



Hughes 4500 User Guide

H62751
Revision C
July 12, 2021

Copyright © 2021 Hughes Network Systems, LLC

All rights reserved. This publication and its contents are proprietary to Hughes Network Systems, LLC. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Network Systems, LLC, 11717 Exploration Lane, Germantown, Maryland 20876.

Hughes Network Systems, LLC has made every effort to ensure the correctness and completeness of the material in this document. Hughes Network Systems, LLC shall not be liable for errors contained herein. The information in this document is subject to change without notice. Hughes Network Systems, LLC 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

HUGHES, HughesNet, HughesON, IPoS, SPACEWAY, and JUPITER are trademarks of Hughes Network Systems, LLC. All other trademarks are the property of their respective owners.

Contents

Understanding safety alert messages	5
Messages concerning personal injury	5
Messages concerning property damage	5
Safety symbols.....	5
Additional symbols.....	5
Warnings for satellite terminal.....	6
Equipment users.....	7
 Chapter 1	
Introduction	9
1.1 Overview.....	9
1.2 About this user guide.....	9
1.3 Package contents.....	9
1.4 Minimum system requirements for laptop/PC	10
1.4.1 System requirements to support maintenance port	10
1.4.2 Additional hardware	10
 Chapter 2	
Using the Hughes 4500	12
2.1 Before getting started	12
2.2 Quick start.....	12
2.3 Connecting the terminal to the computer	12
2.3.1 Connecting by Ethernet.....	12
2.3.2 Connecting by USB	12
 Chapter 3	
Using the Web UI	13
3.1 Accessing the Web UI	13
3.2 Home page.....	13
3.3 Connections.....	14
3.3.1 Manage connections.....	14
3.3.2 APN Profiles.....	15
3.3.3 Connection Profiles	16
3.4 Settings page	18
3.4.1 General setup.....	18
3.4.2 IP address/DHCP settings.....	19
3.4.3 Ethernet security.....	20
3.4.4 Security.....	21
3.4.5 Outbound filters	23
3.4.6 Port forwarding	24
3.4.7 Remote management	26
3.5 Usage statistics	28
3.6 Support page	28
3.6.1 Information	28
3.6.2 Troubleshooting	29
3.6.3 Satellite Diagnostics	31
3.6.4 Update Software	32

3.6.5	Restore Factory Defaults Procedure	33
Chapter 4		
	Troubleshooting	35
Chapter 5		
	Technical specifications	37
	Acronyms.....	39

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 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 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:



Indicates a safety message that concerns a potential electric shock hazard.



Indicates a safety message that concerns potential for personal injury.



Indicates a safety message that concerns radio frequency (RF) energy.

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 half 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 half 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 cause said conditions.

1.1 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 allows the user to send and receive IP packets via Ethernet.



Figure 1: Hughes 4500 Terminal

1.2 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 focuses on the specific information required to operate the Hughes 4500 Terminal and 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. After you have completed these steps, you are ready to start using the data services.

1.3 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), its PIN, and satellite terminal configuration instructions. You will need these to access the satellite network.

1.4 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

1.4.1 System requirements to support maintenance port

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

- Microsoft Windows 7
- Microsoft Windows 10

1.4.2 Additional hardware

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

Table 1: Additional hardware items from the Hughes catalog

Item	Part Number	Specifications
Fixed Mounting Bracket	3501366-0001	High-quality, corrosion-resistant angle bracket for mounting the terminal to a vertical, flat surface. Pole mounting can be accomplished by adding U-clamps, which can be sourced separately.
Magnetic Mounting Kit	3501365-0001	Custom-designed kit for mounting the terminal to a horizontal, magnetic, flat surface. The kit contains all the parts needed to add magnetic mounting to the terminal.
Pole Mount Kit	POLE-MOUNT-KIT	Pole mount, U-bolts (2), and a fixed mount bracket for a convenient pole mount install.
Power and Data Cable, Blunt Wire (5 m)	3501314-0002	Ready-made cables for connecting the terminal to DC power and Ethernet data.
Power and Data Cable, Blunt Wire (10 m)	3501314-0003	Ready-made cables for connecting the terminal to DC power and Ethernet data.
Power and Data Cable, Cigarette Lighter Plug, and RJ45 Socket (5 m)	3501314-0004	The cigarette lighter plug and RJ45 version are ideal for temporary vehicular installs.
RJ45 Wiring Block	9510250-0002	The RJ45 wiring block is useful with blunt wire cables.

Item	Part Number	Specifications
Mating Power and Data Connector (bare)	9509554-0001	
Custom Power and Data Cable, 8.5 mm OD (100 m)	9509897-0001	The bulk cable and solder-ready barrel connector allow for custom cable installations.

Chapter 2

Using the Hughes 4500

2.1 Before getting started

NOTICE

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



Figure 2: Inserting the USIM card

2.2 Quick start

The Hughes 4500 Terminal must first obtain a GPS fix. In order to do this, the terminal must be positioned 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 seconds.

2.3 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

2.3.1 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.

2.3.2 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

3.1 Accessing the Web UI

The Hughes 4500 includes an internal Web User Interface (Web UI). To access the Web UI, open your preferred web browser and enter the internal IP address of the terminal.

- If you are using an Ethernet port, enter this Ethernet IP address:
 - <http://192.168.128.100>
- If you are using a USB port, enter 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**.

3.2 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 the receive signal strength and if you are registered with the IMS.
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 (MGRS). The time is displayed in UTC.
3. **Terminal Properties:** This field indicates miscellaneous status information.

