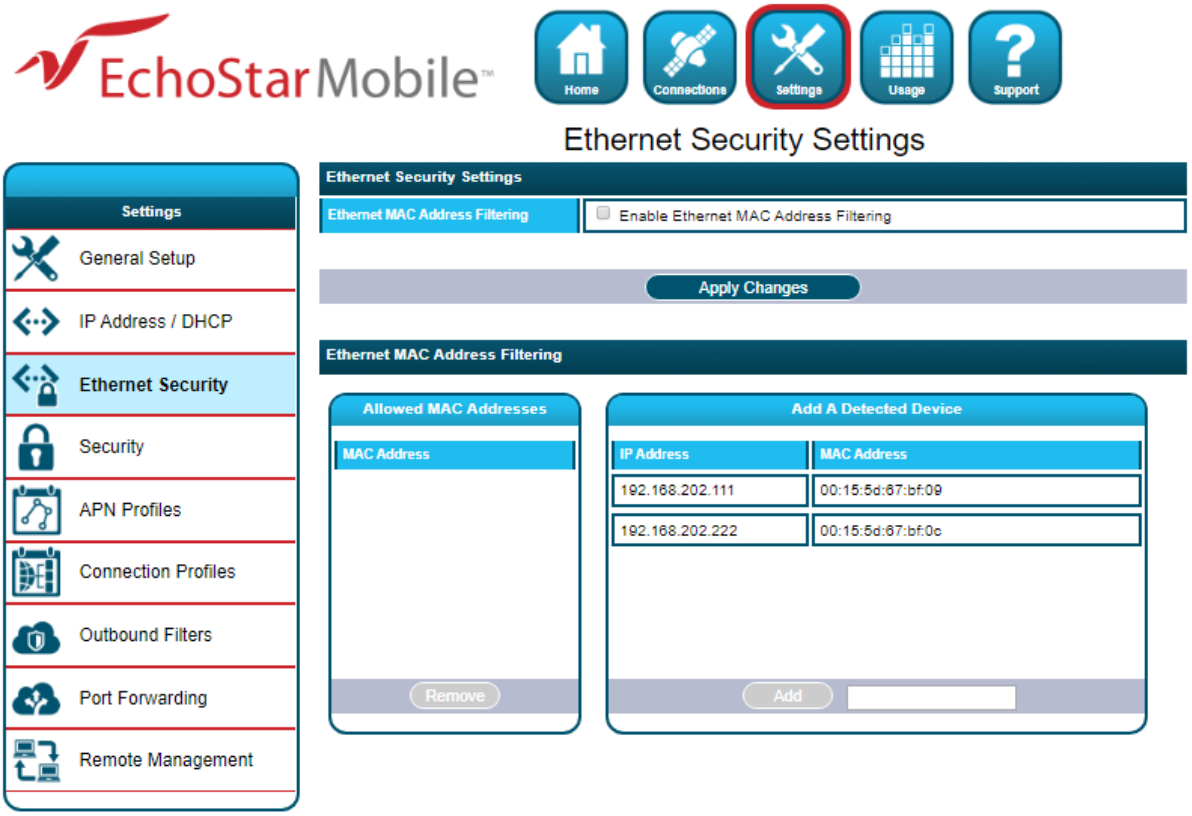

Figure 7: Ethernet Security screen

Security

This page allows the user to setup and enable/disable various passwords for the terminal.

- **SIM PIN –** This is a four-digit field that can be enabled and configured by the user to secure the SIM against unwanted use. The SIM PIN is stored on the SIM itself. Once enabled, the terminal will require the SIM PIN at startup.

  Note: After 3 incorrect attempts to enter the PIN, the user will have to use the PUK number to reset the PIN of the SIM car.

- **SIM Lock PIN –** Use up to 8 digits to lock the terminal to the current SIM card. The SIM Lock PIN code will have to be entered any time a different SIM card is used with the terminal.
- **Local Access Password –** This password prevents all local access to the terminal settings from being viewed or changed by unauthorized users once the terminal is configured properly. Once enabled, this password will have to be entered before any settings can be changed. A pop-up will come up if the Local Access Password is enabled and the user attempts to change a protected configuration parameter.
- **Administration Password –** This password allows to prevent terminal settings from being changed by unauthorized users once the terminal is configured properly. Once enabled, this password will have to be entered before protected settings can be changed. A pop-up will come up if the Administration Password is enabled and the user attempts to change a protected configuration parameter.

