

## DRAFT

### MissionLINK User Guide

*This document contains technology controlled for export by the U.S. Department of Commerce in accordance with Export Administration Regulations. Diversion contrary to U.S. law prohibited.*



## RECORD OF CHANGES

[illegible]

**WARNING – INFORMATION SUBJECT TO EXPORT CONTROL RESTRICTIONS**

*This document contains technology controlled for export by the U.S. Department of Commerce in accordance with Export Administration Regulations (EAR). Diversion contrary to U.S. law prohibited. Include this notice with any reproduced portion of this document.*

**Export Compliance:**

This product is controlled by the export laws and regulations of the United States of America. The U.S. Government may restrict the export or re-export of this product to certain individuals and/or destinations. For further information, contact the U.S. Department of Commerce, Bureau of Industry and Security.

This product User shall comply with all applicable laws related to export and import of this product in any jurisdiction and/or government authority. User shall be responsible for complying with any and all export and import restrictions, laws and regulations in any country User is conducting business.

**Disclaimer:**

This manual contains information that is current as of the date shown on the front cover. Every effort has been made to ensure the correctness and completeness of the material in this document. The information in this document is subject to change without notice. Thales® and any other Thales trademark or Thales service mark referred to or displayed in this document are trademarks or registered trademarks of Thales.

**Legal Notices**

This product is subject to a Limited Warranty, Limitations, Exclusions, and Terms and Conditions, which can be found on line at [www.thalesdsi.com](http://www.thalesdsi.com).

Prior to Installing this product, read and understand this Installation Guide and the User Manual, including the safety warnings and information. Failure to do so could result in serious injury or death.

**Intellectual Property**

User acknowledges that the Products involve valuable patent, copyright, trademark, trade secret and other proprietary rights of Thales and others. No title to or ownership of any proprietary rights related to any Product is transferred to User or any Customer pursuant to the use of this product. The purchase of any Thales products shall not be deemed to grant either directly or by implication or otherwise, any license under copyrights, patents, or patent applications of Thales or any third party software providers, except for the normal, nonexclusive, royalty free license to use that arises by operation of law in the sale of a product.

**Content Copyright**

User is exclusively responsible for the use of this product, including proper use of third party copyrighted materials. If the User violates these terms, the User agrees to defend, indemnify and hold Thales harmless with respect to any claims or actions by third parties related to the improper use of copyrighted material and to pay all costs, damages, fines and other amounts incurred by Thales, or on its behalf, in the defense of any such claims or actions.

**Indemnity**

User agrees to defend, indemnify and hold Thales harmless with respect to any claims or actions by any governmental entities or other third parties related to any violation of law with use of the Product or Accessories, misuse of the Product or Accessories under these Terms and Conditions, or any other violation of these Terms and Conditions and further agrees to pay all costs, damages, fines and other amounts incurred by Thales, or on Thales's behalf, in the defense of any such claims or actions.

**SOFTWARE LICENSE**

The following terms govern User's access and use of the Thales-supplied software ("Software") contained on the Product or Accessories.

License. Conditioned upon compliance with these Terms and Conditions, Thales grants to USER a nonexclusive and nontransferable license to use for USER's internal purposes the Software and the Documentation. "Documentation" means any written information pertaining to the Software and made available by Thales with the Software in any manner. USER shall use the Software solely as embedded for operation of this product.

**No other licenses are granted by implication, estoppel or otherwise.**

**Thales Product Warranty Claim Process**

Please see the Thales website at [www.thalesdsi.com](http://www.thalesdsi.com).

**User Documentation:**

Thales Defense & Security, Inc. continually evaluates its user documentation for accuracy and completeness. Any suggestions you may have for changes or additions should be sent to [THALES\\_ILS@thalesdsi.com](mailto:THALES_ILS@thalesdsi.com) Subject Line: MissionLINK Installation Guide (PN 84468).



## Table of Contents

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1-1</b>
INTRODUCTION.....	1-1
ABOUT THIS MANUAL.....	1-1
THE IRIIDIUM SATELLITE NETWORK .....	1-1
<b>CHAPTER 2 SYSTEM OVERVIEW .....</b>	<b>2-1</b>
DESCRIPTION .....	2-1
<i>Terminal Unit (TU)</i> .....	2-4
<i>Broadband Active Antenna (BAA)</i> .....	2-6
CONTROLS AND INDICATORS .....	2-6
<i>Location of Controls – Terminal Unit</i> .....	2-6
<i>Indicators – Terminal Unit</i> .....	2-7
<b>CHAPTER 3 THALES MANAGEMENT PORTAL.....</b>	<b>3-1</b>
GETTING TO KNOW THE THALES MANAGEMENT PORTAL.....	3-1
<i>Menu Components</i> .....	3-3
<i>Main Dashboard</i> .....	3-7
<i>Status</i> .....	3-8
<i>Alerts</i> .....	3-11
<i>Calls</i> .....	3-13
<i>Distress</i> .....	3-14
<i>Settings</i> .....	3-16
<i>System</i> .....	3-32
<i>Diagnostics</i> .....	3-36
<i>About</i> .....	3-39
<i>Help</i> .....	3-41
<b>CHAPTER 4 GETTING STARTED .....</b>	<b>4-1</b>
GETTING STARTED .....	4-1
<b>CHAPTER 5 FIRMWARE UPGRADE.....</b>	<b>5-1</b>
1.1 DOWNLOADING THE FIRMWARE FROM THE THALES WEBSITE .....	5-1
1.2 INSTALLING THE FIRMWARE ON MISSIONLINK.....	5-2
<b>CHAPTER 6 TROUBLESHOOTING.....</b>	<b>6-1</b>
TROUBLESHOOTING.....	6-1
<i>System Resets</i> .....	6-5
<i>Alerts</i> .....	6-8
<b>CHAPTER 7 TECHNICAL SPECIFICATIONS .....</b>	<b>7-1</b>
TECHNICAL SPECIFICATIONS .....	7-1
TEMPERATURE .....	7-2
PHYSICAL CHARACTERISTICS .....	7-2
CONNECTOR DETAILS:.....	7-3
<i>General Purpose Inputs / Outputs (GPIO)</i> .....	7-3

TU 12V Connection Detail .....	7-5
TU 10-32VDC Connection Detail.....	7-6
<b>CHAPTER 8 ACRONYMS / GLOSSARY.....</b>	<b>8-1</b>
ACRONYMS / GLOSSARY.....	8-1
<b>CHAPTER 9 SPARE PARTS.....</b>	<b>9-1</b>
SPARE PARTS .....	9-1

## List of Figures

FIGURE 1-1 EARTH SHOWING IRIDIUM SATELLITES IN SIX DEFINED ORBITAL PLANES.....	1-2
FIGURE 1-2 TYPICAL IRIDIUM NETWORK FLOW OF A VOICE OR DATA CALL.....	1-3
FIGURE 2-1 3-CHANNEL VOICE CALLING OVERVIEW.....	2-1
FIGURE 2-2 UNLIMITED COMMUNICATIONS .....	2-2
FIGURE 2-3 MISSIONLINK SYSTEM WITH CONNECTED HARDWARE .....	2-3
FIGURE 2-4 TERMINAL UNIT (TU).....	2-4
FIGURE 2-5 TERMINAL UNIT FRONT PANEL DETAIL .....	2-5
FIGURE 2-6 TERMINAL UNIT BACK PANEL DETAIL .....	2-5
FIGURE 2-7 BROADBAND ACTIVE ANTENNA (BAA) UNIT .....	2-6
FIGURE 2-8 TERMIANL UNIT – POWER SWITCH AND USER CONNECTIONS .....	2-6
FIGURE 2-9 SYSTEM, SATELLITE AND WI-FI STATUS LED’S.....	2-7
FIGURE 3-1 QUICK LINK ICONS .....	3-3
FIGURE 3-2 QUICK LINK – SYSTEM STATUS .....	3-4
FIGURE 3-3 QUICK LINK – SATELLITE STATUS.....	3-5
FIGURE 3-4 QUICK LINK – WI-FI STATUS.....	3-5
FIGURE 3-5 QUICK LINK – LAN 1 STATUS (LAN 2 AND LAN 3 SIMILAR).....	3-6
FIGURE 3-6 QUICK LINK – WAN STATUS.....	3-6
FIGURE 3-7 THALES MISSIONLINK DASHBOARD - MAIN SCREEN .....	3-7
FIGURE 3-8 STATUS→ CURRENT DEVICES SCREEN.....	3-8
FIGURE 3-9 STATUS→ GPS SCREEN .....	3-9
FIGURE 3-10 STATUS→ LAN SCREEN .....	3-9
FIGURE 3-11 STATUS→ PHONES SCREEN .....	3-10
FIGURE 3-12 STATUS→ SERVICES SCREEN.....	3-11
FIGURE 3-13 STATUS→ SIM SCREEN.....	3-11
FIGURE 3-14 ALERTS SCREEN.....	3-12
FIGURE 3-15 CALL LOG SCREEN .....	3-13
FIGURE 3-16 CLEAR CALL LOG.....	3-13
FIGURE 3-17 DISTRESS (DISABLED VIEW).....	3-14
FIGURE 3-18 DISTRESS (ENABLED VIEW) .....	3-15
FIGURE 3-19 CONFIRMATION REQUIRED – SEND A DISTRESS MESSAGE .....	3-15
FIGURE 3-20 SETTINGS → GENERAL SCREEN .....	3-16
FIGURE 3-21 SETTINGS → DISTRESS (INITIAL SCREEN) .....	3-17
FIGURE 3-22 SETTINGS → DISTRESS .....	3-18
FIGURE 3-23 SETTINGS→ SATELLITE SCREEN .....	3-20
FIGURE 3-24 SETTINGS→ WI-FI SCREEN .....	3-22
FIGURE 3-25 SETTINGS→ LAN SCREEN .....	3-24
FIGURE 3-26 SETTINGS→ WAN SCREEN .....	3-26
FIGURE 3-27 SETTINGS→ PHONE SCREEN.....	3-28
FIGURE 3-28 SETTINGS→ DATA SCREEN .....	3-30

