



Hughes 4510

User Guide

H65874
Revision C
May 18, 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.....	6
Warnings for satellite terminal.....	6
Equipment users.....	8
 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 the maintenance port	10
1.4.2 Additional hardware	10
 Chapter 2	
Using the Hughes 4510	13
2.1 Before getting started	13
2.2 Quick start.....	13
2.3 Connecting the terminal to the computer	13
2.3.1 Connecting via Ethernet.....	13
2.3.2 Connecting via USB	13
 Chapter 3	
Using the Web UI	15
3.1 Accessing the Web UI	15
3.2 Home page.....	15
3.3 Connections page	17
3.3.1 Cellular Connections	17
3.3.2 Satellite Connections.....	18
3.3.3 WAN Interfaces	19
3.3.4 APN Profiles.....	21
3.3.5 Connection Profiles	22
3.4 Settings page	23
3.4.1 General Setup.....	23
3.4.2 IP Address/DHCP	24
3.4.3 Ethernet Security.....	26
3.4.4 Security.....	26
3.4.5 Outbound Filters	28
3.4.6 Port Forwarding	30
3.4.7 Concurrent Routing.....	32
3.4.8 Remote Management	33
3.5 Usage	35
3.6 Support	36
3.6.1 Information	36

3.6.2	Troubleshooting	37
3.6.3	Cellular Diagnostics	38
3.6.4	Satellite Diagnostics	39
3.6.5	Update Software	40
Chapter 4		
Troubleshooting		42
Chapter 5		
Technical specifications		45
5.1	Features	45
Acronyms.....		46

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.



DANGER indicates a potentially hazardous situation which, if not avoided, *will* result in death or serious injury.



WARNING indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.



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:



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 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 the warning is active.



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, such as 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 all regulations and 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 interacting with the satellite terminal, we suggest you follow these guidelines:

- Maintain a distance of at least half meter between the front and sides of the main antenna 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..

1.1 Overview

The Hughes 4510 Satellite and Cellular Dual Mode Terminal provides reliable satellite connectivity over the EchoStar® Mobile GMR-1 3G satellite network and cellular networks for mobile packet data network applications. The Hughes 4510 Terminal comes in a very small form factor and is environmentally sealed for long-term outdoor installation or installation on a vehicle, fixed site, or boat. The installation consists of a single 4510 unit that can be placed at the end of a single cable carrying Ethernet and power. The SIM cards are mounted securely under the SIM cover.



Figure 1: Hughes 4510 terminal

1.2 About this user guide

This user guide contains the most up-to-date information available on this product when the guide was generated. It focuses on the specific information required to operate the Hughes 4510 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 4510 mobile terminal kit, you will find the following:

- Hughes 4510 terminal
- Quick Start User Guide
- Cellular SIM card tray (2 pieces)

Your service provider will supply you with a UMTS Subscriber Identification Module (USIM), its PIN, and the satellite terminal configuration instructions. You will need these to access the satellite network. In order to access the cellular network, you will need to acquire a cellular SIM card from your service provider or activate the integrated embedded SIM (eSIM) in the product.

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 the maintenance port

The following Operating Systems (OS) have been tested for their ability to support the maintenance port, which is intended to be a USB port, and 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 price list for the purchase of any additional optional 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.
Mating Power and Data Connector (bare)	9509554-0001	

Item	Part Number	Specifications
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.
SIM Tray	9510093-0001	SIM tray for insertable cellular SIM with the 4510 terminal. Two SIM trays will be provided in the kit box.

Chapter 2

Using the Hughes 4510

2.1 Before getting started

Follow these steps below before powering up the unit:

1. Remove the SIM door
2. Insert the satellite SIM card supplied by your service provider in the SAT SIM slot
3. Most users will be using the integrated eSIM, so no further action is required.

Note: If you are using a third-party cellular service, the insertable cellular SIM should be used.

- a. Insert the cellular SIM card supplied by your service provider in the CELL SIM holder provided.
- b. Insert the CELL SIM holder into the CELL SIM slot. These slots can be seen in [Figure 2](#).

Please refer to the Install Guide for further details on the installation.

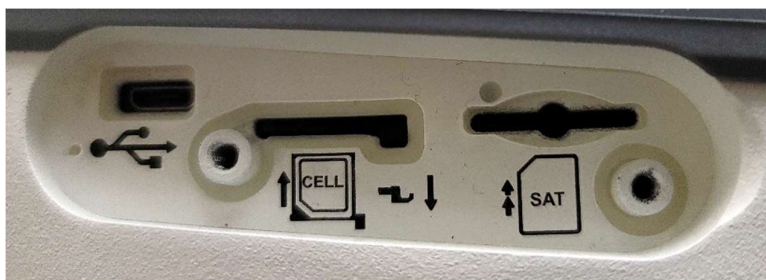


Figure 2: Hughes 4510 SIM slots

2.2 Quick start

The Hughes 4510 terminal must first obtain a GPS fix. In order to do this, 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 4510 with one or more of the following interfaces:

- Ethernet
- Micro-USB

2.3.1 Connecting via Ethernet

To connect the Hughes 4510 terminal to a device using Ethernet:

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

2.3.2 Connecting via USB

The common installation access port is the Micro-USB port. To connect the Hughes 4510 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 4510 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 in the address bar.

- If you are using an Ethernet port, enter the following Ethernet IP address:
 - `http://192.168.128.100`
- If you are using a USB port, enter the following maintenance IP address:
- `http://169.254.1.1`

The Web UI will then open the **Terminal Status** page. Along the top of all Web UI pages are icons representing the categories of available subpages, such as **Home**, **Connections**, **Settings**, **Usage**, and **Support**.

3.2 Home page

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

On the left side of the page is the **Status** bar. The fields in this section are updated automatically when the status of any item changes.

1. **Network:** This field indicates the status of the cellular and satellite connections. Once connected to the network, the **Terminal Status** page will show that the UT is registered with the network. It also shows the signal strength. See [Table 2](#) for additional information.
2. **Position:** This field displays the current position status. If the terminal acquired a GPS fix, it will display the latitude, longitude, altitude, last time the GPS position was updated, and geocoordinates in the Military Grid Reference System (MGRS). The time is displayed in UTC format.
3. **Terminal Properties:** This field has been designed to indicate miscellaneous status information.