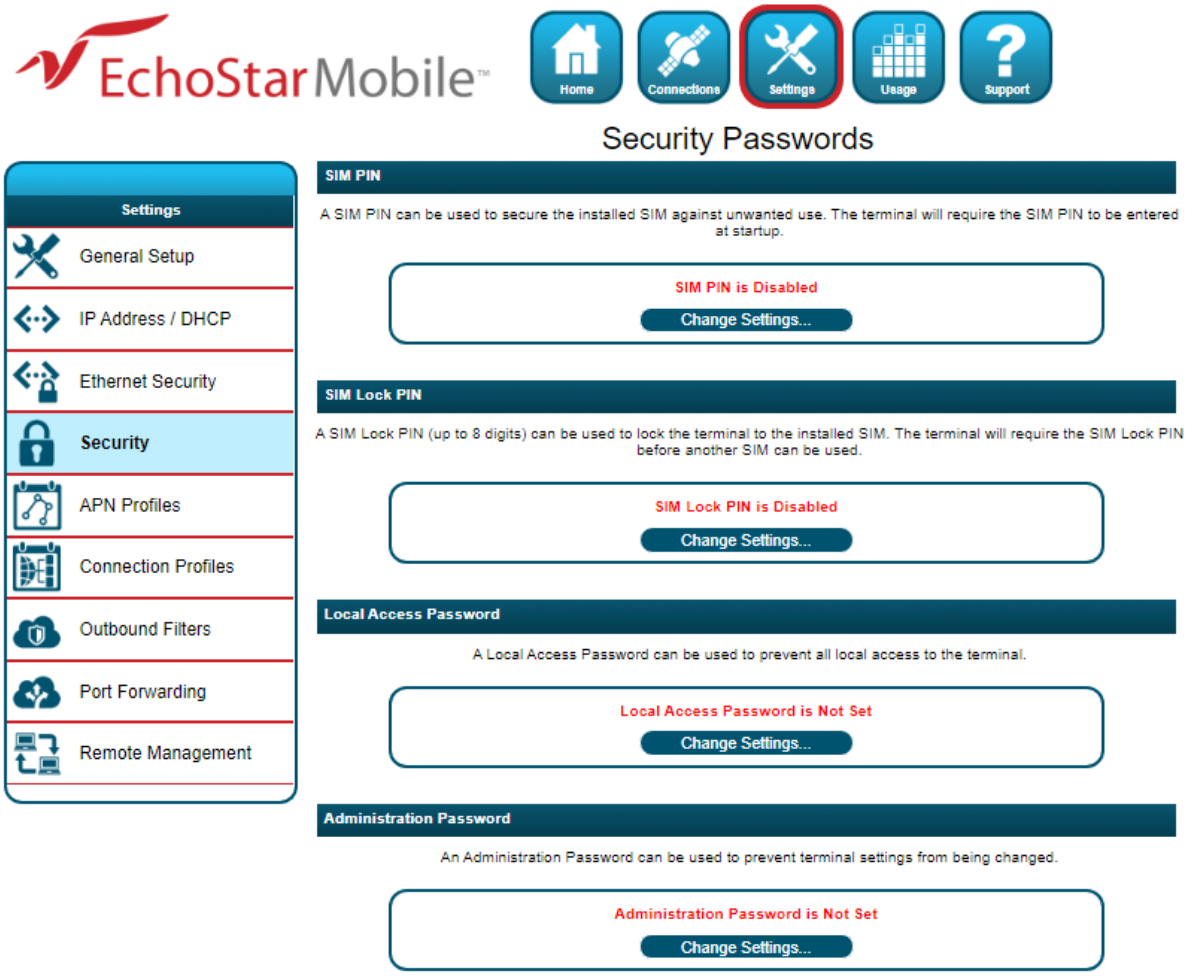

Figure 8: Security screen

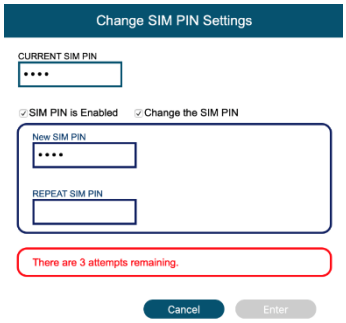

Figure 9: Change SIM PIN Settings screen

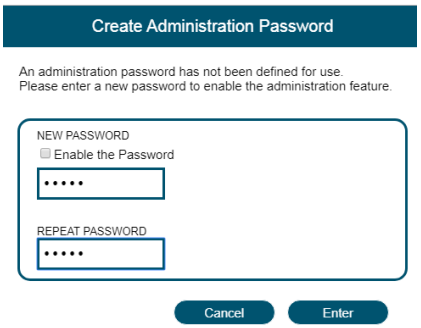

Figure 10: Create Administration Password screen

APN Profiles

- **Profile Settings –** This section allows the user to choose the Default APN Profile, selecting from the drop-down menu the APN Profile and clicking to Apply Changes. At least one Profile needs to be configured and selected as the Default Profile.

  The SW also supports APNs stored on the USIM. If available, the USIM APN is automatically set as the Default APN.

- **Defined APN Profiles –** This section allows the user to configure up to five APN Profiles by entering:

  — Profile Label
  — Profile APN
  — APN Username, the username is not required but optional.
  — APN Password, the password is not required but optional.

  The profile can be configured to prompt for the password when selecting it for use.

Figure 11: APN Profiles screen

Connection Profiles

This page allows to configure the user data connections (Shared and Dedicated) choosing the APN Profile and the Activation Method.

- **Connection Watchdog** – This section allows the user to enable the Connection Watchdog feature.

  When the feature is enabled, the traffic on the space link is monitored and the terminal will reboot if there is no traffic detected during the monitoring period. The user can also configure the following:

- **Traffic Monitoring**
  - Do not monitor
  - Monitor only incoming
  - Monitor only outcoming
  - Monitor bi-directional
- **Traffic Monitoring Timeout**

  The default duration is 60 minutes. If the user wants to change the duration this needs to be at least 5minutes.

  Note: The Traffic Monitoring Timeout needs to be programmed for a longer duration than anticipated rate of user traffic to avoid unnecessary reboots.