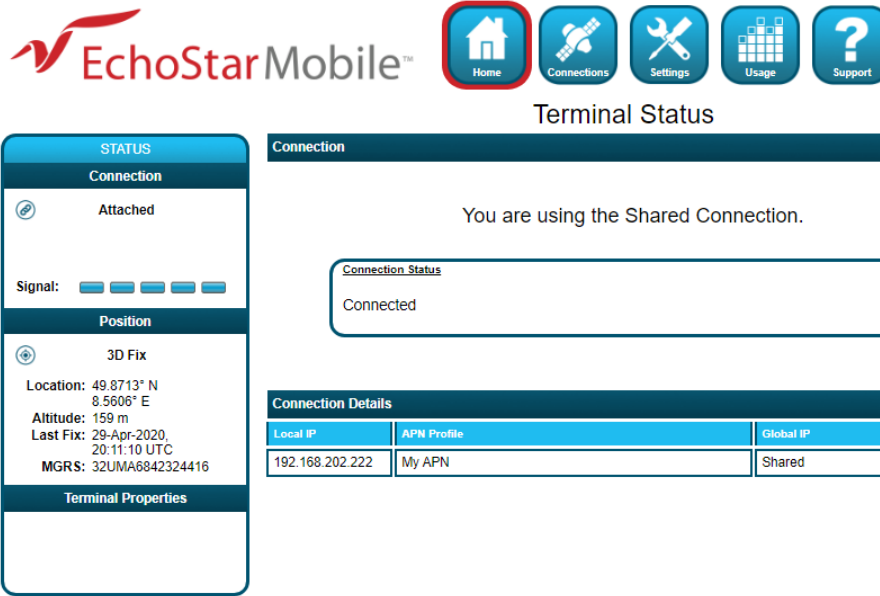


Figure 3: Terminal Status page

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 Terminal Equipment's (TE) local IP address.

For basic connectivity, the terminal would function with one signal bar. For more details, the user can reference the **Diagnostics** page to see if the Signal Quality Index (SQI) is at least 5 dB. It is desirable to have 10 dB or better.

3.3 Connections

The **Connections** page allows the user to manage the data connections. The following are the available subpages:

- **Manage Connections**
- **APN Profiles**
- **Connection Profiles**

3.3.1 Manage connections

This page allows the user to manage the satellite connections:

- **Shared Connection:** This section displays the connection status, global IP, and an action button to disconnect or connect. The shared connection is automatically established when the terminal powers up.
- **Local Devices Using the Satellite Shared Connection:** This section displays the local IP addresses of all devices connected to the satellite shared connection (port translation NAT).
- **Dedicated Connection 1 and Dedicated Connection 2:** This section displays the status of the custom dedicated connections, the local IP, the APN profile, the global IP, and an action button to disconnect or connect. The dedicated connection is specific to the TE, which is configured to use the connection. This makes the TE directly addressable from the Global Networking Space

(basic NAT). After a TE establishes a dedicated data connection, it no longer uses the shared connection.

To establish a connection with the network, select one of the profiles from the **APN Profile** dropdown menu and click the **Connect** button. Once connected, the global IP field will be populated, and the **Connect** button will change to **Disconnect**.

EchoStar Mobile™

Home Connections Settings Usage Support

Manage Connections

STATUS

Network

Attached

Signal:

Connections

Manage Connections

APN Profiles

Connection Profiles

Shared Connection

Connection Status	Global IP	Action
Connected	100.64.96.244	Disconnect

Local Devices Using the Satellite Shared Connection

Local IP
192.168.202.111
192.168.202.222

Dedicated Connection 1

Local IP	APN Profile	Global IP	Action
192.168.202.222	User Profile Neco2297	--	Connect

Dedicated Connection 2

Local IP	APN Profile	Global IP	Action
192.168.202.223	User Profile Neco2370	--	Connect

Figure 4: Connection page

3.3.2 APN Profiles

- **Profile Settings:** This section allows the user to choose the default satellite APN profile by selecting the APN profile from the dropdown menu and clicking the **Apply Changes** button. At least one profile needs to be configured and selected as the default profile.
- **Defined APN Profiles:** This section allows the user to configure up to five APN profiles for use with satellite or cellular connections. Enter values for the following fields to define a new APN profile:
 - Profile Label
 - Profile APN
 - APN Username
 - APN Password

Note: The APN Username and APN Password fields are mandatory.

After clicking **Apply Changes**, an APN profile will be created and will appear on the APN profile table. The profile can be configured to prompt for a password when selected.

APN Profiles

STATUS

Network

Attached

Signal:

Connections

Manage Connections

APN Profiles

Connection Profiles

Profile Settings

Default APN Profile

User Profile Neco0200D

The Default APN Profile cannot prompt for a password because it will be used (by default) for automatic connections.

Apply Changes

Defined APN Profiles

APN profiles can be configured to allow connections with a specific Access Point Name (APN) and username. The APN password can be supplied or the profile can be configured to prompt for the password when selecting it for use.