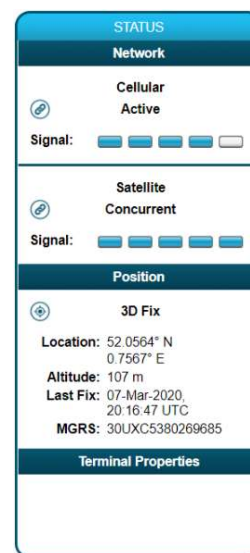



Table 2: Status bar messages






Status	Meaning	Comment
Connecting...	Connecting to cellular network.	Cellular only
Connect Failed	Attempt to connect to cellular network failed.	
Connected	Connected to cellular network (not yet ready).	
Stopping...	Stopping WAN connection/modem.	
Stopped	WAN connection/modem has been stopped.	
Pending	Cellular WAN is configured for ACA, and no devices are present.	
Attaching...	Connecting to satellite network.	Satellite only

Status	Meaning	Comment
Attach Failed	Connection to satellite network failed.	
Attached	Connected to satellite network (not yet ready).	
Concurrent	Concurrent Dual WAN feature activated. Using the primary and backup at the same time.	
Searching...	Searching for satellite/searching for cellular signal.	
Traffic Blocked	WAN failed ping test.	Displayed after a WAN fails a ping test
Restarting...	WAN is restarting.	
Ready	WAN is connected and ready but not active.	
Active	WAN is connected and ready and active for passing traffic.	
Disabled	WAN is disabled(WAN interfaces configuration).	
Upgrading	Upgrading terminal software (service mode).	
Rebooting	Terminal is rebooting.	
Resetting	Terminal is resetting to defaults.	

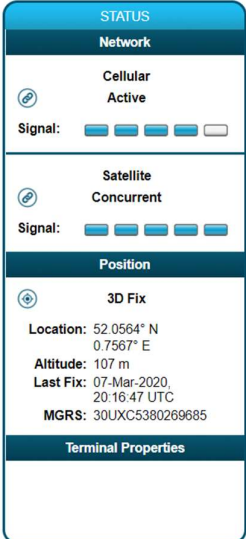
For basic satellite connectivity, the terminal functions with one signal bar. For more details, the user can reference the **Diagnostics** page to see if the Signal Quality (SQI) is at least 5 dB. It is desirable to have 10 dB or better.

Note: This does not apply to cellular connectivity.



Terminal Status



User Data Connection

You are using the Cellular Shared Connection.

Cellular Connection Status

Connected — Active

Satellite Connection Status

Connected — Concurrent

Connection Details

Local IP	APN Profile	Global IP
192.168.128.105	Cellular	Shared

Figure 3: Terminal Status page

On the **Terminal Status** page, you will find the following sections:

- **User Data Connection:** This section indicates the status of the cellular and satellite connections.
- **Connection Details:** This section displays *Local IP*, *APN Profile*, and *Global IP*.

3.3 Connections page

The **Connections** page allows the user to manage the data connections (cellular/satellite). The available subpages are as follows:

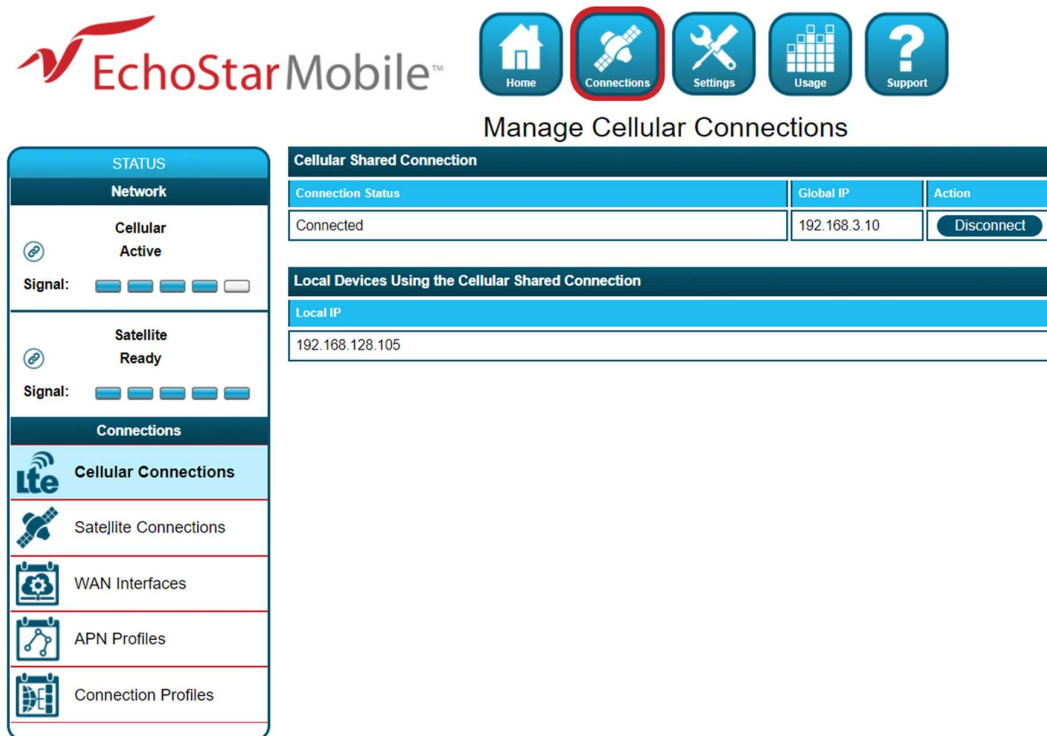
- **Cellular Connections**
- **Satellite Connections**
- **WAN Interfaces**
- **APN Profiles**
- **Connection Profiles**

3.3.1 Cellular Connections

This page allows the user to manage the cellular connections.

- **Cellular Shared Connection:** This section displays the connection status, the global IP address, and an action button to disconnect or connect.
- **Local Devices Using the Cellular Shared Connection:** This section displays the local IP addresses of all devices connected to the cellular shared connection.