FIGURE 3-29 SETTINGS → LOCATION SERVICES SCREEN.....	3-31
FIGURE 3-30 SYSTEM → BACKUP SCREEN.....	3-32
FIGURE 3-31 SYSTEM → DATA USAGE SCREEN.....	3-33
FIGURE 3-32 SYSTEM → RESET.....	3-34
FIGURE 3-33 SYSTEM → FIRMWARE SCREEN.....	3-35
FIGURE 3-34 DIAGNOSTICS → SELF-TEST SCREEN.....	3-36
FIGURE 3-35 PERFORM SELF-TEST CONFIRMATION.....	3-36
FIGURE 3-36 DIAGNOSTICS → SATELLITE MODEM SCREEN.....	3-38
FIGURE 3-37 DIAGNOSTICS → LOGS SCREEN.....	3-39
FIGURE 3-38 ABOUT SCREEN.....	3-40
FIGURE 3-39 HELP SCREEN.....	3-41
FIGURE 4-1 TERMINAL UNIT FRONT PANEL DETAIL.....	4-1
FIGURE 4-2 MISSIONLINK IMEI AND IMSI FROM MOBILE DEVICE.....	4-2
FIGURE 4-3 INSTALLING SIM CARD AND ENGAGING THE LOCK.....	4-3
FIGURE 4-4 SYSTEM, SATELLITE AND WI-FI STATUS LED'S.....	4-3
FIGURE 4-5 MISSIONLINK USER INTERFACE LOGIN.....	4-5
FIGURE 5-1 SYSTEM → FIRMWARE.....	5-2
FIGURE 5-2 FIRMWARE BEING STAGED.....	5-3
FIGURE 5-3 SYSTEM → FIRMWARE UPDATE CONFIRM.....	5-3
FIGURE 5-4 FIRMWARE UPDATE IN PROCESS.....	5-4
FIGURE 5-5 SYSTEM → FIRMWARE UPDATE COMPLETED.....	5-5
FIGURE 6-1 LOCATION OF POWER BUTTON ON TERMINAL UNIT (TU).....	6-5
FIGURE 6-2 MANAGEMENT PORTAL - SYSTEM → RESET.....	6-5
FIGURE 6-3 RESET BUTTON.....	6-6
FIGURE 7-1 RADIO GATEWAY FOR ADVANCED LAND MOBILE SERVICES.....	7-3
FIGURE 7-2 GPIO CONNECTOR PIN DETAIL.....	7-4
FIGURE 7-3 12V INPUT AND MATING CONNECTOR DETAIL.....	7-5
FIGURE 7-4 10-32 VDC AND MATING CONNECTOR DETAIL.....	7-6

## List of Tables

TABLE 2-1 TERMINAL UNIT LED STATUS.....	2-7
TABLE 3-1 QUICK LINK ICONS.....	3-3
TABLE 3-2 THALES MISSIONLINK DASHBOARD - MAIN SCREEN.....	3-7
TABLE 3-3 SETTINGS → GENERAL SETTINGS.....	3-16
TABLE 3-4 SETTINGS → DISTRESS.....	3-18
TABLE 3-5 SETTINGS → SATELLITE.....	3-21
TABLE 3-6 SETTINGS → WI-FI.....	3-22
TABLE 3-7 SETTINGS → LAN.....	3-24
TABLE 3-8 SETTINGS → WAN.....	3-26
TABLE 3-9 SETTINGS → PHONE.....	3-29
TABLE 3-10 SETTINGS → DATA.....	3-30
TABLE 3-11 SETTINGS → LOCATION SERVICES.....	3-31
TABLE 4-1 TERMINAL UNIT LED STATUS.....	4-4
TABLE 6-1 TROUBLESHOOTING.....	6-1
TABLE 6-2 ALERTS / ERROR MESSAGES.....	6-8
TABLE 7-1 TECHNICAL SPECIFICATIONS.....	7-1
TABLE 7-2 OPERATING AND STORAGE TEMPERATURES.....	7-2
TABLE 7-3 PHYSICAL CHARACTERISTICS.....	7-2
TABLE 7-2 GPIO CONNECTOR PIN DEFINITION.....	7-4
TABLE 8-1 LIST OF ACRONYMS.....	8-1
TABLE 8-2 LIST OF DEFINITIONS.....	8-2
TABLE 9-1 LIST OF EQUIPMENT.....	9-1
TABLE 9-2 MISSIONLINK ACCESSORIES.....	9-2

## SAFETY

The MissionLINK system should only be installed by a qualified installers of land electronic systems. Improper installation could lead to system failure or could result in injury.. The following are general safety precautions and warnings that all personnel must read and understand prior to installation, operation and maintenance of the MissionLINK system. Each chapter may have other specific warnings and cautions.



**WARNING**

### **SHOCK HAZARD**

The MissionLINK system is a sealed system and is not meant to be opened for repair in the field by operators or technicians. Covers must remain in place at all times on the Terminal Unit and Broadband Active Antenna to maintain the warranty terms. Make sure the system is correctly grounded and power is off when installing, configuring and connecting components.



**WARNING**

### **DO NOT OPERATE IN AN EXPLOSIVE ATMOSPHERE**

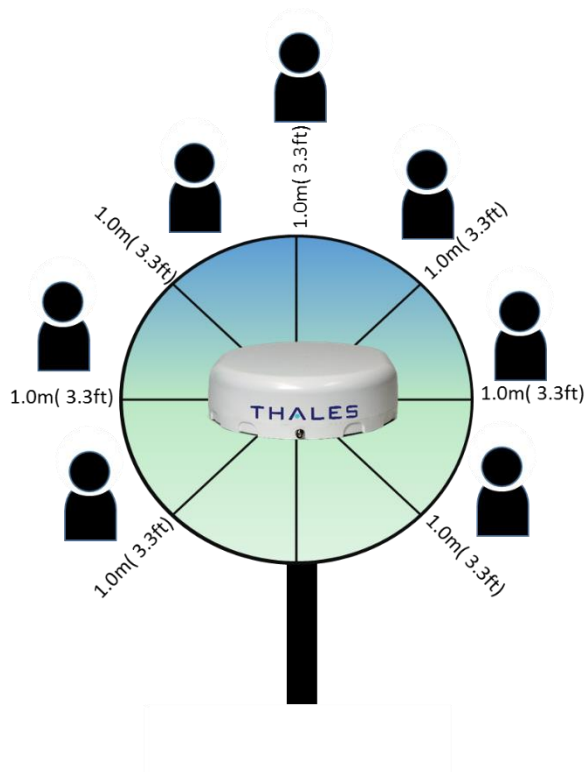
This equipment is not designed to be operated in explosive environments or in the presence of combustible fumes. Operating this or any electrical equipment in such an environment represents an extreme safety hazard.



## WARNING

### ANTENNA RADIATION HAZARDS

During operation, the antenna radiates high power at microwave frequencies that can be harmful to individuals. While the unit is operating, personnel should maintain a minimum safe distance of **1.0 meters (3.3 ft.)** from the antenna. The antenna should be mounted in an area that prevent the possibility of close exposure to the antenna's radiation.





## CHAPTER 1 INTRODUCTION

### INTRODUCTION

Thank you for your recent purchase of a Thales MissionLINK product. Powered by the Iridium global satellite network it's the only system with truly pole-to-pole coverage for voice and data communications. This USER MANUAL will cover a basic overview and advanced options of the MissionLINK system.

Additional information can be found in the following documents:

- The Thales MissionLINK installation process is simple and is covered in the Installation Manual (Document # 84465).
- The Thales MissionLINK Quick Start Guide (QSG) (Document # 3402174-1)

### ABOUT THIS MANUAL

This user manual is intended for anyone who intends to operate and configure the MissionLINK system. It, however, cannot cover all topics and advanced features. For questions or topics that are not covered in this manual please contact your airtime provider or Thales at [www.Thalesdsi.com/IRIDIUM/support](http://www.Thalesdsi.com/IRIDIUM/support).

### THE IRIDIUM SATELLITE NETWORK

The Iridium satellite network is comprised of 66 Low-Earth Orbiting (LEO), cross-linked satellites, providing voice and data coverage over Earth's entire surface. The satellites operate in six orbital planes, 781 kilometers (485 miles) from Earth. Each orbital plane has 11 satellites. Each satellite completes one orbit around Earth every 100 minutes, traveling at a rate of 16,832 miles per hour. There are spare satellites in orbit ready to replace a non-functioning satellite. Iridium has gateways in Arizona, Alaska and additional telemetry, tracking and control facilities in Canada and Norway. It is the largest commercial satellite constellation in the world.

This constellation ensures that every region on the globe is covered by at least one satellite at all times. Each satellite is cross-linked to four other satellites; two satellites in the same orbital plane and two in an adjacent plane.