APN Profiles

User Profile Neco0200D

User Profile Neco2297

User Profile Neco2370

Remove Profile

Profile Details

Profile Label

User Profile Neco2370

Profile APN

echonet.eml.com

APN Username

Neco2370

APN Password

Prompt for Password

☐ Prompt for password when selecting profile

Clear Form

Add Profile

Save Changes

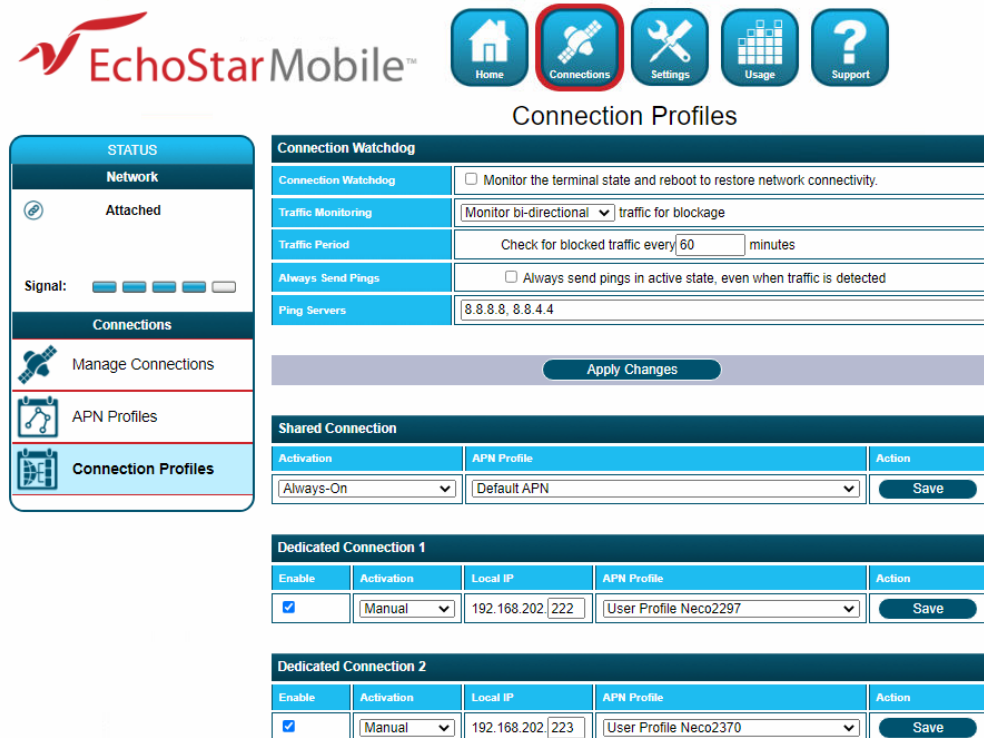
Figure 5: APN Profiles page

3.3.3 Connection Profiles

This page allows the user to configure the user data connections (shared and dedicated) by selecting an APN profile and an activation method.

- Connection Watchdog:** This section allows the user to enable the Connection Watchdog feature in order to monitor the traffic. The user can also configure the following options:
 - Traffic Monitoring:**
 - Do not monitor
 - Monitor only incoming
 - Monitor only outgoing
 - Monitor bi-directional
 - Traffic Period:** This is the period of the traffic monitoring feature. This value should be set based on the expected data usage of the terminal. The default duration is 10 minutes.
 - Always Send Pings:** This feature allows the UT to send pings, even when the traffic flow is detected.
 - Ping Servers:** This displays the IP addresses of servers to be used when verifying link connectivity.

- **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 each of the dropdown menus and confirm them by clicking **Save**.
- **Connection Profile – Dedicated Connection 1 and Dedicated Connection 2:** This section allows for automatic activation of a dedicated satellite connection. The user can enable a dedicated connection by checking the Enable box. The user can also configure the activation as noted below:



EchoStar Mobile™

Home Connections Settings Usage Support

Connection Profiles

STATUS

Network

Attached

Signal: ■ ■ ■ ■ ■

Connections

Manage Connections

APN Profiles

Connection Profiles

Connection Watchdog

Connection Watchdog ☐ Monitor the terminal state and reboot to restore network connectivity.

Traffic Monitoring Monitor bi-directional traffic for blockage

Traffic Period Check for blocked traffic every 60 minutes

Always Send Pings ☐ Always send pings in active state, even when traffic is detected

Ping Servers 8.8.8.8, 8.8.4.4

Apply Changes

Shared Connection

Activation	APN Profile	Action
Always-On	Default APN	Save

Dedicated Connection 1

Enable	Activation	Local IP	APN Profile	Action
<input checked="" type="checkbox"/>	Manual	192.168.202.222	User Profile Neco2297	Save

Dedicated Connection 2

Enable	Activation	Local IP	APN Profile	Action
<input checked="" type="checkbox"/>	Manual	192.168.202.223	User Profile Neco2370	Save

Figure 6: Connection Profiles page

– **Activation Method:**

- **Manually:** The user manually connects and disconnects the connection on the Web UI.
- **Always-On:** The connection is automatically established after attaching to the network, and it will automatically re-establish 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.

The user must select the local IP address for the connection and select the APN profile and activation method using options available from the dropdown menus. Clicking the **Save** button confirms the changes.

Note: The dedicated connection profile must be enabled to take effect. When a dedicated connection is configured for manual activation, the connection profile settings will be used as hard-coded defaults on the **Manage Connections** screen. This allows a user with the administration password to lock the settings that can be used when activating dedicated connections.

3.4 Settings page

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

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

3.4.1 General setup

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

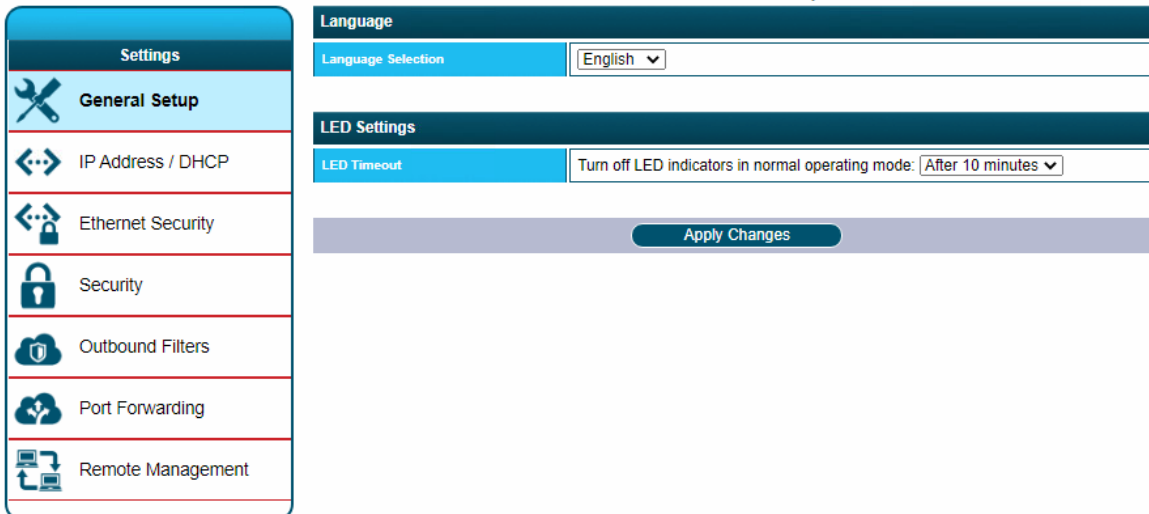
- **Language:** The user can choose between the different language options by selecting a language from the dropdown menu and clicking the **Apply Changes** button.
- **LED Settings:** The user can select between three different display options for the LED indicators in normal operating mode. After selecting a new display option from the dropdown menu, the user can confirm the setting by clicking **Apply Changes**.