As shown in [Figure 4](#), if the cellular connection is active (i.e., available and in use), the local IP address of the connected device will be displayed.



EchoStar Mobile™

Home Connections Settings Usage Support

Manage Cellular Connections

STATUS

Network

Cellular Active

Signal: [Progress Bar]

Satellite Ready

Signal: [Progress Bar]

Connections

Cellular Connections

Satellite Connections

WAN Interfaces

APN Profiles

Connection Profiles

Cellular Shared Connection

Connection Status	Global IP	Action
Connected	192.168.3.10	Disconnect

Local Devices Using the Cellular Shared Connection

Local IP
192.168.128.105

Figure 4: Cellular Connections page

3.3.2 Satellite Connections

This page allows the user to manage the satellite connections:

- **Satellite 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).

As shown in the example below, if the satellite connection is ready (i.e., available and in use), no local devices are using the satellite connection.

- **Dedicated Satellite Connection 1 and Dedicated Satellite 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 Terminal Equipment (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 Satellite Connections

STATUS

Network

Cellular Active

Signal: [Progress Bar]

Satellite Ready

Signal: [Progress Bar]

Connections

Cellular Connections

Satellite Connections

WAN Interfaces

APN Profiles

Connection Profiles

Satellite Shared Connection

Connection Status	Global IP	Action
Connected	10.15.0.50	Disconnect

Local Devices Using the Satellite Shared Connection

Local IP

The Satellite Shared Connection is not currently active

Dedicated Satellite Connection 1

Local IP	APN Profile	Global IP	Action
192.168.128.105	EchoStar Mobile	--	Connect

Dedicated Satellite Connection 2

Local IP	APN Profile	Global IP	Action
192.168.128.105	EchoStar Mobile	--	Connect

Figure 5: Satellite Connections page

3.3.3 WAN Interfaces

- **WAN Interface Configuration:** This section allows the user to select the primary and backup WAN interfaces and to enable or disable the Connection Watchdog feature.
 - **Primary WAN Interface:** Assigning priority to one WAN option (cellular or satellite) means that the highest-level priority is used as much as possible. If the primary WAN option is not meeting operational criteria, the terminal will switch to backup WAN (if available). Whenever the primary WAN is available, the terminal will switch back to the initial configuration.
 - **Backup WAN Interfaces:** If the primary interface is not available, the terminal will automatically switch the WAN interface in order to restore connectivity. When the primary WAN interface returns, the terminal will switch back to the initial configuration.
 - **Concurrent Backup WAN:** By enabling this feature, the user can route specified traffic over the backup WAN Interface. When this feature is enabled, the user can manage advanced configurations for the firewall, NAT, and routing.
 - **Connection Watchdog:** When this feature is enabled, the traffic on the link is monitored, and the terminal will perform a ping test on the active WAN interface if there is no traffic detected during the active period defined by the user. If the ping test fails, the terminal will switch WAN interfaces or reboot to re-establish the link.
- **Connection Watchdog Options:** This section allows the user to enable the Connection Watchdog feature for both WLAN interfaces (cellular and satellite). The user can also configure the following options:
 - **Active Monitoring:**
 - *Do not monitor*
 - *Monitor only incoming*
 - *Monitor only outgoing*
 - *Monitor bi-directional*
 - **Active 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 over the primary WAN, even when traffic flow is detected.
 - **Ping Servers:** This displays the IP addresses of servers to be used when verifying link connectivity. Each WAN interface should be configured to ping a maximum of three IP addresses, separated by commas. A successful ping will satisfy link connectivity, so the second IP address will only be pinged if the first server cannot be reached.
 - **Backup State Pings:** This feature allows the UT to send pings over the backup WAN to ensure that the link is ready.
 - **Backup Period:** This defines the interval between two consecutive pings on the backup interface. The default duration is 3 hours.

Note: The *Active Period* must be programmed for a longer duration than the anticipated rate of user traffic to avoid unnecessary ping tests and terminal reboots.

WAN Interfaces

STATUS

Network

Cellular Active

Signal:

Satellite Concurrent

Signal:

Connections

Cellular Connections

Satellite Connections

WAN Interfaces

APN Profiles

Connection Profiles

WAN Interface Configuration

Primary WAN Interface	Cellular
Backup WAN Interface	Satellite
Concurrent Backup WAN	<input checked="" type="checkbox"/> Route specified traffic over the Backup WAN interface
Connection Watchdog	<input checked="" type="checkbox"/> Monitor the terminal state and switch WAN interfaces/reboot to restore connectivity

Apply Changes

Connection Watchdog Options

When active monitoring is enabled, pings will be sent to test connectivity when no traffic has been detected.

WAN Interfaces

Cellular

Satellite

WAN Interface Details

Active Monitoring	Monitor bi-directional traffic for blockage
Active Period	Check for blocked traffic every 10 minutes
Always Send Pings	<input type="checkbox"/> Always send pings in active state, even when traffic is detected
Ping Servers	8.8.8.8
Backup State Pings	<input type="checkbox"/> Send pings in backup state to keep the connection ready
Backup Period	Send pings in backup state every 180 minutes

Apply Changes

Figure 6: WAN Interfaces page

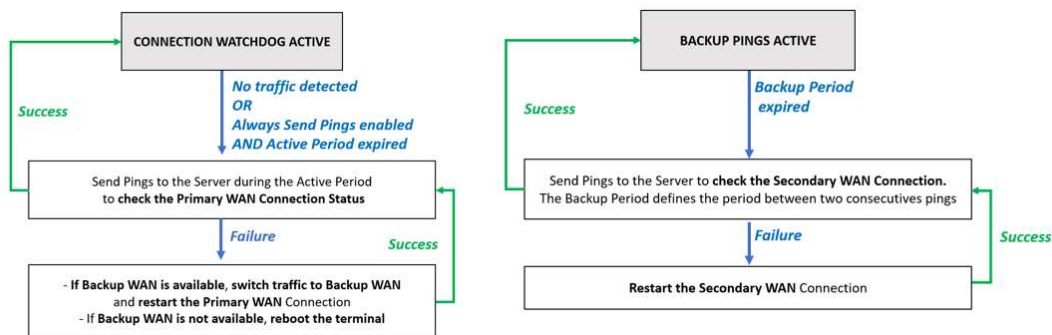


Figure 7: Functional diagram of Connection Watchdog and backup pings

3.3.4 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

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.