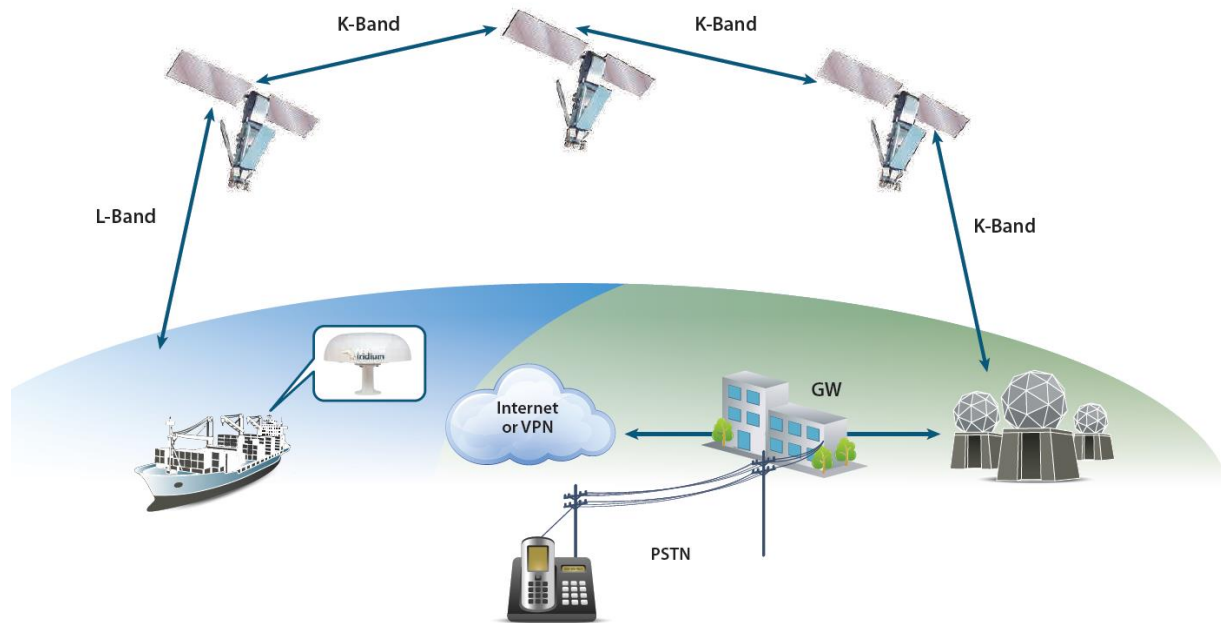
The Iridium NEXT satellite constellation replaces the older Block 1 Iridium satellite constellation and supports faster data rates, more capacity and better voice quality.



*Figure 1-1 Earth showing Iridium satellites in six defined orbital planes.*

Figure 1-2 shows a typical flow over the Iridium network of a call made from the MissionLINK system.

A MissionLINK voice or data call is sent to the closest satellite overhead that has a high signal strength. The traffic is then routed through the satellite network until it lands at the Alaska Ground Station, and, is then routed over terrestrial networks to the Gateway in Arizona. At the gateway, traffic is converted back to internet protocol (IP) and voice, depending on call type and delivered to the IP cloud or the public switched telephone network (PSTN).



*Figure 1-2 Typical Iridium network flow of a voice or data call.*

**THIS PAGE INTENTIONALLY LEFT BLANK**

## CHAPTER 2 SYSTEM OVERVIEW

### DESCRIPTION

The MissionLINK system operates using Iridium Certus<sup>SM</sup> broadband services over a network of 66 satellites that cover 100% of the globe, including remote locations and the poles. The solution utilizes this robust network service to provide highly reliable, mobile and essential voice, text and web communications. For best operation, a clear view of the sky is necessary as satellites can be as low as eight degrees above the horizon. The service capabilities of the system are outlined below.

#### Certus<sup>SM</sup> Multi-Services Platform

- Satellite data sessions up to 352kbps (current) & 700kbps (future)
- Streaming of 14.4 kbps up to 256kbps (future) → available 2019
- 3 high quality voice lines
- Short Burst Data
- Location tracking service with subscription at [www.clrSight.com](http://www.clrSight.com)

### Satellite Voice

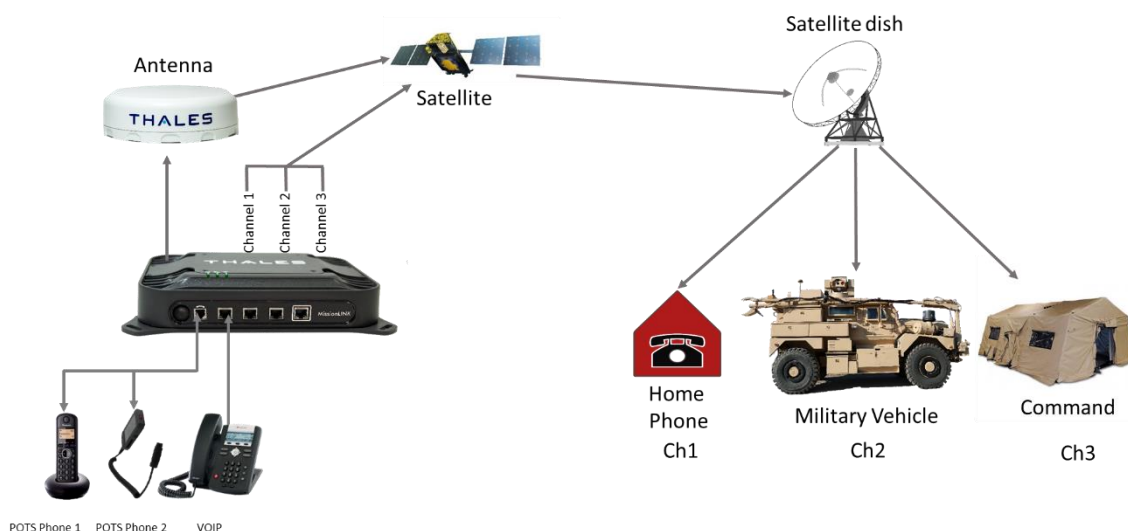


Figure 2-1 3-Channel Voice Calling Overview

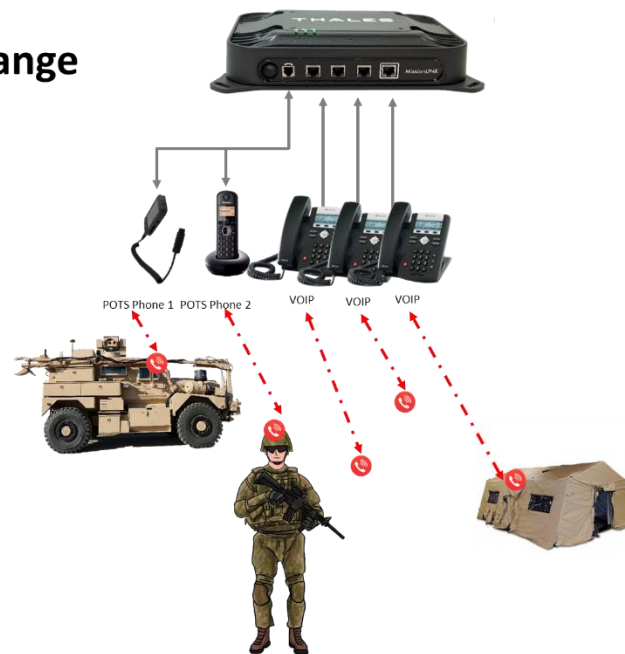


## Additional Features

- Embedded 802.11b/g/n Wi-Fi access point
- Multiple user capability
- Intuitive Management Portal user interface for configuration, monitoring and system status
- Application Programming Interface (API) for remote management and issue resolution
- PBX (Private Branch Exchange) functionality provides free local calling for internal vessel communications (see Figure 2-2).
- Least Cost Routing automatically switches the data path to an external non-Iridium network (i.e., cellular, Wi-Fi, etc.) for faster, lower cost transmission when connected
- Ruggedized tethered Thales IP Handset for system configuration, monitoring and voice calls (Future)
- Custom Thales softphone application for use on iOS and Android devices including the Thales IP handset
- IP67 BAA with single RF cable to the Terminal Unit (TU)
- Radio Gateway feature allows Land Mobile radios to access the satellite voice network

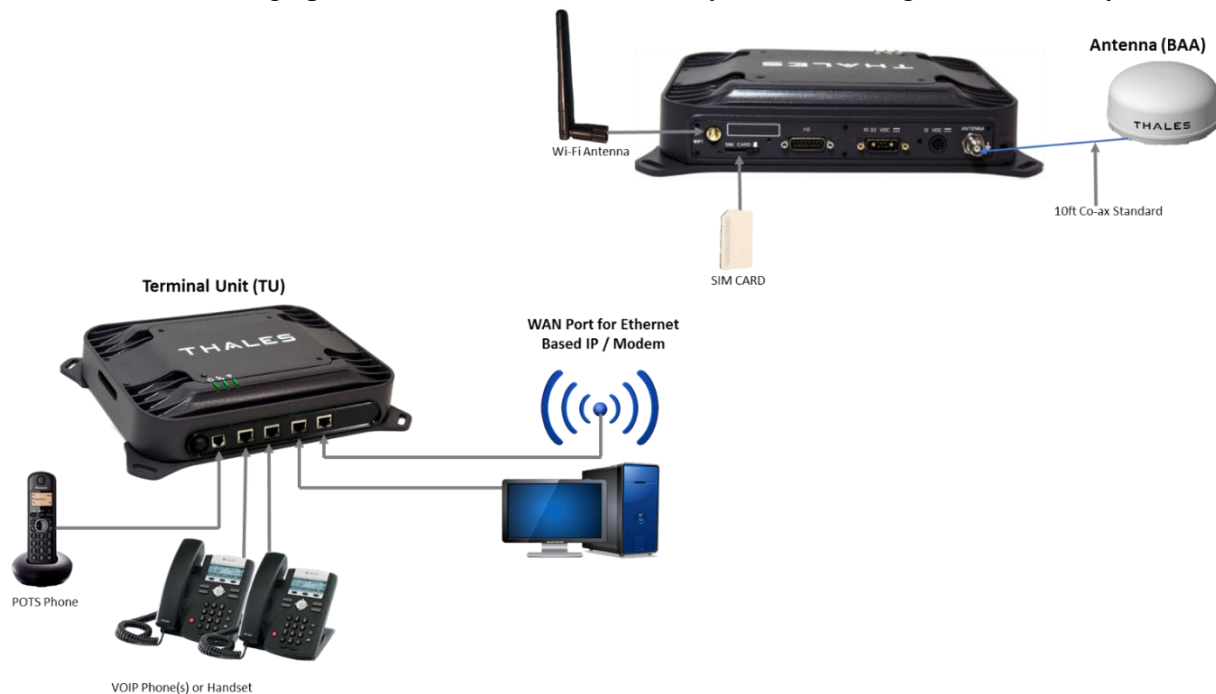
### **Private Bench Exchange (PBX)**

Local call extensions for calling



*Figure 2-2 Unlimited Communications*

A typical user setup that includes the standard kit items as well as a POTS phone, VoIP phones and a computer is shown in Figure 2-3. A cellular modem can be connected to the WAN port for data least-cost routing operations. Voice calls are always routed through the Iridium system.