The LED states in normal operating mode **are explained** in **Table 2**:

Table 2: LED states in normal operating mode

State	LED
Powering up	Solid GREEN
Network acquisition	Flashing GREEN
Registered and IP context active	Solid GREEN
Hardware fault	Solid RED

General Setup



Settings

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

Language

Language Selection: English ▼

LED Settings

LED Timeout: Turn off LED indicators in normal operating mode: After 10 minutes ▼

Apply Changes

Figure 7: Settings page

3.4.2 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 three octets of the DHCP address range will also change automatically.
- **DHCP Server:** This 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. Changing the DHCP address range requires an immediate reboot. The following IP addresses are reserved by the UT:
 - IP address of the terminal (e.g., 192.168.128.100)
 - IP address just below (e.g., 192.168.128.099)

Note: When updating the DHCP address range, the following settings will be updated or reset and may need to be revisited:

- DHCP Address Range
- DHCP Reservations
- Port Forwarding
- Port Triggering
- Outbound Filters
- **DHCP Reservations:** This section allows the user to add an IP address that will permanently be assigned to a particular connected device based on the detected device's MAC address.

EchoStar Mobile™

Home Connections **Settings** Usage Support

IP Address / DHCP Settings

Settings
General Setup
IP Address / DHCP
Ethernet Security
Security
Outbound Filters
Port Forwarding
Remote Management

Terminal Local IP Address

Terminal Local IP Address: 192 . 168 . 202 . 100

DHCP Server

DHCP Server: ☐ Enable DHCP Server

DHCP Address Range: 192.168.202.101 to 199

Apply Changes

DHCP Reservations

Reserved IP Addresses

IP Address	MAC Address
192.168.202.111	00:15:5d:67:bf:09

DHCP IP Address:
MAC Address:

Add A Detected Device

IP Address	MAC Address
192.168.202.111	00:15:5d:67:bf:09
192.168.202.222	00:15:5d:67:bf:0e

Figure 8: IP address/DHCP screen

3.4.3 Ethernet security

This 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 and then add it to the Allowed MAC Address field.

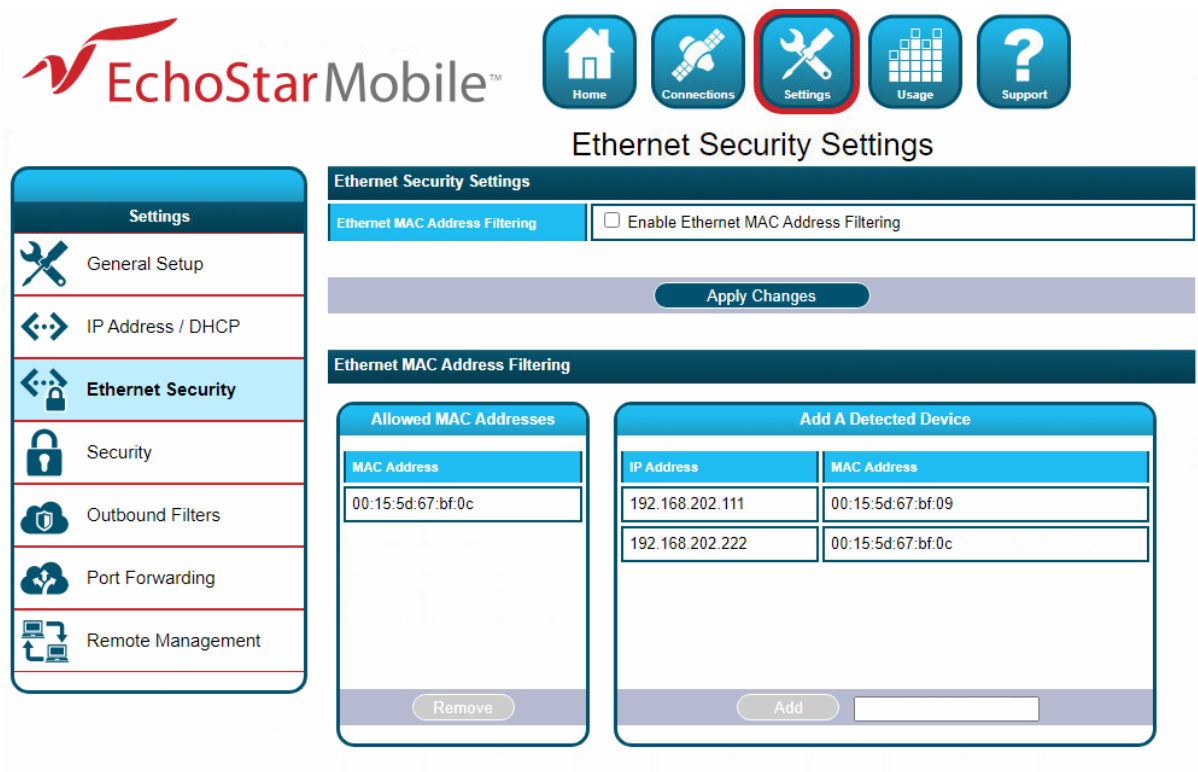


Figure 9: Ethernet Security screen

3.4.4 Security

This page allows the user to set up 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 three incorrect attempts to enter the PIN, the user will have to use the PUK number to reset the PIN of the SIM card.
- SIM Lock PIN:** This is a field that allows up to eight digits to lock the terminal to the current SIM card. The SIM Lock PIN code must be entered whenever a different SIM card is used with the terminal.
- Local Access Password:** Once enabled, this password prevents all local access to the terminal settings from unauthorized users. This includes all access to the Web UI and AT command interface, SFTP, and interfaces used for debugging purposes. Once enabled, the terminal can be unlocked by entering the local access password on a special lock screen. This will unlock local access to the terminal for period of 15 minutes, after which the terminal will be automatically locked again. The terminal can also be manually locked before the timeout period elapses by clicking the **Lock Terminal** button that appears on this page when the *Local Access Password* feature is enabled. This feature is designed to prevent physical tampering/reconfiguration of the terminal when it is installed for remote operation. Locking the terminal does not affect user data traffic.

Note: If the local access password is lost, the terminal can only be recovered through remote access or by resetting to factory default settings using the button next to the USB connector.