Note: The Cellular Default APN is hardcoded and configured to work with the cellular default user profile configured for EM SYNERGY Service. Additional APN profiles can be manually configured for use with insertable cellular SIM.

EchoStar Mobile™

Home Connections Settings Usage Support

APN Profiles

STATUS

Network

Cellular Ready

Signal: [Progress Bar]

Satellite Active

Signal: [Progress Bar]

Connections

Lte Cellular Connections

Satellite Connections

WAN Interfaces

APN Profiles

Connection Profiles

Profile Settings

Default Satellite APN Profile: Default Sat

The Default Satellite APN Profile cannot prompt for a password because it can be used 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	Profile Details
Cellular echostar	Profile Label: [Text Field]
Default Sat	Profile APN: [Text Field]
Satellite Dedicated 1	APN Username: [Text Field]
	APN Password: [Text Field]
	Prompt for Password: <input type="checkbox"/> Prompt for password when selecting profile
Remove Profile	Clear Form Add Profile Save Changes

Figure 8: APN Profiles page

3.3.5 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 Profile – Cellular Shared Connection:** This section allows the user to select the cellular SIM used (eSIM or insertable SIM), the APN profile of the cellular 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 the **Save** button.
Note: The eSIM option is always selected by default. The Cellular Default APN is configured to work with cellular default user profile configured for EM SYNERGY.
- **Connection Profile – Satellite Shared Connection:** This section allows the user to define the APN profile of the satellite 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 Satellite Connection 1 and Dedicated Satellite 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.

EchoStar Mobile™

Home Connections Settings Usage Support

Connection Profiles

STATUS

Network

Cellular Ready

Signal: [Progress Bar]

Satellite Active

Signal: [Progress Bar]

Connections

Cellular Connections

Satellite Connections

WAN Interfaces

APN Profiles

Connection Profiles

Cellular Shared Connection

Activation	Cellular SIM	APN Profile	Action
Always-On	eSIM	Cellular Default APN	Save

Satellite Shared Connection

Activation	APN Profile	Action
Always-On	Satellite Default APN	Save

Dedicated Satellite Connection 1

Enable	Activation	Local IP	APN Profile	Action
<input checked="" type="checkbox"/>	Manual	192.168.203.111	Satellite Dedicated 1	Save

Dedicated Satellite Connection 2

Enable	Activation	Local IP	APN Profile	Action
<input type="checkbox"/>	Manual	192.168.203.223	Satellite Default APN	Save

Figure 9: 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**
- **Outbound Filters**
- **Port Forwarding**
- **Concurrent Routing**
- **Remote Management**

3.4.1 General Setup

This subpage allows the user to configure general parameters of the Hughes 4510 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**.

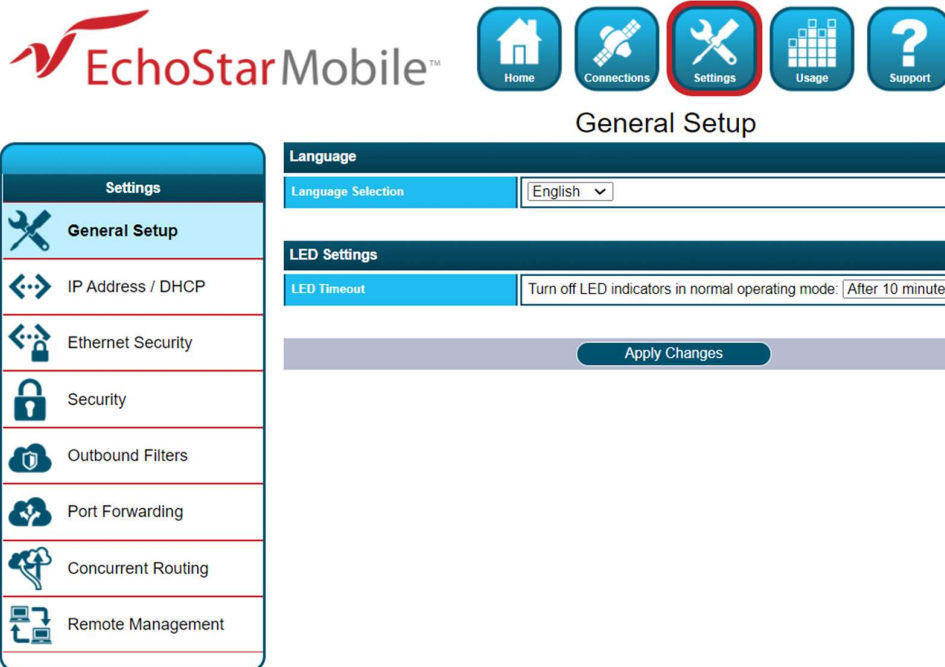


Figure 10: General Setup page

The LED states in normal operating mode are explained in the following table:

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

3.4.2 IP Address/DHCP

- **Terminal Local IP Address:** This section allows the user to change the local IP address of the terminal from the default Ethernet IP address of 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 change automatically. Changing the terminal's local IP address requires an immediate reboot.

Note: When updating the local IP address, 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

IP Address / DHCP Settings

Settings

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

Terminal Local IP Address

Terminal Local IP Address: 192 . 168 . 128 . 100

DHCP Server

DHCP Server: ☒ Enable DHCP Server

DHCP Address Range: 192.168.128.101 to 199

Apply Changes

DHCP Reservations

Reserved IP Addresses		Add A Detected Device	
IP Address	MAC Address	IP Address	MAC Address
192.168.128.115	AA:BB:CC:DD:EE:FF	192.168.128.105	34:e8:94:d7:b1:cc
<p>DHCP IP Address: <input type="text"/></p> <p>MAC Address: <input type="text"/></p> <p style="text-align: center;">Remove Save Add</p>			

Figure 11: IP Address/DHCP Settings page

- **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 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)
 - IP address ending in xxx.xxx.xxx.255
- 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.