*Figure 2-3 MissionLINK System with Connected Hardware*

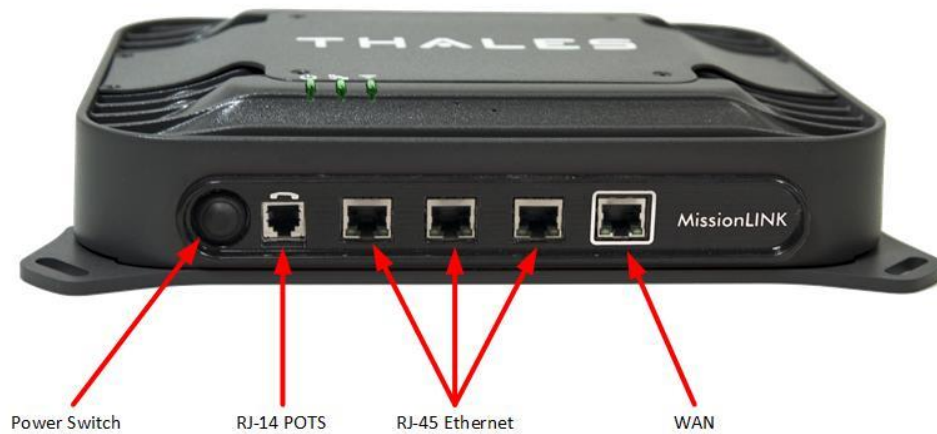
## Terminal Unit (TU)

The Terminal Unit (TU) supports voice and data communications in a land mobile or terrestrial fixed environment. The TU is capable of supporting wireless voice and data that links the user with the Iridium satellite network. The TU, depending on Line of Site (LOS) and LEO Satellites, will be able to maintain satellite connectivity while experiencing conditions varying from urban canyons to high vibration from road movement. As a wireless access point, the TU provides Wi-Fi (802.11) access for data. Three RJ-45 Ethernet connectors and one RJ14 jack enables the user to tether directly to the TU, if desired. The Management Portal is a graphical user interface that can be used to modify system settings and indicate system status. The TU is powered by an included DC power cable with a 10-32V input range, accommodating all types of vehicles and battery types. It also can be powered by an optional 12 Volt AC to DC power source for fixed applications where AC power or a DC power inverter is available.



*Figure 2-4 Terminal Unit (TU)*

The Terminal Unit has three status LEDs on the top of the unit that indicate status of system power-up, satellite connection and the Wi-Fi. The Terminal Unit front panel (left to right) has a main power switch, one RJ-14 jack for POTS (Plain Old Telephone Service) Phone(s), three POE (Power over Ethernet) RJ-45 connections for VoIP phones or Ethernet-based devices, and one WAN (Wide Area Network) connection primarily used to connect an external cellular modem.



*Figure 2-5 Terminal Unit Front Panel Detail*

The Terminal Unit back panel (left to right) has a Wi-Fi antenna connector, SIM Card slot, GPIO connector, 10-32Volt DC input connector, 12Volt DC power input, antenna connector, and chassis grounding lug.



*Figure 2-6 Terminal Unit Back Panel Detail*

## Broadband Active Antenna (BAA)

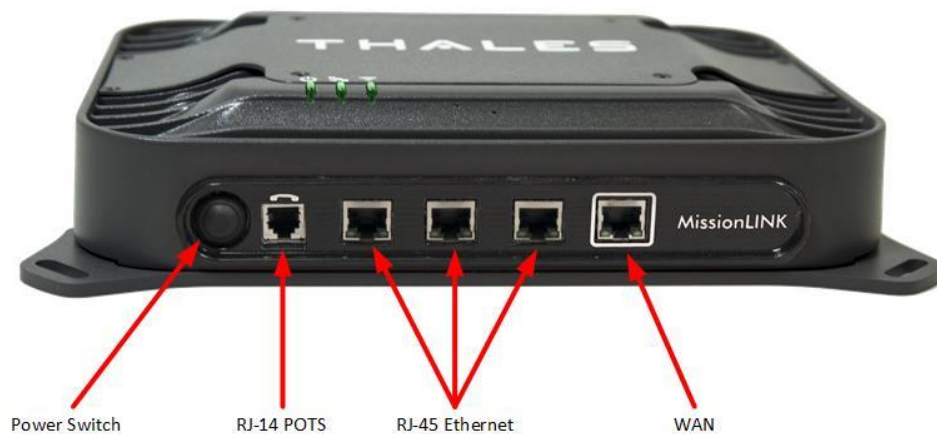
The BAA is a standalone unit that connects to the Terminal Unit through a single coaxial cable. DC power, RF transmit and receive signals, control data and GPS data are communicated between the BAA and Terminal Unit using this single coaxial cable. Connect provided cable to the antenna after installing the antenna and before connecting it to the Terminal Unit.



*Figure 2-7 Broadband Active Antenna (BAA) Unit*

## CONTROLS AND INDICATORS

### Location of Controls – Terminal Unit



*Figure 2-8 Terminal Unit – Power switch and user connections*






## Indicators – Terminal Unit



Figure 2-9 System, Satellite and Wi-Fi Status LED's

Table 2-1 Terminal Unit LED Status

Indicator	Description
 <b>System</b>	
Solid GREEN	System functioning properly
Flashing GREEN	System busy (Booting up)
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)
 <b>Satellite</b>	
Solid BLUE	Connected and passing data (over satellite)
Solid GREEN	System functioning properly
Flashing GREEN	Acquiring satellite
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)
 <b>Wi-Fi</b>	
OFF	Wi-Fi OFF
Flashing GREEN	Wi-Fi busy
Solid Green	System functioning properly
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)



### NOTE

The Indicator Colors are:

Solid Green: all is OK

Flashing Green: start-up or in progress of configuring or acquiring service.

Solid Red: fault requires user attention (Open management portal for Alerts)

Flashing Red: critical fault requiring immediate attention (Open Management portal and contact service provider.

## CHAPTER 3 THALES MANAGEMENT PORTAL



### NOTE

To access the Management Portal from a laptop:

- Power on the MissionLINK TU and let it boot up (may take a couple minutes)
- Open a web browser
- Type: <http://portal.thaleslink> (do not type .com or any other extension)
- The Management Portal appears in “guest” mode.
- To make changes, log in as an administrator by selecting LOGIN at the top of the window
- When prompted, enter the default Username (admin) and Password (admin)
- Immediately change the Password for added security (SETTINGS→GENERAL)



### NOTE

To access the Management Portal from a wireless device using Wi-Fi:

- Power on the MissionLINK TU and let it boot up (may take a couple minutes)
- On the wireless device, find and select THALES LINK as an available Wi-Fi access point.
- Open a browser and type: <http://portal.thaleslink> (do not type .com or any other extension)
- The Management Portal appears in “guest” mode.
- To make any changes, log in as an administrator by selecting LOGIN at the top of the window
- When prompted, enter the default Username (admin) and Password (admin)
- Immediately change the Password for added security (SETTINGS→GENERAL)

## GETTING TO KNOW THE THALES MANAGEMENT PORTAL

The Thales Management Portal is a graphical user interface with an intuitive menu structure that is used to configure and monitor the MissionLINK system. The Management portal provides key information and status alerts about the operation and condition of the system and Iridium network. The Thales Management Portal is resident on the TU and can be accessed and viewed on almost any smart device or computer including phones, tablets, laptops and desktop computers. The menu structure and content will automatically scale to the device’s screen size. The descriptions below are applicable for all devices but screen shots apply to larger display devices such as laptop computers. The actual view may vary depending on the size of the screen being used.

The Thales Management Portal is the primary user interface for the MissionLINK system. It provides four access levels, two of which are for local access and two for remote access to the system. Local access levels include “guest” access, which is for general users of the system that do not need to make configuration changes. The second local access is for administrators who need to view all data, perform software updates and make configuration changes. The first remote access level is for remote users who need to monitor of the system, but no configuration changes are permitted. This is similar to the “guest” access except that it is a remote user instead of a local user. The second remote access level is for remote administrators such as Service Providers. This level allows for viewing all data and making configuration changes through the custom Thales Application Programming Interface (API).