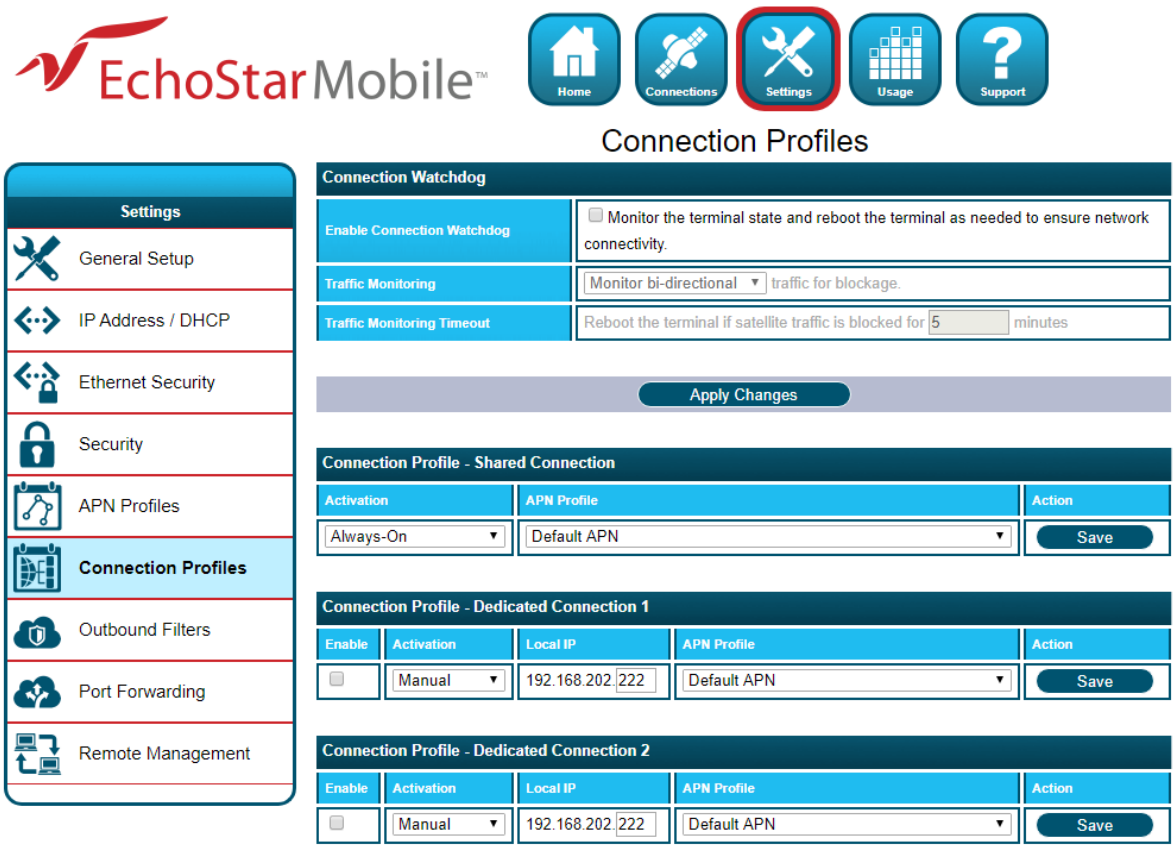

Figure 12: Connection Profiles screen

- **Connection Profile - Shared Connection** – This section allows the user to define the APN Profile of the Shared Connection. And how the Shared Connection is established. The user can select the options available from the drop-down menu and click the Save button.
  - **Activation Method**
    - Manually: the user manually connects and disconnects the connection on the WebUI.
    - Always-On: the connection is automatically established after attach to the network and it will automatically reestablish when dropped unexpectedly.
    - Automatic Context Activation (ACA): the connection is automatically established when eligible devices are detected. This refers to a connected device that matches the local IP address criteria to activate the automatic context.
- **Connection Profile - Dedicated Connection 1 and Dedicated Connection 2**
  - This section allows the manual activation of a Dedicated Connection. The user can enable a Dedicated Connection by checking the Enable box.

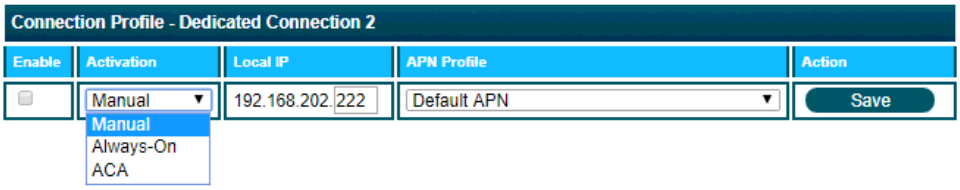

Figure 13: Dedicated Connection section

The user has to select the local IP Address for the connection and select the APN Profile and the Activation Method, selecting the options available from the drop-down menu. And then click the Save button.

When a Dedicated Connection is enabled and it is configured with a Manual Activation and an associated APN Profile; these settings will be used as default settings on the Manage Connections screen. This allows the user with an Administration password to lock down settings that can be used when activating dedicated connections.

Outbound filters

Outbound Filters are used to control access to the network. The filter rules provide the flexibility to either block or allow specific access. The rules can be based on address and port numbers of source or destination based on the protocol.

- **Outbound Filters –** This section allows the user to enable or disable this feature by checking the box and clicking on Apply Changes button.
- **Outbound Filter Rules –** In this section the user can configure the rule details and name the rule in the **Rules** section. You can configure up to five rules. The following rule parameters are configurable:

- Rule Name
- Rule Precedence
- Rule Action
  - Block
  - Allow
- Rule Enabled

At least one of the following optional parameters must be provided:

- Source Address
- Destination Address
- Destination Port Low
- Destination Port High
- Rule Protocol
  - TCP
  - UDP
  - TCP & UDP