3.4.3 Ethernet Security

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

- **Ethernet MAC Address Filtering:** The 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 Addresses* field.

EchoStar Mobile™

Home Connections **Settings** Usage Support

Ethernet Security Settings

Ethernet Security Settings

Ethernet MAC Address Filtering ☐ Enable Ethernet MAC Address Filtering

Apply Changes

Ethernet MAC Address Filtering

Allowed MAC Addresses

MAC Address

Remove

Add A Detected Device

IP Address	MAC Address
192.168.128.105	34 e8 94 d7 b1 cc

Add

Figure 12: Ethernet Security Settings page

3.4.4 Security

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


- **Satellite 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.


- **Satellite 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.


Security Passwords


Settings


 General Setup


 IP Address / DHCP


 Ethernet Security

 **Security**

 Outbound Filters

 Port Forwarding

 Concurrent Routing

 Remote Management

Satellite SIM PIN

A SIM PIN can be used to secure the installed Satellite SIM against unwanted use. The terminal will require the SIM PIN to be entered at startup.

Satellite SIM PIN is Disabled

Change Settings...

Satellite SIM Lock PIN

A SIM Lock PIN (up to 8 digits) can be used to lock the terminal to the installed Satellite SIM. The terminal will require the SIM Lock PIN before another Satellite SIM can be used.

Satellite SIM Lock PIN is Disabled

Change Settings...

Local Access Password

A Local Access Password can be used to prevent all local access to the terminal.

Local Access Password is Not Set

Change Settings...

Administration Password

An Administration Password can be used to prevent terminal settings from being changed.

Administration Password is Disabled

Change Settings...

Figure 13: Security Passwords page

- 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 requiring the password will appear if the administration password is enabled and the user attempts to change a protected configuration parameter.

Note: The **Advanced Settings** pages are protected by the administration password. If the user wants to commit changes on the **Advanced Settings** pages, the user will need the administration password.

Figure 14: Security Settings details

3.4.5 Outbound Filters

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

Note: If you have configured the advanced firewall configuration rules, you cannot make any changes on the **Outbound Filters** page. Go to the **Advanced Firewall Configuration** page at the bottom of the page to disable the feature.

- **Outbound Filters:** This section allows the user to enable or disable this feature by checking the box and clicking the **Apply Changes** button.
- **Outbound Filter Rules:** In this section, the user can configure the rule details and name the rule in the *Rule Details* section.

Outbound Filter Settings

Settings

General Setup

IP Address / DHCP

Ethernet Security

Security

Outbound Filters

Port Forwarding

Concurrent Routing

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

Remove Rule

Rule Details

Rule Name

Rule Precedence

Rule Action

Rule Enabled

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

Source Address (Optional)

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

Advanced Firewall Configuration

Click this button to access the Advanced Firewall Configuration settings.

Advanced Configuration

Figure 15: Outbound Filter Settings page

You can configure up to five rules and configure these parameters:


- *Rule Name*
- *Rule Precedence*
- *Rule Action: Block or 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 or UDP or TCP & UDP*

- **Advanced Firewall Configuration:** In this section, the user can configure advanced firewall rules by typing or by loading a file. Click the **Advanced Configuration** button to access the page dedicated to the configuration.

Note: For the *Advanced Rules* settings, a *Concurrent Dual WAN Configuration User Manual* document will be provided on request to ensure successful configuration at the



An EchoStar Company

Chapter 3 • Using the Web UI
H65874 Revision C

29

customer site. For more information, please visit our website:
<https://www.hughes.com/products-and-technologies/satellite-ground-systems/mobile-satellite-terminals/echostar-mobile-satellite-terminals>

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.

Figure 16: Port Forwarding page

Note: If you have configured the advanced NAT configuration rules, you cannot make any changes on the **Port Forwarding** page. Click the **Advanced Configuration** button to go to the **Advanced NAT Configuration** page and make your changes.

- **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*
- *Incoming Port*
- *Incoming Protocol: TCP or UDP or TCP & UDP*
- *Incoming Protocol*
- *Rule Enabled*
- **Port Triggering:** This allows 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 or UDP or 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

Advanced NAT Configuration

Click this button to access the Advanced NAT Configuration settings.

Advanced Configuration

Figure 17: Port Triggering and Advanced NAT Configuration

When the TE custom application opens *Trigger Port X*:

- NAT sets up a translation rule for *Trigger Port X*.
- NAT adds translation rules for network-initiated connections to Incoming Ports X1, X2, and X3 for a period of 120 seconds.

Figure 18: Port forwarding concept

- **Advanced NAT Configuration Rules:** In this section, the user can configure advanced NAT rules by typing or by loading a file. Click the **Advanced Configuration** button at the bottom of the page to access the page dedicated to the configuration.

Note: For the *Advanced Rules* settings, a *Concurrent Dual WAN Configuration User Manual* document will be provided on request to ensure successful configuration at the customer site. For more information, please visit our website:

<https://www.hughes.com/products-and-technologies/satellite-ground-systems/mobile-satellite-terminals/echostar-mobile-satellite-terminals>

HUGHES
An EchoStar Company

Chapter 3 • Using the Web UI
H65874 Revision C

31

3.4.7 Concurrent Routing

This page allows the user to enable the *Concurrent Routing* feature and configure the rules for outgoing traffic. The rules can be based on address and port numbers of source or destination based on the protocol.

Note: If you have configured the advanced routing configuration rules, you cannot make any changes on the **Concurrent Routing** page. Click the **Advanced Configuration** button at the bottom of the page to go to the **Advanced Routing Configuration** page to disable the feature.

- **Concurrent Routing:** This section allows the user to route specified traffic over the backup WAN Interface by enabling this feature. To enable or disable the feature check the box and click the **Apply Changes** button.
- **Advanced WAN Routing Rules:** In this section, the user can configure the rule details and name the rule in the table.

EchoStar Mobile™

Home Connections **Settings** Usage Support

Concurrent Routing

Concurrent Routing

Enable Concurrent Routing ☒ Route specified traffic over the Backup WAN interface

Apply Changes

Backup WAN Routing Rules

Route outgoing traffic onto the Backup WAN based upon the matching rules below.