The guest access level is not password protected, so when the Management Portal is accessed, the guest user can view the current configuration and status of the system and any alerts that have been generated, but cannot change any parameters. The three other access levels are password protected. Passwords can be controlled and changed by the administrator in the **SETTINGS → GENERAL** menu, where the local administrator is denoted as “admin”, the remote user is denoted by “wan\_user” and the remote administrator is denoted by “wan\_admin”. By password control, the local system administrator can enable or prevent any remote access to the system.

Administrators, after initially logging in with the default Username (admin) and Password (admin), can view all data and also make changes to all the configuration settings to customize the MissionLINK system. It is highly recommended that the administrator creates a new Password immediately after signing in with the default username and password for added security and protection.

In the following pages, the Thales Management Portal is described in detail. Read through the entire contents before attempting to configure the TU for the first time.

When you first enter into the Thales Management Portal, menu items appear on the left side of the screen (see Figure 3-1). Each of these menu items is discussed in the following sections. A short description of each menu item is below.

- **Status** – Provides status of each of the items listed below. These screens cannot be edited and are provided for information only.
  - Current Devices
  - GPS
  - LAN
  - Phones
  - Services
  - SIM
- **Alerts** – Provides a listing of system alerts
- **Calls** – Provides information relating to Calls, including current calls, call history, and call management.
- **Distress** – Allows the operator to send a distress message.

- Settings – Enables the Administrator to configure parameters/ settings for sending messages, using Wi-Fi, WAN, LAN, Satellite, data, and phone.
- System – Enables the Administrator to perform system backups, view data usage, reset the system, and view/update system firmware.
- Diagnostics – Enables the administrator to run self-test, check system status, and view diagnostics logs entries.
- About – Provides system level information for the antenna, modem, power supply, system, VOIP Module, and Wi-Fi.
- Help – Provides a link to the MissionLINK User Documentation (Users Guide, Installation Instructions, and Quick Start Guide (QSG)).

## Menu Components

The System Status Icons at the top of the screen, highlighted in Figure 3-1, provide system level information that is useful to the user. When selected, these icons provide addition screen(s) of information and a quick way to make certain configuration setting changes by the administrator.

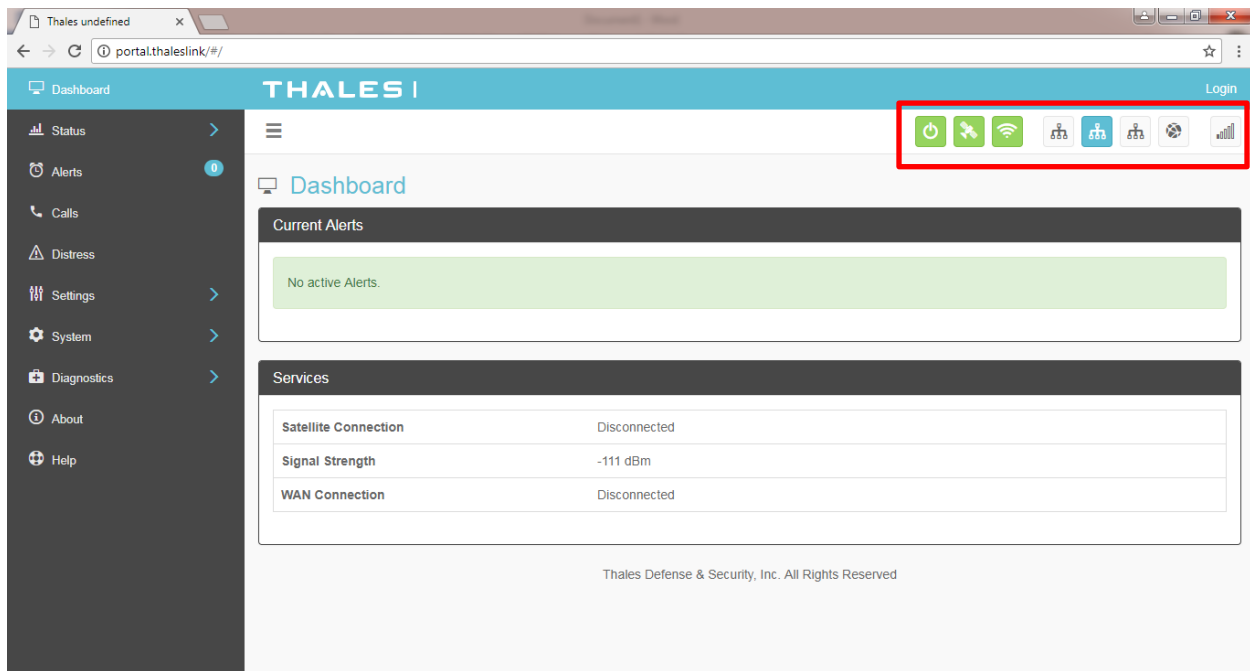








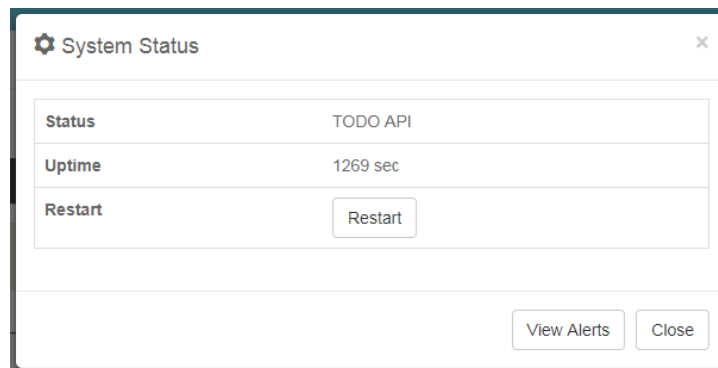
Figure 3-1 Quick Link Icons

Table 3-1 Quick Link Icons

ICON	Description
	System Status
	Satellite Status
	WI-FI Status

ICON	Description
	LAN 1, 2, and 3 Status
	WAN Status
	Signal Strength

- **System Status** – The System Status icon provides a quick view of the state of the system. It mirrors the status of the System LED on the TU. Selecting the System Status icon brings up the additional information in Figure 3-2. “Status” shows the current condition of the system. “Uptime” indicates how long the terminal has been in use. The RESTART button allows an administrator to reboot the terminal. Selecting VIEW ALERTS opens the ALERTS window and displays any Current Alerts.



*Figure 3-2 Quick Link – System Status*



## NOTE

If the system requires a “RESTART”, the operator can simply press RESTART to reboot the terminal. Once the system has rebooted, verify that you are connected to the WI-FI for the terminal. Once you are connected to the terminal, you will be prompted to reenter the user name and password.

- **Satellite Status** – The Satellite Status icon provides a quick view of the Satellite Status. It mirrors the status of the Satellite LED on the TU. Selecting the Satellite Status icon displays the information in Figure 3-3, showing “Connection Status”, “Signal Strength” and the “Current Data Path”. Selecting ACTIVATE / DEACTIVATE enables and disables data sessions. Changes will take effect once SAVE CHANGES is selected. Selecting VIEW STATUS will open the STATUS → SERVICES Window.



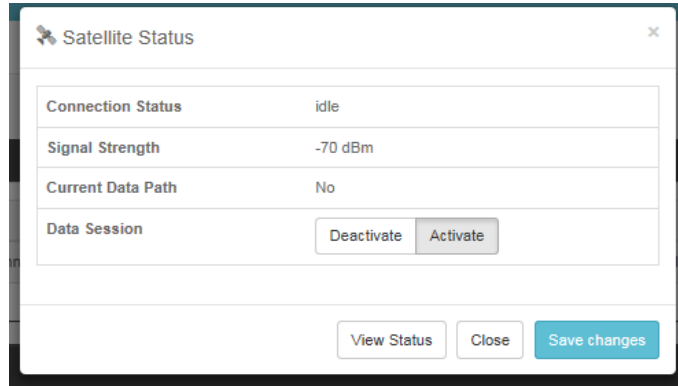


Figure 3-3 Quick Link – Satellite Status

- **Wi-Fi Status** – The Wi-Fi Status icon provides a quick view of the Wi-Fi status. It mirrors the Wi-Fi LED on the TU. Selecting the Wi-Fi Status icon displays the “Connected User Count” (number of users connected to the ThalesLINK Wi-Fi) and allows an administrator to **ENABLE** / **DISABLE** the Wi-Fi connection. Changes will only take effect once **SAVE CHANGES** is selected.



#### NOTE

If connected to the terminal through a Wi-Fi connection, disabling the Wi-Fi causes loss of the Wi-Fi signal and removal from the wireless device’s Wi-Fi menu. To regain use of the Wi-Fi, connect a computer via supplied Ethernet cable to the TU, open the Management Portal, select the Wi-Fi Status icon and select **ENABLE**.