- **Administration Password:** This password prevents terminal settings from being changed by unauthorized users once the terminal is configured properly. Once enabled, this password must be entered before protected settings can be changed. A popup requesting the password will appear if the administration password is enabled and the user attempts to change a protected configuration parameter.

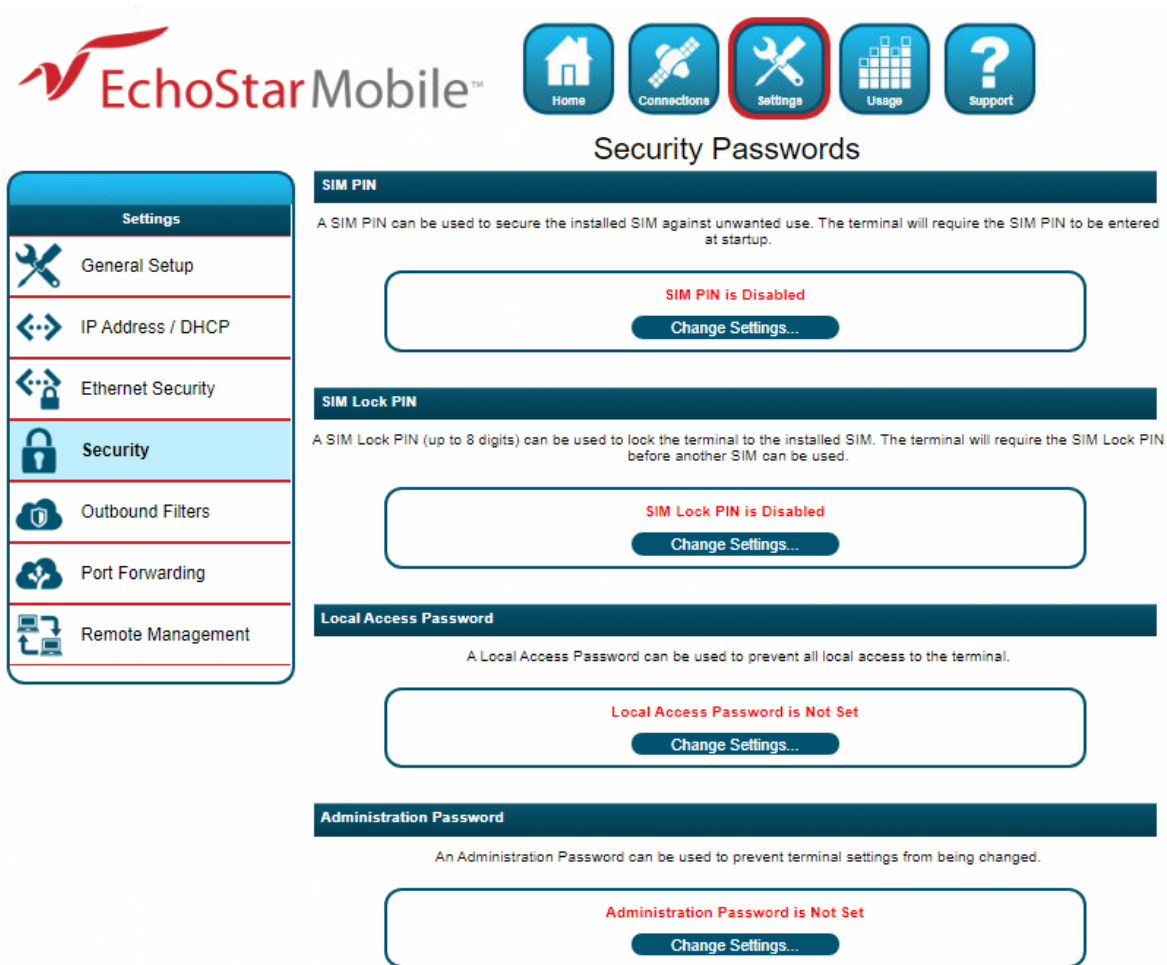


Figure 10: Security screen

Figure 11: Security Settings screen

3.4.5 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 **Apply Changes**.
- **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


Outbound Filter Settings


Settings


 General Setup


 IP Address / DHCP

 Ethernet Security

 Security

 Outbound Filters

 Port Forwarding

 Remote Management

Outbound Filters

Enable Filters

☐ Enable Outbound Filters

Apply Changes

Outbound Filter Rules

Outbound traffic is executed against rules from higher to lower Precedence until a match is found. Place exception rules before general Block/Allow rules.

Rules in Order of Execution

5) Google blocked

4) Googleallowed

Remove Rule

Rule Details

Rule Name	
Rule Precedence	5 - Execute Rule First
Rule Action	Block
Rule Enabled	<input type="checkbox"/> Enable Rule for Outbound Traffic
At least <u>one</u> of the following optional criteria must be provided:	
Source Address (Optional)	192.168.202. /
Destination Address (Optional)	. . . /
Destination Port Low (Optional)	
Destination Port High (Optional)	
Rule Protocol (Optional)	--

Outbound Filter Rules will not be applied unless the Outbound Filters feature has been enabled.

Clear Form

Add Rule

Save Changes

Figure 12: Outbound Filters screen

3.4.6 Port forwarding

The **Port Forwarding** page allows the user to enable and set up 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

EchoStar Mobile™

Home Connections **Settings** Usage Support

Port Forwarding

Settings

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

DMZ Settings

Enable DMZ	<input checked="" type="checkbox"/> Route all unassigned incoming traffic to the DMZ Address
DMZ Address	192.168.202.111

Apply Changes

Port Forwarding

Forward incoming content to Local Devices based on the port matching rules below.

Port Forwarding Rules

Remove Rule

Rule Details

Rule Name	
Local Address	192.168.202.
Incoming Port	
Incoming Protocol	TCP
Rule Enabled	<input type="checkbox"/> Enable Forwarding for this Port

Clear Form Save Changes Add Rule

Figure 13: Port Forwarding screen

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

Port Triggering

Port Triggering allows for outgoing traffic to automatically configure port forwarding to the originating device.