Rules in Order of Execution

Rule Name

Remove Rule

Rule Details

Rule Name	
Rule Precedence	5 - Execute Rule First
Rule Enabled	<input type="checkbox"/> Enable Rule for Backup WAN Routing
Destination Address	
Source Address (Optional)	192.168.128 / 32
Type of Service (Optional)	
Rule Protocol (Optional)	

Clear Form Add Rule Save Changes

Advanced Routing Configuration

Click this button to access the Advanced Routing Configuration settings.

Advanced Configuration

Figure 19: Concurrent Routing page

You can configure up to five rules and configure these parameters:

- Rule Name
- Rule Precedence
- Rule Enabled
- Destination Address

- *Source Address*
- *Type of Service*
- *Rule Protocol*

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

- *Rule Name*
 - *Rule Precedence*
 - *Rule Enabled*
 - *Destination Address*
- **Advanced Routing Configuration:** In this section, the user can configure advanced routing rules by typing or by loading a file. Click the **Advanced Configuration** button to access the page dedicated to the configuration.

Note: For the *Advanced Rules* settings, a *Concurrent Dual WAN Configuration User Manual* document will be provided on request to ensure successful configuration at the customer site. For more information, please visit our website:

<https://www.hughes.com/products-and-technologies/satellite-ground-systems/mobile-satellite-terminals/echostar-mobile-satellite-terminals>

3.4.8 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 and the cellular connection. Click the **Change Settings** button to enable the 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.

After initial configuration, disabling Remote Management or changing the password will require the user to enter the current remote password.

Figure 20: Change Remote Management settings details

- **Remote Management Access Setup:** This section allows the user to configure the Remote Management setup. Click the **Apply Changes** button to save the settings changes.
 - **Primary Access Interface:** Remote access is not supported simultaneously through both WAN Interfaces. Therefore the user has to select a primary access interface from the dropdown menu.

- **Backup Access:** By enabling this feature the user allows the remote management to use backup access when the primary WAN interface is not available. This is a recommended setting.
- **Access Port:** The access port is always the same for both WAN Interfaces. Port 8443 is the default value, but the user can change the port number.
- **APN:** An Access Point Name must be provided for the satellite remote management connection. An APN username and password are required for operation.
- **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 then clicking the **Remove Address** button.
 - **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 field and then click the Add Address button. The IP address will appear in the Management Addresses table on the left.

EchoStar Mobile™

Home Connections **Settings** Usage Support

Remote Management

This terminal can be configured so that it can be managed remotely over a satellite or cellular connection.

Remote Management is Enabled
Change Settings...

Remote Management Access Setup

Primary Access Interface: Satellite

Backup Access: ☒ Allow remote management to use backup access when the primary access interface is not available

Access Port: Use port 8443 for HTTPS access to the terminal.

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

APN: echonet.eml.com

APN Username: remote_4510_new

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
100.64.96.244
100.64.96.203

Remove Address

Add Management Address

IP Address:

Clear Form Add Address

Figure 21: Remote Management page

3.5 Usage

This page shows the statistics of data transmitted and received (in megabytes) for each data connection (cellular and satellite).

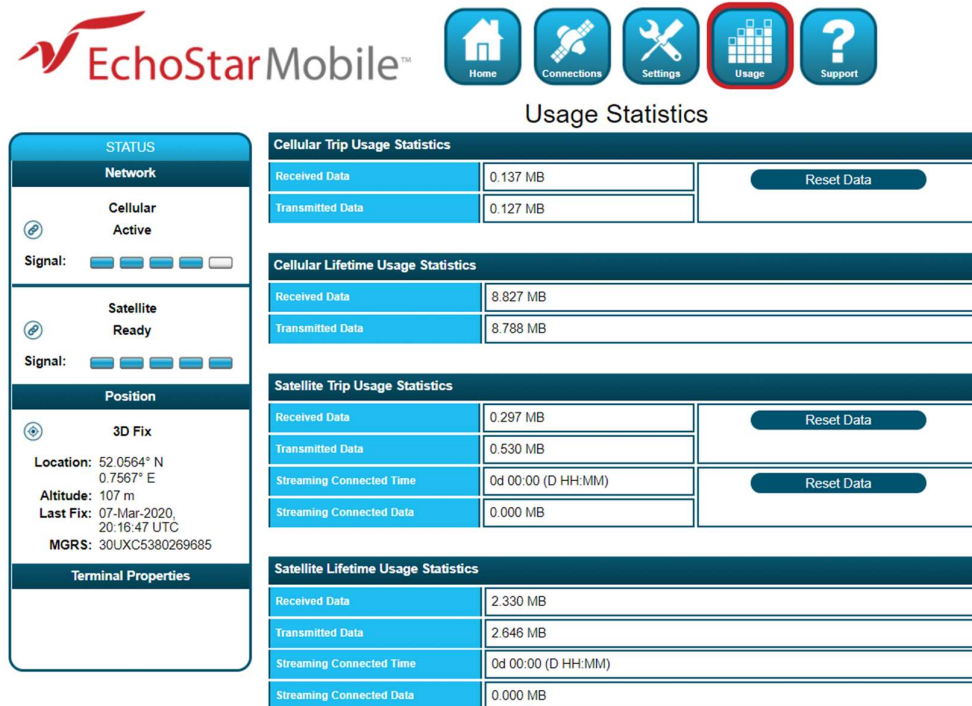


Figure 22: Usage Statistics page

NOTICE

The *Trip Statistics* can be reset, but the *Lifetime Statistics* cannot be reset, similar to the odometer of a car.

The *Usage Statistics* are only an estimate and do not reflect the actual billing system.