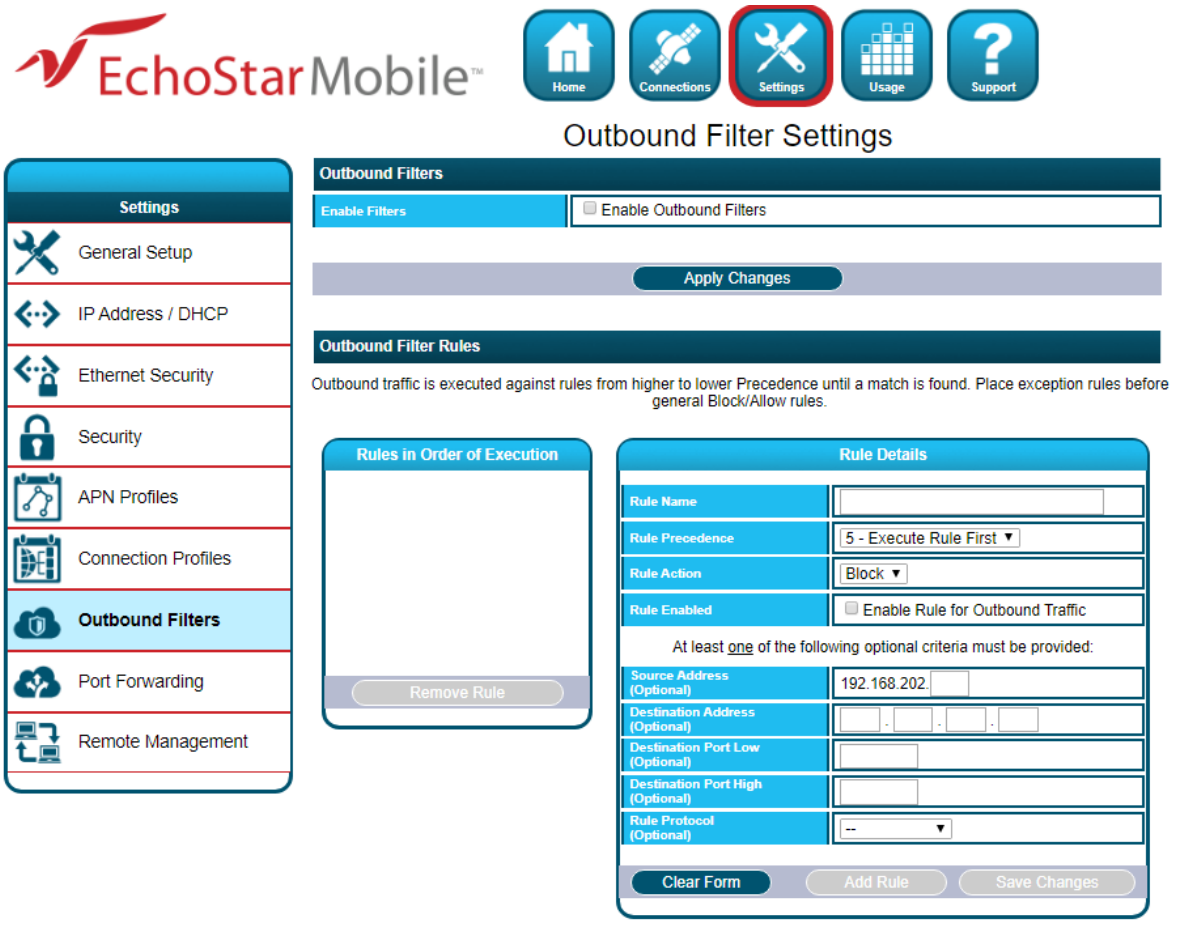

Figure 14: Outbound Filters screen

Port forwarding

The Port Forwarding page allows the user to enable and setup a DMZ IP address and specific Port Forwarding rules. If both DMZ and Port Forwarding rules are enabled, then the Port Forwarding rules take precedence and all other traffic is forwarded to the DMZ IP address.

- DMZ Settings – This section allows the user to enable and configure the DMZ IP address. When enabled, all incoming traffic is forwarded to that address.
- Port Forwarding – This section allows the user to configure the Rule details for five separate rules.

  The Port Forwarding parameters to be configured are:

  — Rule name
  — Local Address
  — Incoming Port
  — Incoming Protocol
    - TCP
    - UDP
    - TCP & UDP
  — Rule Enabled

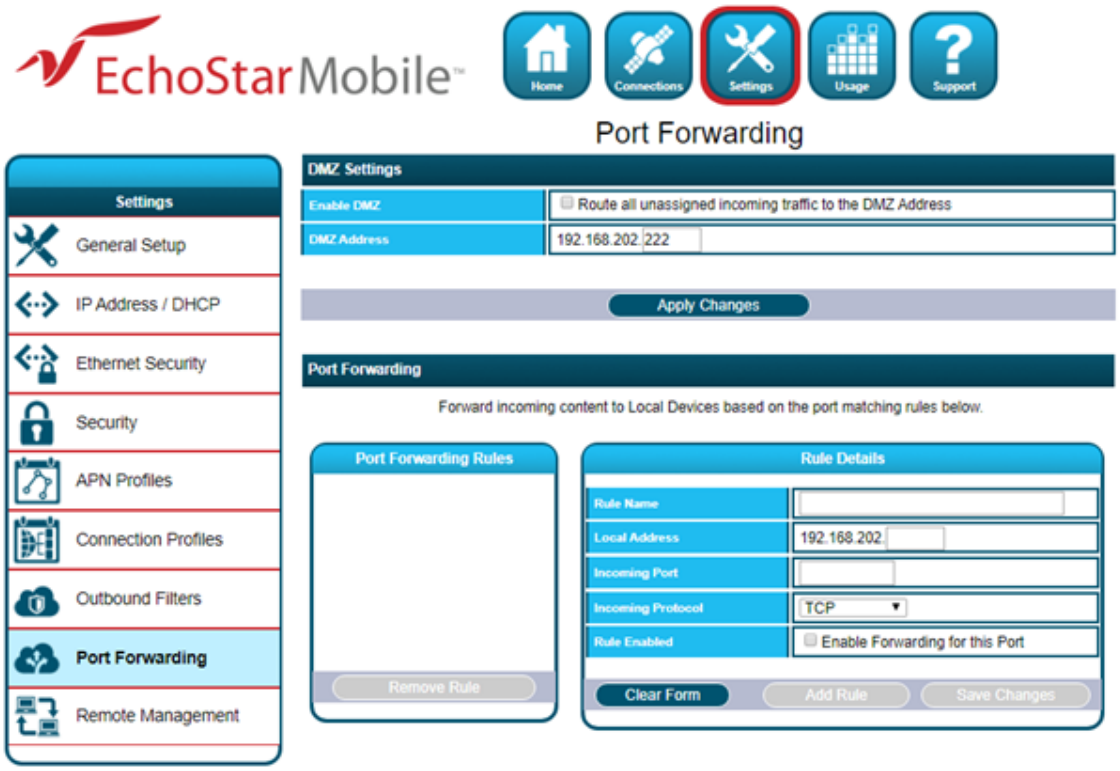

Figure 15: Port Forwarding screen

- **Port Triggering** – This allows for outgoing traffic to automatically configure port forwarding to the originating device. The port forwarding rule is active for 120 seconds after the trigger event occurred.