Port Triggering Rules

Remove Rule

Rule Details

Rule Name	<input type="text"/>
Trigger Port	<input type="text"/>
Trigger Protocol	TCP
Incoming Ports to Open	<input type="text"/> to <input type="text"/>
Incoming Protocol	TCP
Rule Enabled	<input type="checkbox"/> Enable Triggering on this Port

Clear Form

Save Changes

Add Rule

Figure 14: 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.

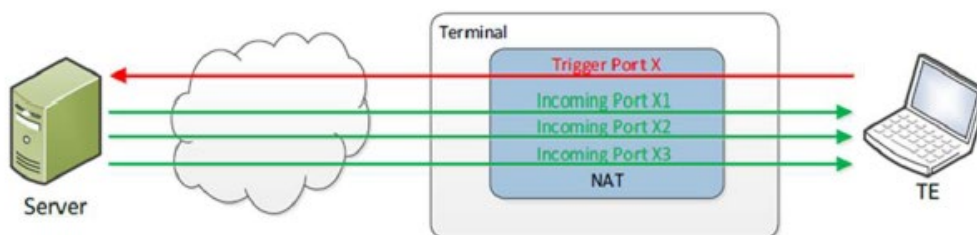


Figure 15: Port Forwarding concept

3.4.7 Remote management

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

- **Remote Management:** This function allows the terminal to be managed remotely over the satellite connection. Click the **Change Settings** button to enable this function. There are no default remote management settings. When configuring the terminal for the first time, the user will need to enter a remote password.
Note: After the initial configuration, updates to these settings will require the user to enter the remote password.
- **Remote Management Access Setup:** This section allows the user to modify the access port HTTPS access to the terminal by filling in the Access Port files. Click the Apply Change button to save the setup.
- **Management Addresses:** This section shows the list of IP addresses allowed to send remote commands. The user can remove an IP address from the list by selecting it and clicking the **Remove Address** button.

Remote Management

Settings

General Setup

IP Address / DHCP

Ethernet Security

Security

Outbound Filters

Port Forwarding

Remote Management

Remote Management

This terminal can be configured so that it can be managed remotely over the satellite connection.

Remote Management is Enabled

Change Settings...

An Access Point Name must be provided for the satellite WAN remote management connection. An APN username and password are required for operation.

Remote Management Access Setup

Access Port	Use port 8443 for HTTPS access to the terminal.
APN	echonet.eml.com
APN Username	remote_4500
APN Password	*****

Apply Changes

Management Addresses

Remote commands can be sent from the IP addresses listed below. Access from other IP addresses is blocked.

Management Addresses

80.101.236.104

217.100.252.50

80.69.85.131

100.64.96.189

Remove Address

Add Management Address

IP Address

Clear Form

Add Address

Figure 16: Remote Management screen

Change Remote Management Settings

CURRENT REMOTE PASSWORD

Remote Management is Enabled

Change the Remote Password

NEW REMOTE PASSWORD

REPEAT REMOTE PASSWORD

REMOTE MANAGEMENT APN

internet.lff

APN USERNAME

MyAPN

APN PASSWORD

....

Cancel

Enter

Figure 17: Change Remote Management Settings screen

3.5 Usage statistics

This page shows the statistics of data transmitted in 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.

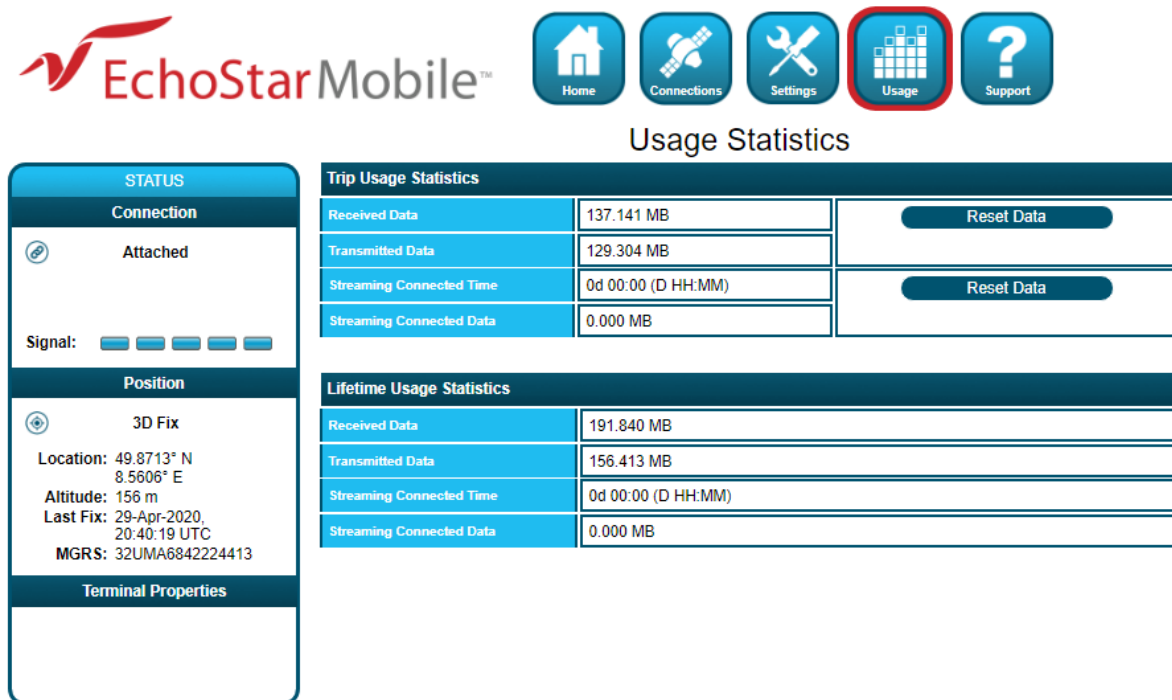


Figure 18: Usage Statistics screen

3.6 Support page

This page allows the user to obtain technical and support information about the terminal. The following is a list of the available subpages:

- **Information**
- **Troubleshooting**
- **Satellite Diagnostics**
- **Update Software**

3.6.1 Information

This subpage allows the user to view the following information:

- **Terminal Information:** This section provides detailed information about the terminal hardware and software.