3.6 Support

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


- **Information**
- **Troubleshooting**
- **Cellular Diagnostics**
- **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.
- **Cellular Modem Information:** This section provides detailed information about the cellular modem and eSIM. Detailed information about the insertable cellular SIM card will be available if one has been inserted in the CELL SIM slot.
- **Satellite 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	4510
Software Version	5.4.1.1, 11-May-2021
Ethernet MAC Address	00:80:AE:7E:72:0F

Cellular Modem Information

Cellular Modem Information	
Cellular IMEI	358244088995752
Cellular Modem Software	REVISION 02.010
Selected Cellular SIM	eSIM
Cellular eSIM IMSI	234500012312778
Cellular eSIM ICCID	8944502404203127780
Cellular eSIM euCCID	89044045757727484800000000383698
Insertable Cellular SIM IMSI	
Insertable Cellular SIM ICCID	

Satellite Modem Information

Satellite Modem Information	
Satellite IMEI	353846-07-002456-6
Satellite Modem Software	5.4.1.1
Satellite Modem Firmware	FW 12.12.20190321 FPGA48
Satellite Modem Hardware	1
Satellite SIM IMSI	9015019800000008
Satellite SIM ICCID	8988250000000000112

Figure 23: 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 Mode**

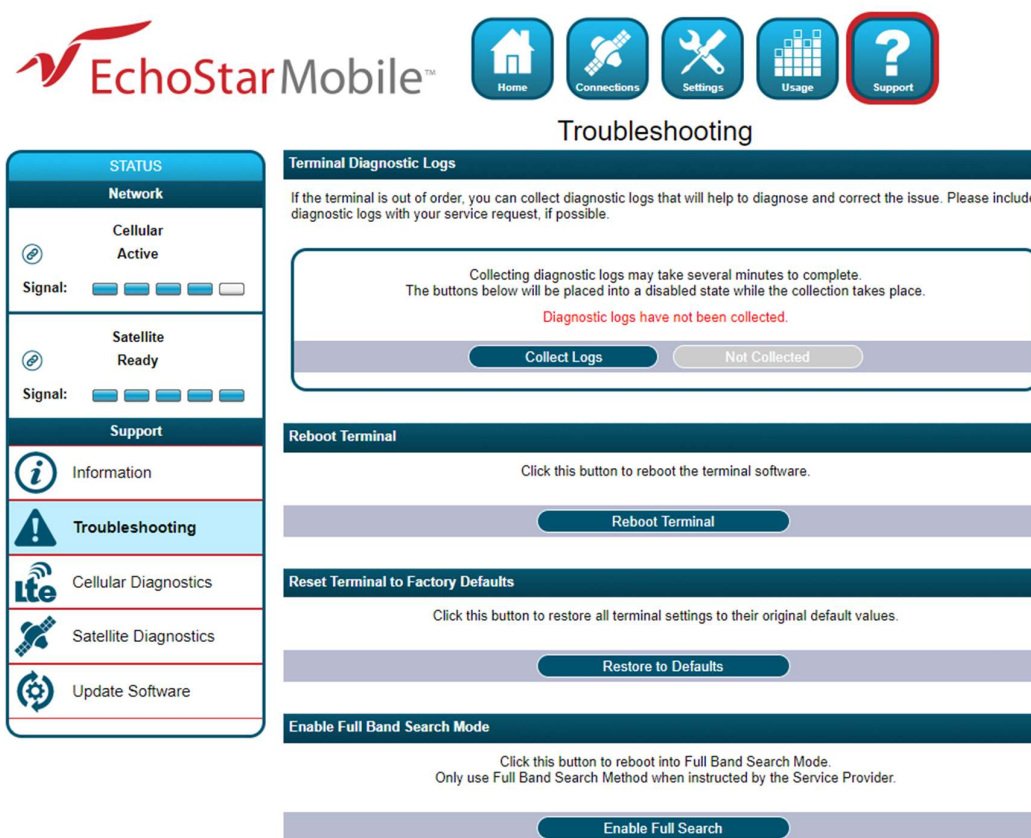


Figure 24: Troubleshooting page

3.6.3 Cellular Diagnostics

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

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



Figure 25: Cellular Diagnostics page

3.6.4 Satellite Diagnostics

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

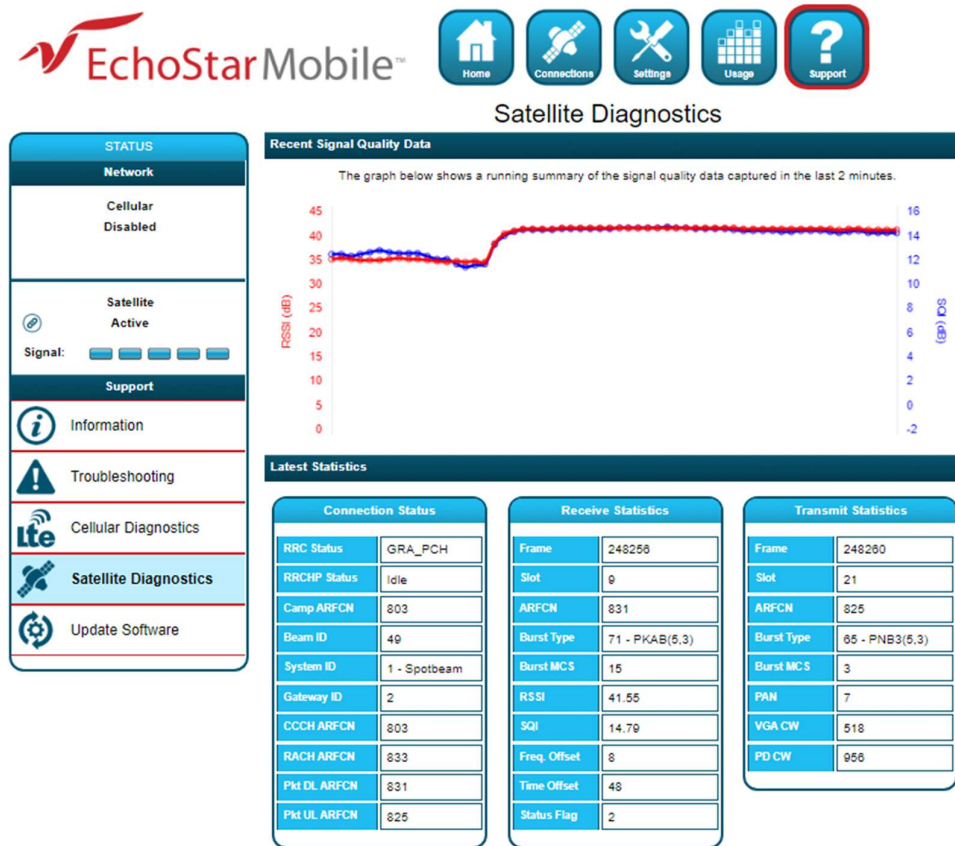


Figure 26: Satellite Diagnostics page

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
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)

Acronym/Term	Definition
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

3.6.5 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_4510_5.x.x.x.hif`, where `x.x.x` correspond 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.