  The Port Triggering parameters to be configured are:

  — Rule name
  — Trigger Port
  — Trigger Protocol
    - TCP
    - UDP
    - TCP & UDP
  — Incoming Ports to Open
  — Incoming Protocol
  — Rule Enabled

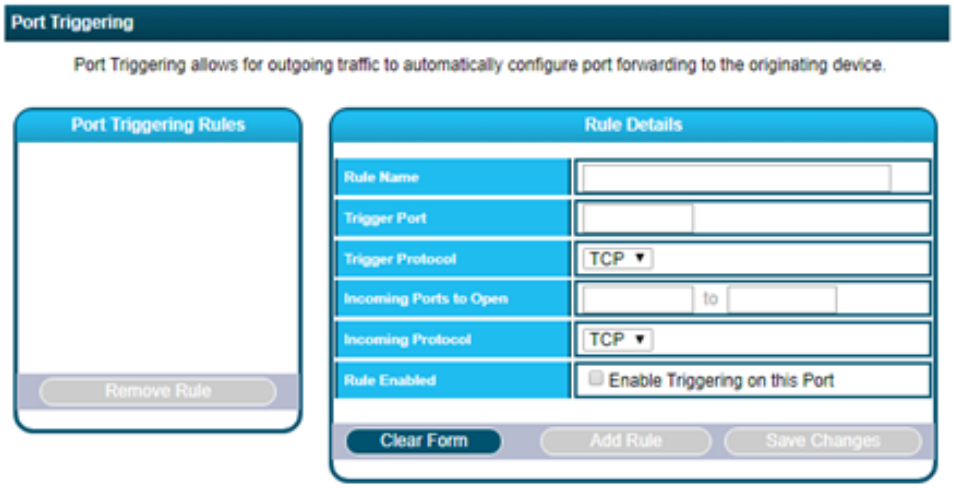

Figure 16: Port Triggering section

When the TE custom application opens “Trigger Port” X, then

— NAT sets up a translation rule for port X
— NAT adds translation rules for network-initiated connections to “Incoming Ports” X1, X2, and X3 for a period of 120 seconds

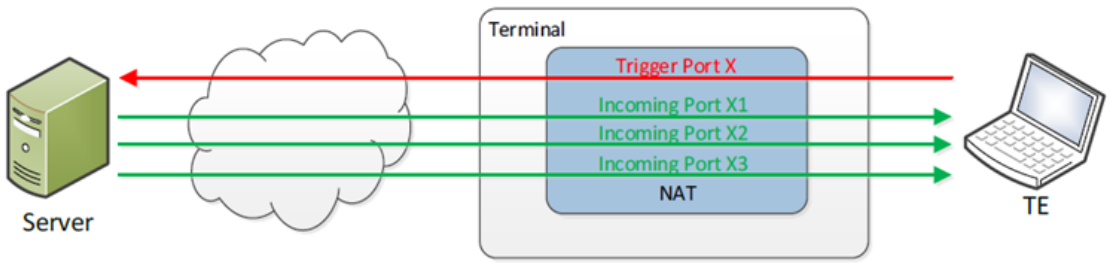

Figure 17: Port Forwarding concept

Remote management

This page allows the user to manage the Remote Management feature applying the changes in the sections here below:

- **Remote Management –** This function allows the terminal to be managed remotely over the satellite connection.
  - **Add Management Address –** This section allows the user to configure a list of IP Addresses that can send remote commands. The user needs to edit the IP Address and then click the Add Address button. The IP address will appear in the Management Address table on the left.
  - **Management Addresses –** This table shows the list of IP addresses allowed to send remote commands. The user can remove an IP address from the list selecting it from the list and then clicking the Remove Address button.

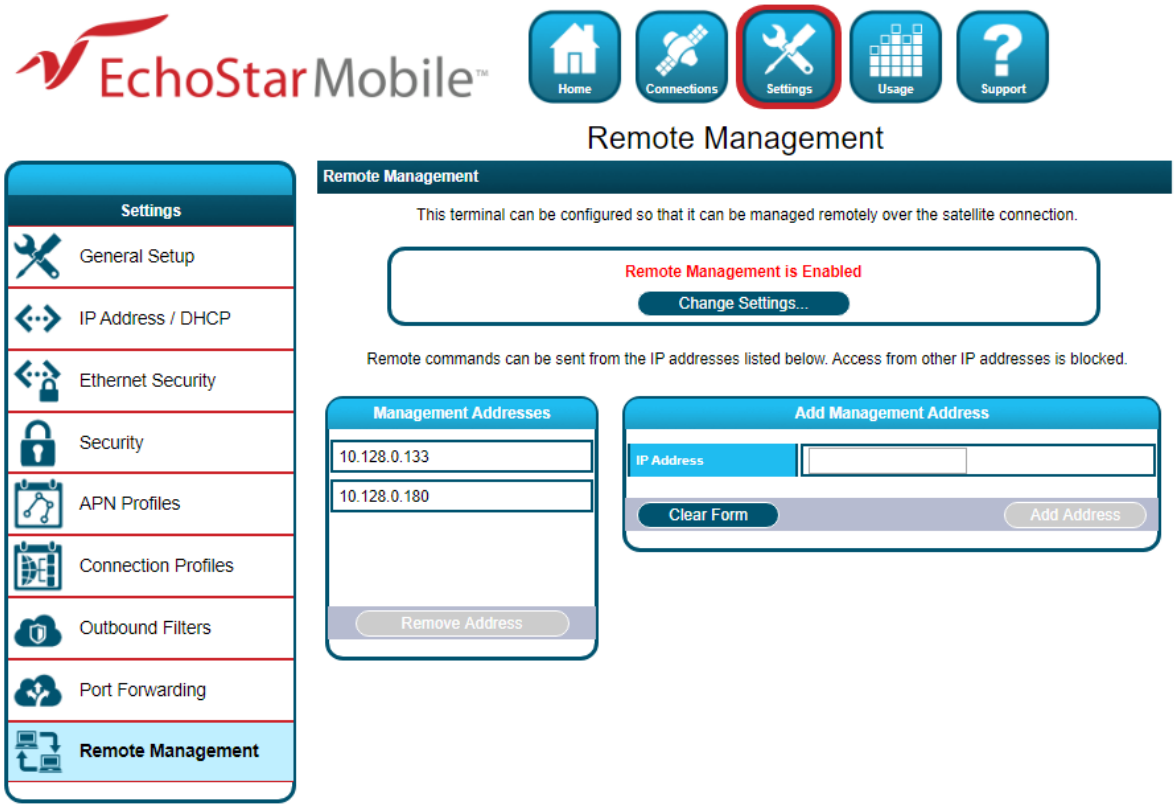

Figure 18: Remote Management screen

Click the Change Settings button to modify the **Remote Management Settings.** The user will need to enter the Current Remote Password in order to change any parameters, as shown in the image below.