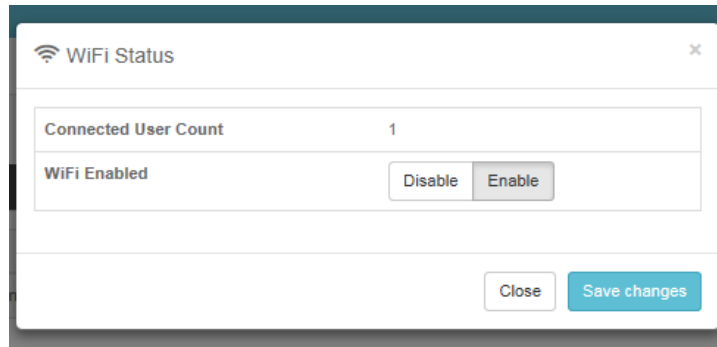
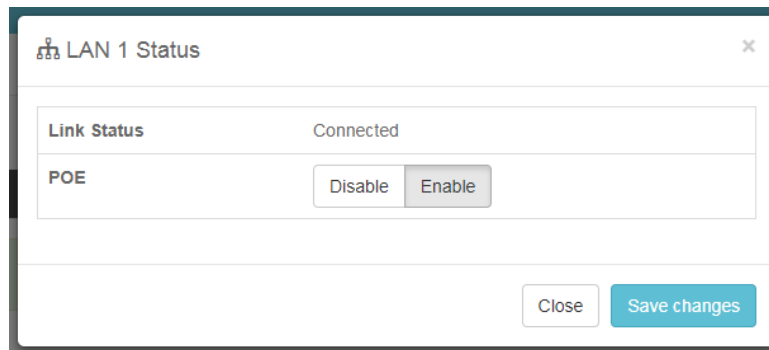


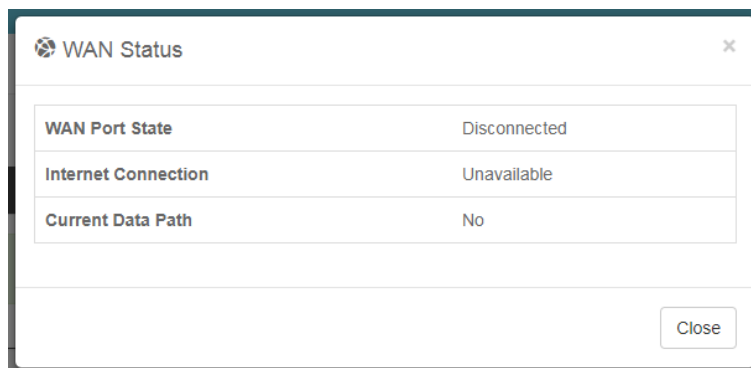
Figure 3-4 Quick Link – Wi-Fi Status

- **LAN Status Icons** – The LAN Status icons (LAN 1, LAN 2 and LAN 3) provide a quick view of each LAN’s Status. Each LAN icon is highlighted in blue when a device is plugged into it. By selecting a LAN icon, the additional information in Figure 3-5 is shown, displaying the “Link Status” and allowing for **ENABLE** / **DISABLE** of the Power over Ethernet (PoE) for that LAN.



*Figure 3-5 Quick Link – LAN 1 Status (LAN 2 and LAN 3 similar)*

- **WAN Status** – The WAN Status icon provides a quick view of the current connection status of the WAN port. The WAN Status icon will be highlighted in blue when an external WAN device is plugged into it. By selecting the WAN icon, the additional information in Figure 3-6 is shown. The details provided on this screen are for information only and include “WAN Port State”, “Internet Connection” and “Current Data Path”



*Figure 3-6 Quick Link – WAN Status*

- **Signal Strength Icon** – Displays the satellite signal strength as 5 vertical bars. More bars are highlighted as the signal strength rises.

## Main Dashboard

When first accessing the Management Portal by typing in <http://portal.thaleslink>, the Dashboard screen comes up by default. The Dashboard can also appear by selecting the top menu item highlighted in blue in Figure 3-7. From the Dashboard, you can see information relating to:

- Current Alerts
- Services

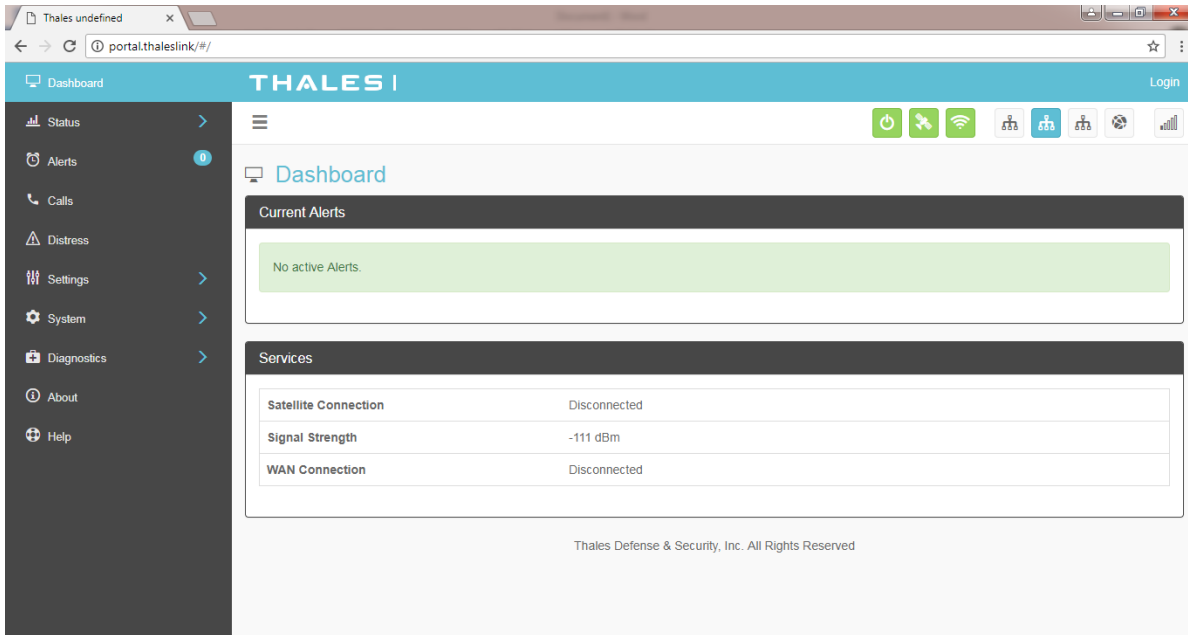


Figure 3-7 Thales MissionLINK Dashboard - Main Screen

Table 3-2 Thales MissionLINK Dashboard - Main Screen

Section	Value	Description
<b>Current Alerts</b>		
Alert Name	Text	Provides information relating all system issues summarized for easy reporting and debug/troubleshooting. For additional information, refer to Chapter 6 Troubleshooting
<b>Services</b>		
Satellite Connection	Disconnected or Connected	Displays whether or not the system is connected to a satellite
Signal Strength	Indicates the strength of the signal	Displays the current satellite signal strength in dBm
WAN Connection	Disconnected or Connected	Displays whether or not a WAN device is plugged into the TU and is connected to the internet

## Status



### NOTE

The STATUS selection screens (CURRENT DEVICE, GPS, LAN, PHONES, SERVICES and SIM) provide information only, and cannot be edited.

### Current Devices:

Displays all devices currently connected to the TU, both wired and via Wi-Fi. “WI-FI CLIENTS” list shows the MAC Address, Hostname and IP Address for the current Wi-Fi connected devices. “ALLOCATED IPS” list shows the MAC address, hostname and IP Address for all devices that have recently been connected to the TU.

MAC	Hostname	IP Address
F0:D7:AA:44:4E:A9	android-95b11c5ec7a17efd	192.168.55.103
90:06:26:65:68:17	android-651626260b9aa1b	192.168.55.104
38:D5:47:4D:BE:AC		

MAC	Hostname	IP Address
D8:BB:2C:57:A3:0D	Work-phone	192.168.55.101
EC:F4:BB:04:F8:C3	SJ-8F3SM12-LT	192.168.55.102
F0:D7:AA:44:4E:A9	android-95b11c5ec7a17efd	192.168.55.103
90:06:26:65:68:17	android-651626260b9aa1b	192.168.55.104
38:D5:47:4D:BE:AC		

Thales Defense & Security, Inc. All Rights Reserved

Figure 3-8 Status → Current Devices Screen

## GPS

The GPS page, provides detailed GPS information as shown in Figure 3-9.

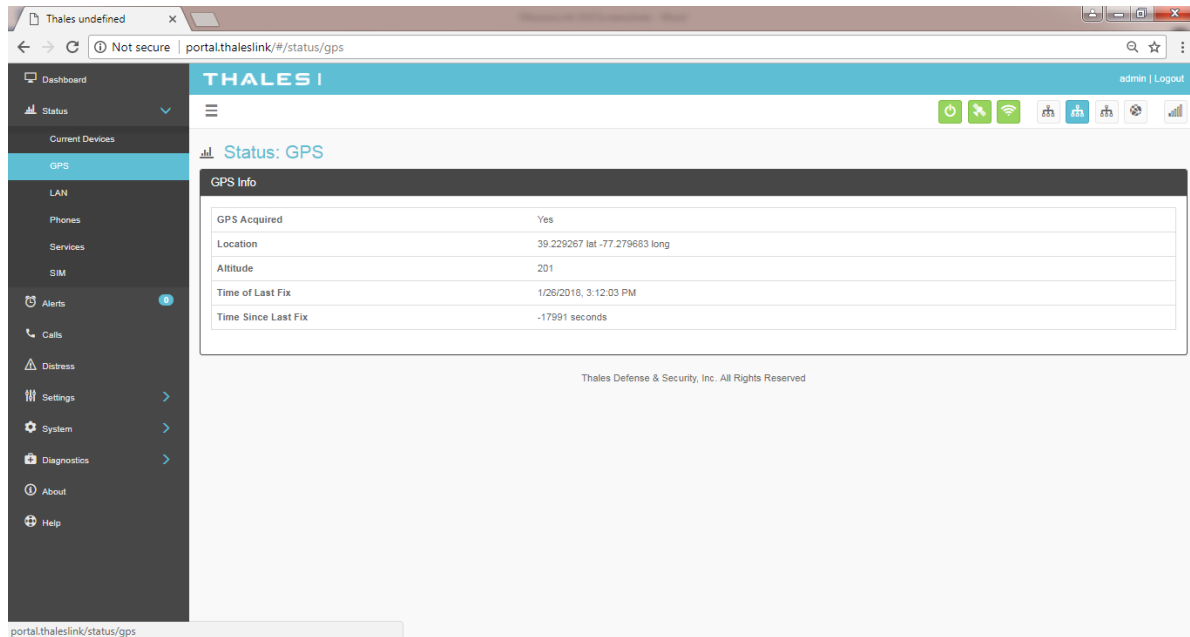


Figure 3-9 Status → GPS Screen

## LAN

The LAN page displays the connection status of the built-in Wi-Fi access point and the LAN ports as shown in Figure 3-10.