- **Modem Information:** This section provides detailed information about the satellite modem and the SIM card. The Satellite IMEI acts as the serial number of the terminal.

Note: Please provide the terminal information when requested by support technicians.

EchoStar Mobile™

Home Connections Settings Usage Support

Terminal Information

Terminal Information	
Terminal Model	4500
Software Version	0.0.0.7, 01-June-2021
Ethernet MAC Address	00:80:AE:C2:FD:93

Modem Information	
IMEI	353846-07-001156-3
Modem Software	0.0.0.8
Modem Firmware	FW 12.12 20190321 FPGA48
Modem Hardware	1
SIM IMSI	9015019800000004
SIM ICCID	8988250000000000096

Figure 19: Terminal Information page

3.6.2 Troubleshooting

This subpage allows the user to:

- **Terminal Diagnostic Logs:** This section allows the user to collect diagnostics logs. The terminal continuously stores logging information during normal operation. In case of an unexpected behavior or malfunction, this information can be useful for troubleshooting the problem.

There are two steps necessary to obtain the logging information:

- Collect the logs by clicking the **Collect Logs** button. This process will package all logging information in an archive. This may take a few minutes.
- Download the log archive from the terminal to the connected PC by clicking the **Not Collected** button.

- **Reboot Terminal**
- **Reset Terminal to Factory Defaults**
- **Enable Full Band Search**

Troubleshooting

STATUS

Network

Attached

Signal:

Support

Information

Troubleshooting

Satellite Diagnostics

Update Software

Terminal Diagnostic Logs

If the terminal is out of order, you can collect diagnostic logs that will help to diagnose and correct the issue. Please include diagnostic logs with your service request, if possible.

Collecting diagnostic logs may take several minutes to complete.
The buttons below will be placed into a disabled state while the collection takes place.

Diagnostic logs have not been collected.

Collect Logs

Not Collected

Reboot Terminal

Click this button to reboot the terminal software.

Reboot Terminal

Reset Terminal to Factory Defaults

Click this button to restore all terminal settings to their original default values.

Restore to Defaults

Enable Full Band Search Mode

Click this button to reboot into Full Band Search Mode.
Only use Full Band Search Method when instructed by the Service Provider.

Enable Full Search

Figure 20: Troubleshooting page

3.6.3 Satellite Diagnostics

This subpage provides access to information related to the satellite connection that may be useful to aid in troubleshooting. Follow the instructions from the technical support personnel to obtain diagnostics information (if required).

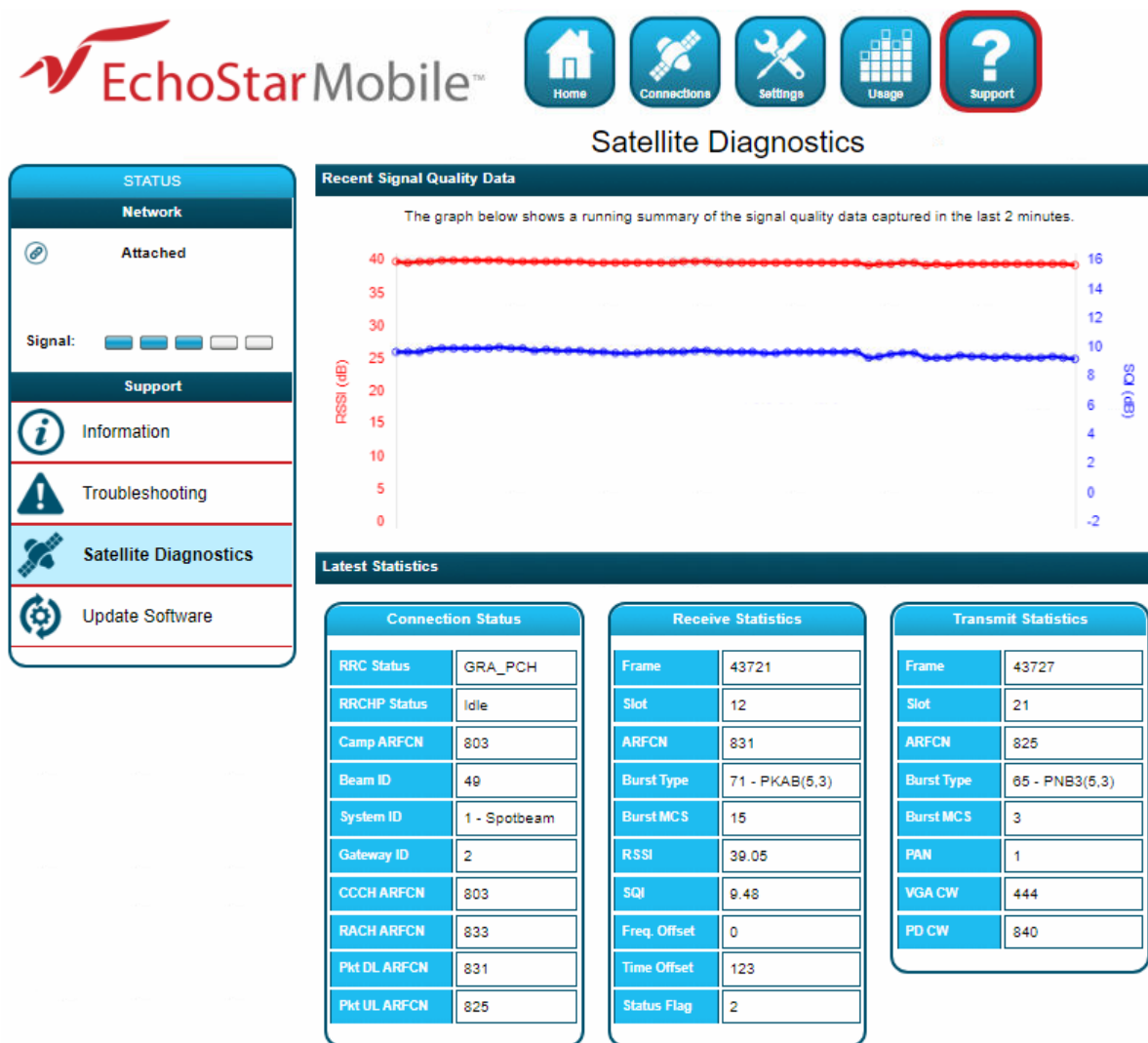


Figure 21: Troubleshooting page

Note: It is useful to provide a screenshot of this page in case there is a problem.