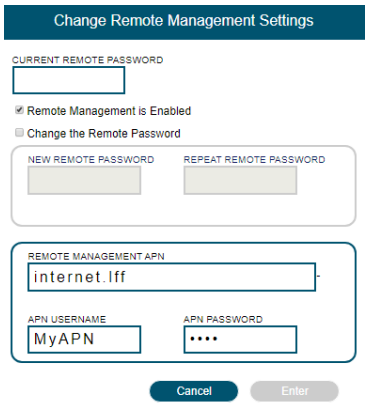

Figure 19: Change Remote Management Settings screen

Usage statistics

This page shows the statistics of data transmitted and received on connections in megabytes. And also shows the streaming data in both time and megabytes.

NOTICE

The **Trip statistics** can be reset, but the **Lifetime statistics** cannot be reset. They are like the odometer of a car.

The usage statistics are only an estimate and do not reflect actual billing system details.

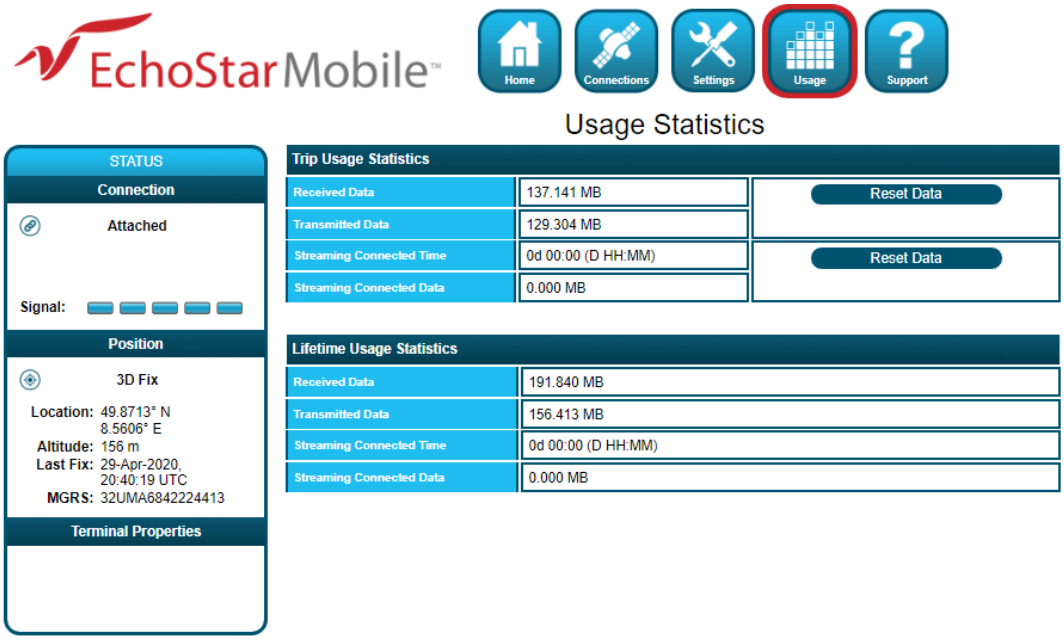

Figure 20: Usage Statistics screen

Support page

This Web page allows the user to obtain technical and support information about the terminal. It also facilitates to:

- **Reboot Terminal**
- **Reset Terminal to Factory Defaults**
- **Enable Full Band Search Mode**
- **Update Terminal Software –** This feature provides a convenient method to upgrade the Terminal Software. Before starting the process please make sure to obtain the latest Terminal Software Package, which is a file with the name “eml_4500_5.x.x.x.hif”, where the X’s correspond to the Software release number. The EML Terminal Software Package contains all necessary images for the Hughes 4500 product. The terminal automatically detects the Software images which apply to the product after loading the Software Package into the terminal.

NOTICE

It is not recommended to downgrade the terminal software to an older release. Doing so will automatically reset all configuration settings to factory default and delete all user data stored on the terminal.

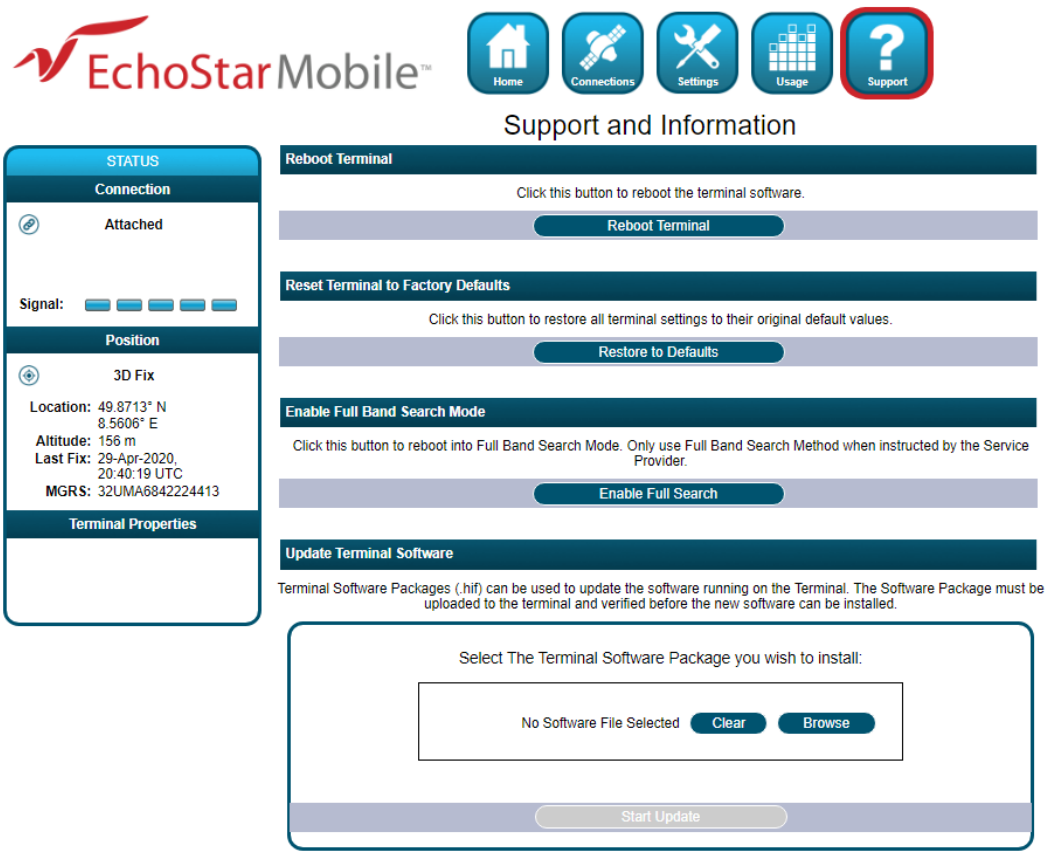

Figure 21: Support page

To upgrade the Terminal Software, follow these steps:

1. Store the Terminal Software Package on the local drive of a computer attached to the terminal.
2. Select the “Browse” button.
3. Navigate to the storage location of the Software Package, select the file and click “Open.”
4. Click the “Start Update” button:

Note: The file selection can be cleared by clicking the “Clear” button.

The terminal will copy the Software Package from the computer to the terminal and prepare the terminal for the SW upgrade.

After the Software Package is uploaded and verified the Web UI will present the components which are ready to be installed.

Click the Install button to start the installation process. This will deactivate all active connections and calls and place the terminal into service mode. After the software installation is complete the terminal will automatically reboot.

Progress of the installation process is indicated to the user with a series of updates on the Web UI.

After the reboot the software version can be verified on the **Support page**.

- **Terminal information –** This section provides detailed information about the terminal hardware and the installed software. Provide this information when requested by support technicians.
- **SIM information –** This section provides detailed information about the SIM card installed in the terminal. Provide this information when requested by support technicians.

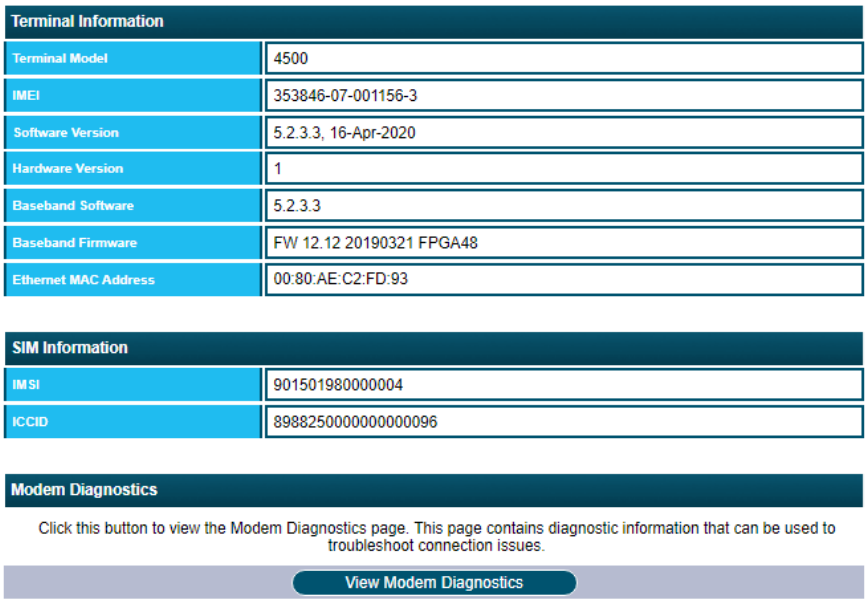

Figure 22: Information screen

- **Modem Diagnostics –** This section provides access to information that may be useful to aid in troubleshooting. Follow instructions of technical support personnel to obtain diagnostics information if needed.