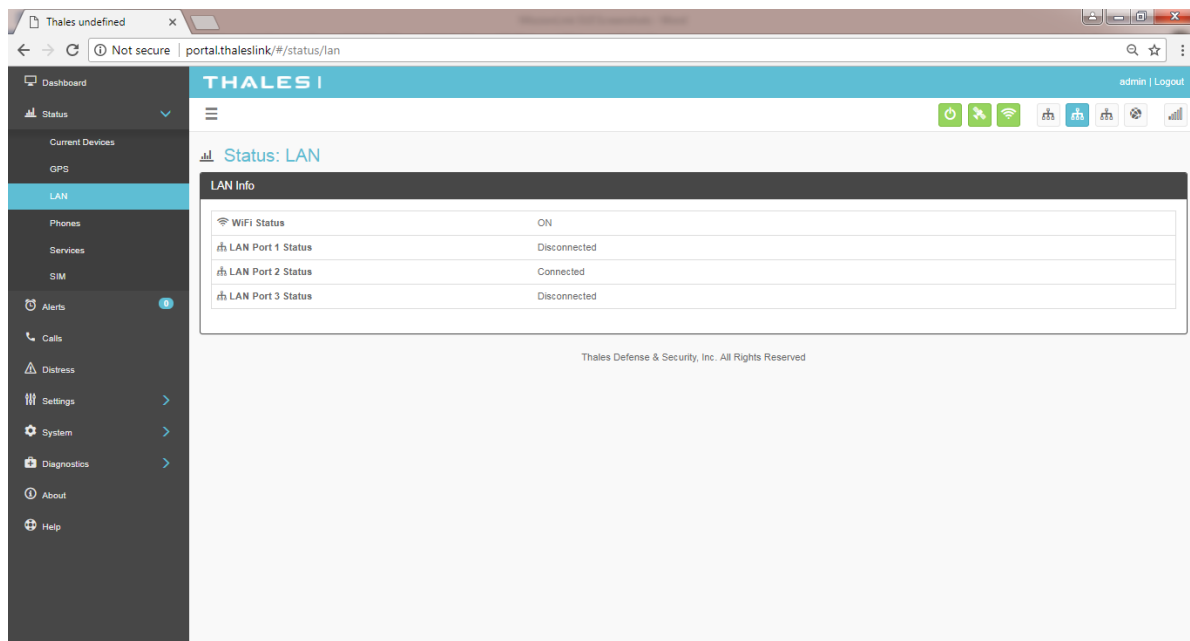


Figure 3-10 Status → LAN Screen



## Phones

The Phone page provides a list of the registered phones that are connected to the system, including the extension that was assigned as shown in Figure 3-11.

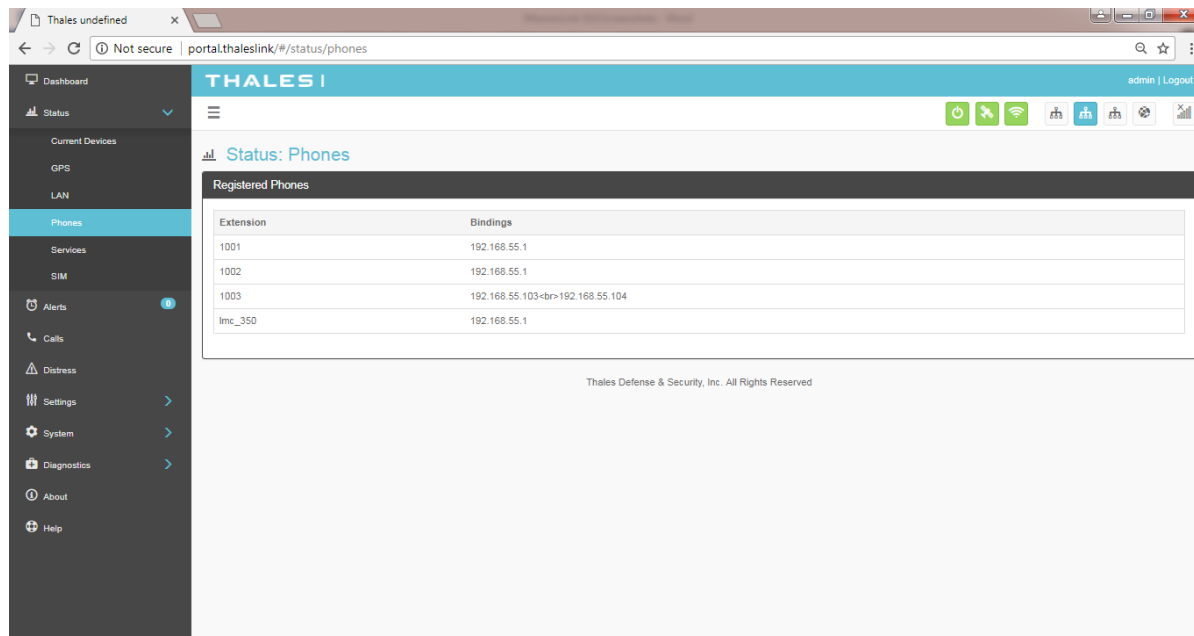


Figure 3-11 Status → PHONES Screen

## Services

The Services page provides the status of Satellite and WAN networks, and the current data route as shown in Figure 3-12.

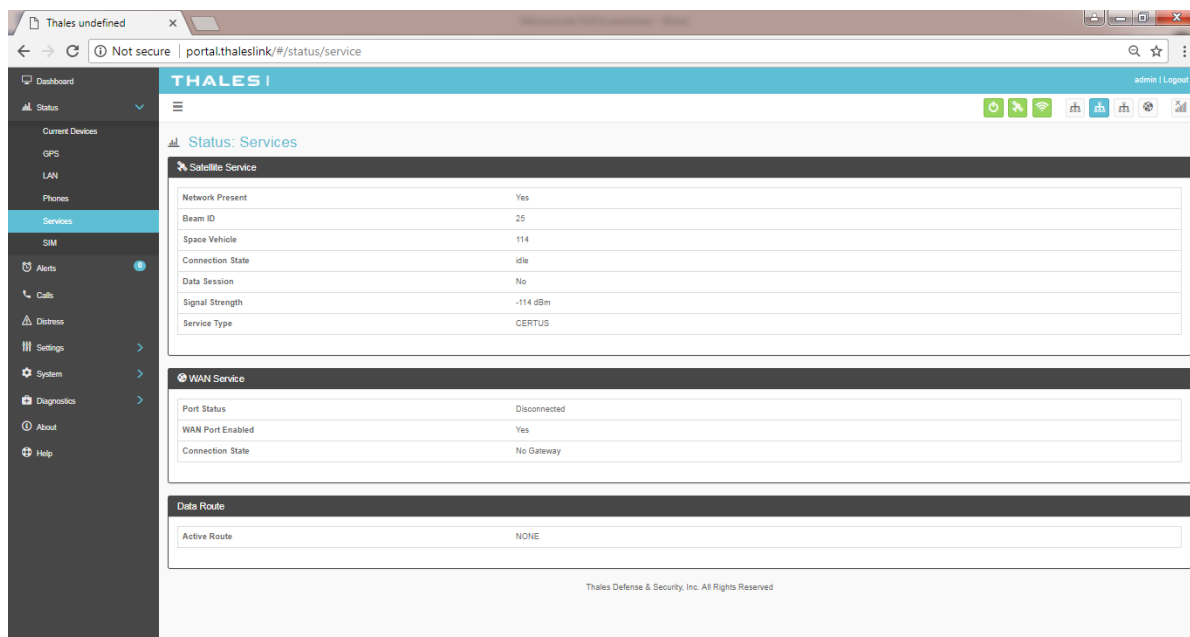


Figure 3-12 Status → SERVICES Screen

## SIM

The SIM page (Figure 3-13) provides the following information:

- **SIM Info** – Status of the SIM card, and its Unique IMSI ID number. The max data rate shows the Certus<sup>SM</sup> service level that the SIM card is provisioned to.
- **Voice Lines** – This section lists the three dedicated Iridium voice lines, what type they are and what their MSISDN is.