See the latest statistics definitions in **Table 3**:

Table 3: Modem diagnostics technical specifications

Acronym/Term	Definition
Connection Status	
Beam ID	Spot beam identifier
Camp ARFCN	Camped beam's control channel number
CCCH ARFCN	Current control channel number

Acronym/Term	Definition
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 (RRC)
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
Status Flag	Physical layer status flag
Time Offset	Received burst time offset
Transmit 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
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

3.6.4 Update Software

This subpage provides a convenient method to upgrade the terminal software. Before beginning the process, please make sure to obtain the latest terminal software package. This package can be found under the file name of em_4500_5.x.x.x.hif, where x.x.x corresponds to the software release number. The EM terminal software package contains all necessary images for the Hughes 4510 product. The terminal automatically detects the software images, which apply to the product after loading the software package into the terminal.

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

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. Click 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 software upgrade.

After the software package is uploaded and verified, the Web UI will present the components 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.

Installation progress is communicated to the user with a series of updates on the Web UI.

After the reboot, the software version can be verified on the **Information** subpage.

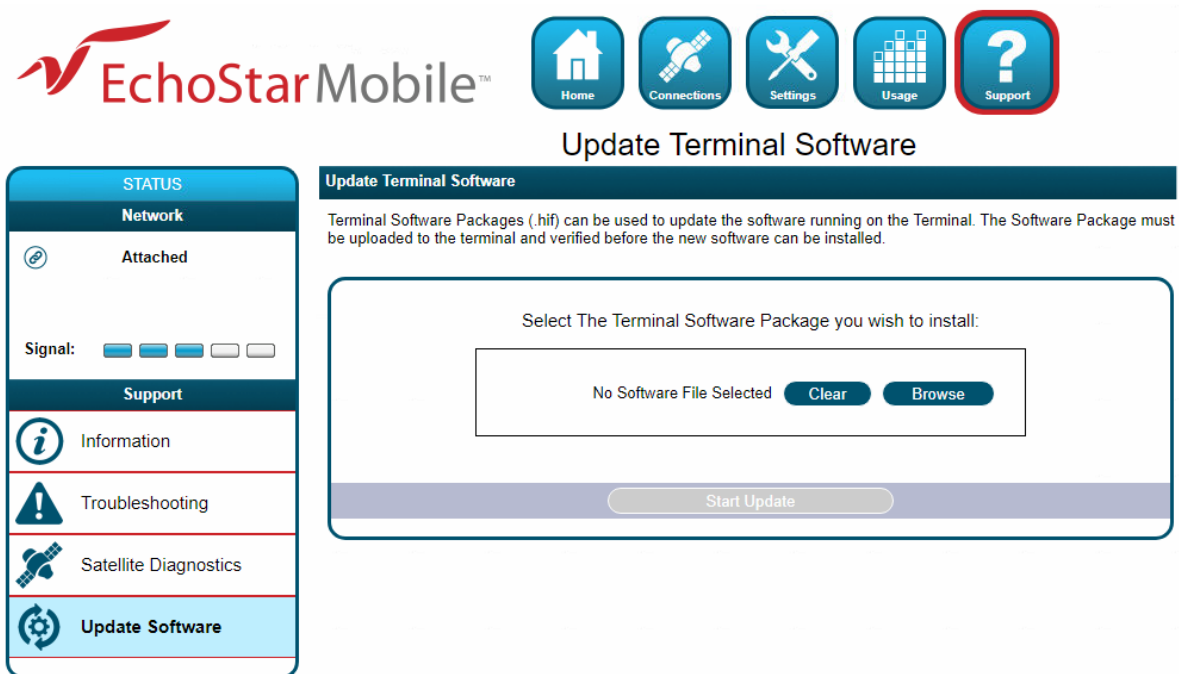


Figure 22: Update Terminal Software page

3.6.5 Restore Factory Defaults Procedure

In order to restore the terminal to factory defaults, please keep the button pressed during 10seconds. The LED sequence will be the following one: **RED** – **GREEN** – **RED** (flashing 0.5 seconds for each color).

Start alternating pattern after 10 sec to acknowledge restore request and begin shutdown. A restore will only be successful if software is able to run.



Figure 23: Factory Defaults button

Chapter 4

Troubleshooting

Table 4: 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 Subsection 2.1. Ensure the USIM is pressed firmly into the SIM slot.
The Web UI will not connect to the terminal.	There is 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.	There is 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.
The terminal is connected to the network but cannot obtain the requested Quality of Service.	The network is temporarily unavailable.	Retry again. If the problem persists, contact your service provider.
The terminal does not obtain a GPS fix.	The terminal's location limits the visibility of three 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 toward the most open area of sky (normally straight up).

Problem	Possible cause	Possible solution
None of the above solutions resolve the problem.	The 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 5: 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 6: 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

Acronym	Definition
SQI	Received burst SQI
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

Acronyms

A

APN – Access Point Name

C

CAI – Common Air Interface

E

EML – EchoStar Mobile Limited

G

GPS – Global Positioning System

H

HW – Hardware

I

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

O

OS – Operating System

P

PIN – Personal

PUK – PIN Unlock Key (Password provided by the USIM card provider to unlock a lost/forgotten PIN code)

R

RJ – Registered Jacks

RTM – Remote Terminal Manager

RX – Receive

S

SIM – Subscriber Identity Module

SIM PIN – USIM Personal Identification Number (located on the USIM card)

T

TCP – Transmission Control Protocol

TE – Terminal Equipment

TX – Transmit

U

UDP – User Datagram Protocol

UI – User Interface

UMTS – Universal Mobile Telecommunications System

URI – Uniform Resource Identifier

USIM – UMTS Subscriber Identity Module

UT – User Terminal

W

Web UI – Web-based User In