NOTICE

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.

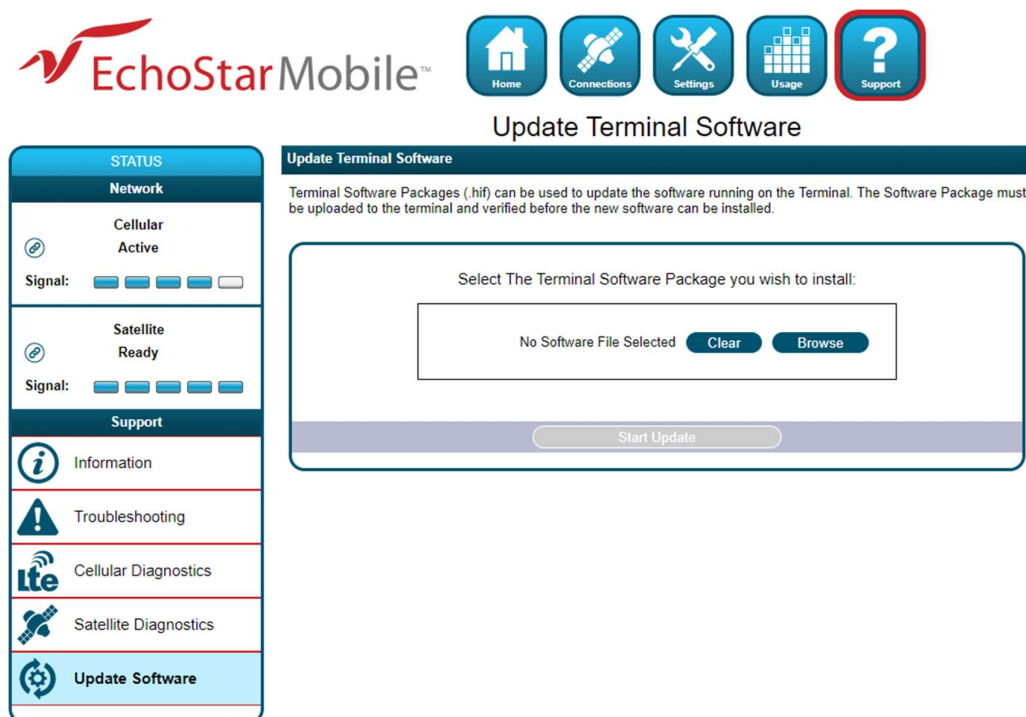


Figure 27: Update Terminal Software page

Chapter 4

Troubleshooting

Table 4: Troubleshooting

Problem	Possible Cause	Possible Solution
The terminal will not turn on.	The remote switch is off.	Connect and turn on the remote switch signal
Cannot get USIM card to lock into position.	The USIM is not correctly oriented for insertion.	Ensure that the USIM is oriented as shown in Section 2.1 on page 13. Ensure that 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 that 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 that 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 (QoS).	The network is temporarily unavailable.	Retry. If the problem persists, contact your service provider.

Problem	Possible Cause	Possible Solution
The terminal will 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 there is as much visibility of the sky as possible. Point the antenna toward the most open area of sky (normally, straight up).
None of the above solutions resolve the problem.	The terminal may have a hardware or software fault and needs to be rebooted.	Remove power. Wait 30 seconds. Reconnect the DC power and turn on the terminal.

Technical specifications

Table 5: Technical Specifications

Item	Specifications
SAT Transmit Frequency	1995–2010 MHz
SAT Receive Frequency	2185–2200 MHz
LTE Bands	1, 2, 3, 4, 5, 7, 8, 12, 18, 19, 20, 28
7-Band UMTS Bands	800, 850, 900, 1700/2100 (AWS), 1800, 1900, 2100 MHz (bands 1, 2, 4, 5, 8, 9, 19)
GSM Bands	850, 900, 1800, 1900
Fallback support for	GPRS/EDGE/HSPA+
GNSS Support	GPS
Weight	1.5 kg
Dimensions	248 mm x 178 mm x 115 mm
Operating Temperature	-25 °C to +65 °C
Storage Temperature	-40 °C to +80 °C
Humidity	95% RH at 40 °C
Wind Loading Survival	200 km/h
Water/Dust	IP-67
Input Voltage +12 V	(Vehicle)

5.1 Features

- S-band satellite operation with data rates up to 200 kbps forward and 150 kbps return.
- The omnidirectional satellite antenna allows for mobile communications with no moving parts.
- Global LTE CAT-1 operation enabled by either an eSIM or a replaceable 2FF SIM.
- Integrated cellular antenna.
- Integrated connection watchdog to ensure “always-on” network connectivity. No manual intervention is required to recover from an outage.
- Supports remote terminal management and firmware upgrades.
- Auto-on/auto-context activation automatically restores power and connection following loss of power or network issues.
- Low power consumption transmit: <16 W (SAT only); <6 W (CELL only); <20 W (SAT and CELL)
- Receive: <10 W
- Idle (SAT only): <1.3 W
- Idle (SAT and CELL): <3 W
- Off (remote switch control): <10 MW
- Simple installation: No PC required.
- Terminal can be vehicle-, pole-, or mag-mounted.
- Weatherproof (IP-67) enclosure.
- Built-in GNSS receiver

Acronyms

A

APN – Access Point Name

C

CAI – Common Air Interface

E

EM – EchoStar Mobile
eSIM – Embedded SIM

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

N

NAT – Network Address Translation

O

OS – Operating System

P

PIN – Personal Identification Number

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

R

RJ – Registered Jack

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

WAN – Wide Area Network

WLAN – Wireless Local Area Network

Web UI – Web-based User Interface