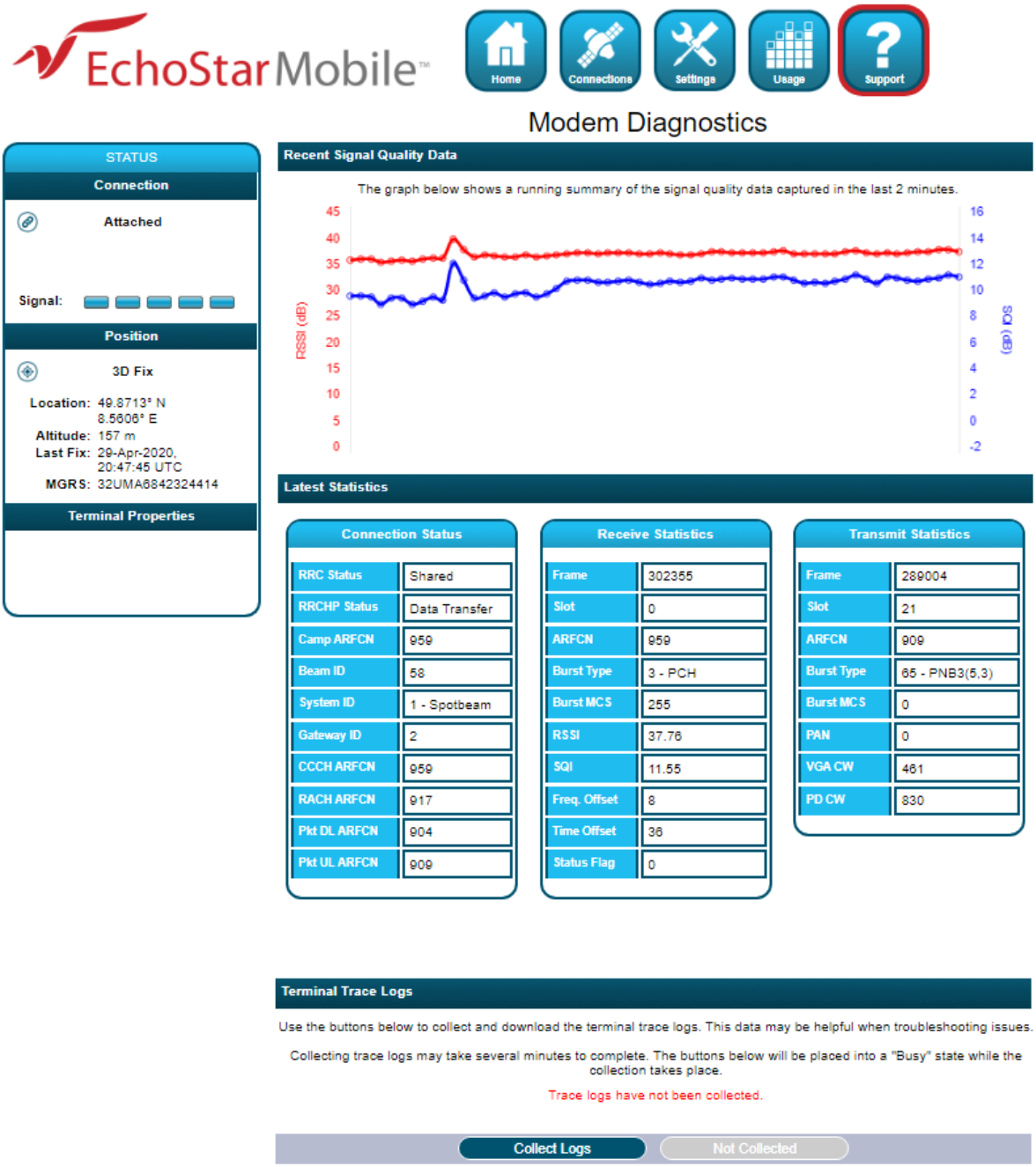

Figure 23: Modem Diagnostic screen

Chapter 4

Troubleshooting

Table 2: Troubleshooting

Problem	Possible cause	Possible solution
Terminal will not turn on	Remote switch is off	Connect and turn on the remote switch signal
Cannot get USIM card to lock into position	USIM is not correctly oriented for insertion	Ensure the USIM is oriented as shown in the "Before Getting Started" Section. Ensure the USIM is pressed firmly into the SIM slot.
The Web UI will not connect to the terminal	No interface connection between the terminal and computer Your computer is configured with a static IP address in the wrong subnet.	Ensure there is an Ethernet connection between the terminal and computer. Check the IP configuration settings on your computer. Enable DHCP or use a static IP address in the same subnet as the terminal's local IP address. The default terminal IP address is: 192.168.128.100.
The Web UI will not connect to the terminal	No interface connection between the terminal and computer Your computer is configured with a static IP address in the wrong subnet.	Ensure there is a USB connection (or Maintenance connection) between the terminal and computer. Check the IP configuration settings on your computer. Enable DHCP or use a static IP address in the same subnet as the terminal's local IP address. The default terminal IP address is: 169.254.1.1.
Terminal is connected to the network but cannot obtain the requested Quality of Service	Network temporarily not available.	Retry again. If problem persists, contact your service provider.
Terminal does not obtain a GPS fix	Terminal's location limits visibility of 3 or more GPS satellites.	Move the terminal to a location where there are few obstructions such as trees or tall buildings, so that as much as possible of the sky is visible. Point the antenna towards the most open area of sky (normally straight up).
None of the above solutions resolve the problem	Terminal may have a hardware or software fault and needs to be re-booted.	Remove power. Wait 30 seconds. Reconnect the DC power and turn on the terminal.

Chapter 5

Technical specifications

Table 3: Technical Specifications

Item	Specifications
Weight	1.4 kg
Dimensions	248 mm x 178 mm x 115 mm
Humidity	95% RH at 40 °C
Power, Max	16 W (when transmitting)
Water/Dust	IP-67
Operating Temperature	-25 °C to +65 °C
Storage Temperature	-40 °C to +80 °C
External Power Supply	10 V (Minimum Voltage Input) 28 V (Maximum Voltage Input)
Wind Loading	Survival: 200 km/h
Power Out EIRP	3.5 dBW
Other Features	Vehicular and fixed mounting kits

Table 4: Modem Diagnostics Technical Specifications

Acronym	Definition
Connection Status	
Beam ID	Spot beam identifier
Camp ARFCN	Camped beam's control channel number
CCCH ARFCN	Current control channel number
Gateway ID	Gateway identification
Pkt DL ARFCN	Downlink traffic channel number
Pkt UL ARFCN	Uplink traffic channel number
RACH ARFCN	Uplink control channel number
RRC Status	Status of Radio Resource Control
RRCHP Status	Status of RRC Idle Procedure
System ID	System identifier
Receive Statistics	
ARFCN	Absolute Radio Frequency Channel Number
Burst MCS	Burst Modulation and Coding Scheme
Burst Type	Physical Layer internal burst type
Frame	Physical Layer internal frame number
Freq. Offset	Received burst frequency offset
RSSI	Received burst RSSI
Slot	Physical Layer internal slot number
SQI	Received burst SQI

Acronym	Definition
Status Flag	Physical Layer status flag
Time Offset	Received burst time offset
Transmit Statistics	
ARFCN	Absolute Radio Frequency Channel Number
Burst MC S	Burst Modulation and Coding Scheme
Burst Type	Physical Layer internal burst type
Frame	Physical Layer internal frame number
PAN	Power Attenuation Notification
PD CW	Physical Layer internal Power Detector Code Word
Slot	Physical Layer internal slot number
VGA CW	Physical Layer internal VGA Code Word

Definitions and acronyms

Table 5: Definitions and Acronyms

Acronym	Definition
APN	Access Point Name
CAI	Common Air Interface
EML	EchoStar Mobile Limited
GPS	Global Positioning System
HW	Hardware
ICCID	Integrated Circuit Card ID
ID	Identifier
IGMP	Internet Group Management Protocol
IMEI	International Mobile Equipment Identity
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMSI	International Mobile Subscriber Identity
ISIM	IMS Subscriber Identity Module
OS	Operating System
PIN	Personal Identification Number
PUK	PIN Unlock Key (Password provided by the USIM card provider to unlock a lost/forgotten PIN code)
RJ	Registered Jack
RTM	Remote Terminal Manager
RX	Receive
SIM	Subscriber Identity Module
SIM PIN	USIM Personal Identification Number (located on the USIM card)
TCP	Transmission Control Protocol
TE	Terminal Equipment
TX	Transmit
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USIM	UMTS Subscriber Identity Module
UT	User Terminal
Web UI	Web based User Interface