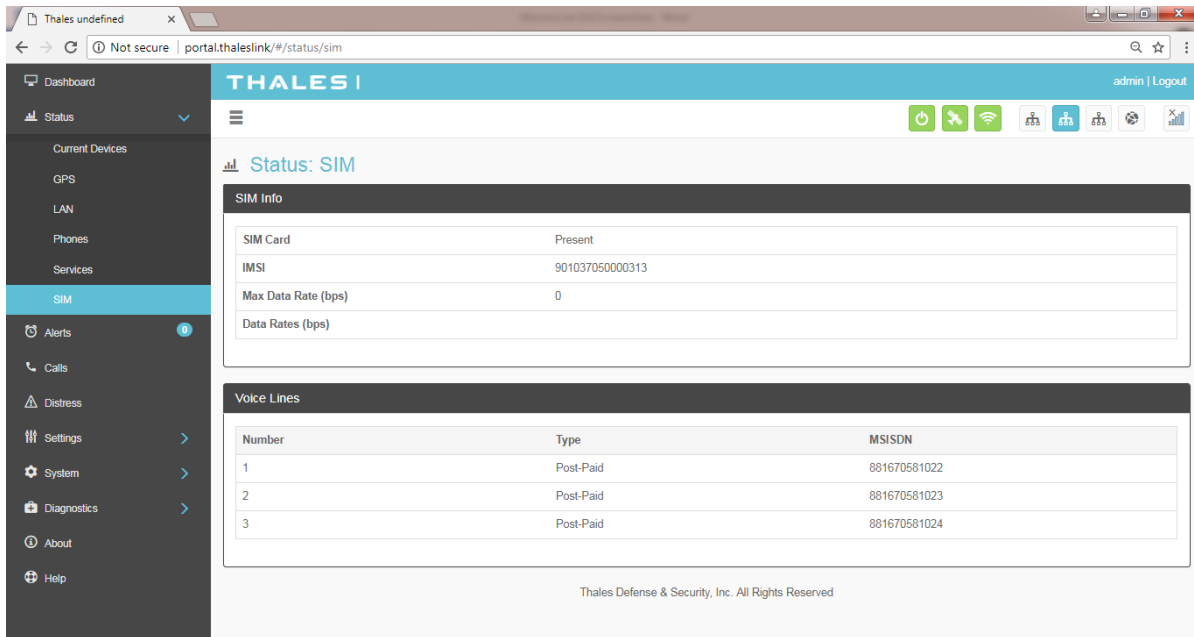
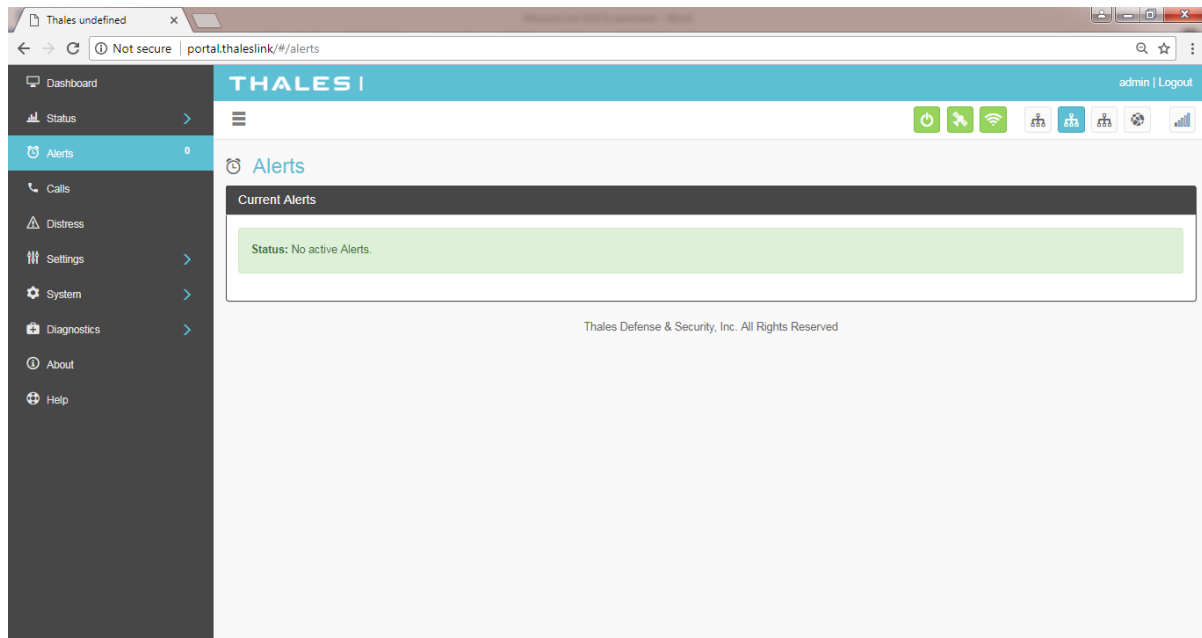


Figure 3-13 Status → SIM Screen

## Alerts

The ALERTS screen (Figure 3-14) will display a list of active Alerts from the system. These alerts may have been generated from a Power-On Self-Test (POST) or during normal operation of the system. The alerts indicate that something may be wrong with the system or network. The alerts will clear if they are no longer affecting the system operation.



*Figure 3-14 ALERTS Screen*



## NOTE

For additional information, refer to Chapter 6 Troubleshooting

## Calls

Selecting the Calls menu item (Figure 3-15) provides the call logs for active and past calls.

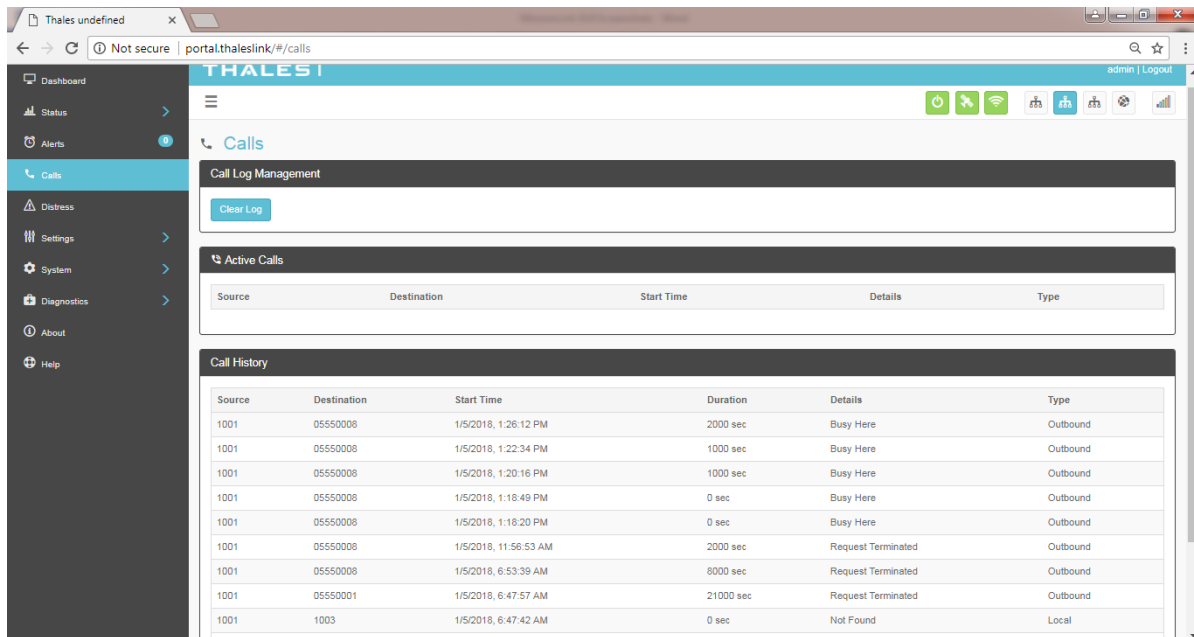


Figure 3-15 Call Log Screen

Under CALL LOG MANAGEMENT, the operator can CLEAR the call log by selecting CLEAR LOG and then confirming by selecting YES, CLEAR LOG.



Figure 3-16 CLEAR Call Log

## Distress



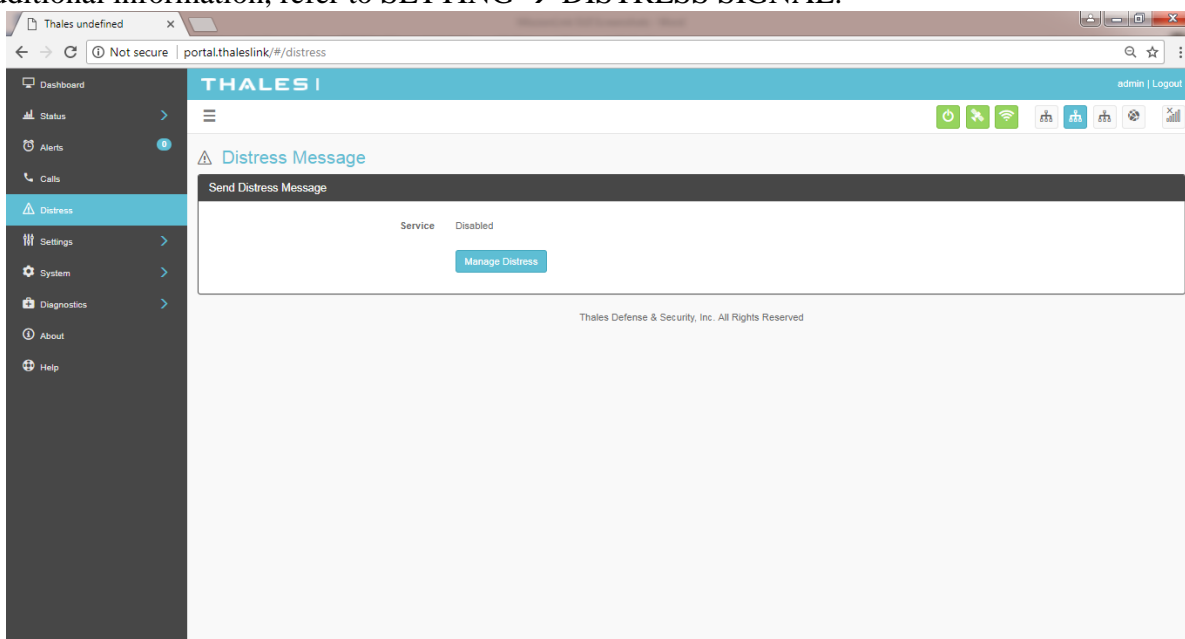
### NOTE

Distress calls can only be configured by the administrator. If the user is not logged in as ADMIN and selects MANAGE

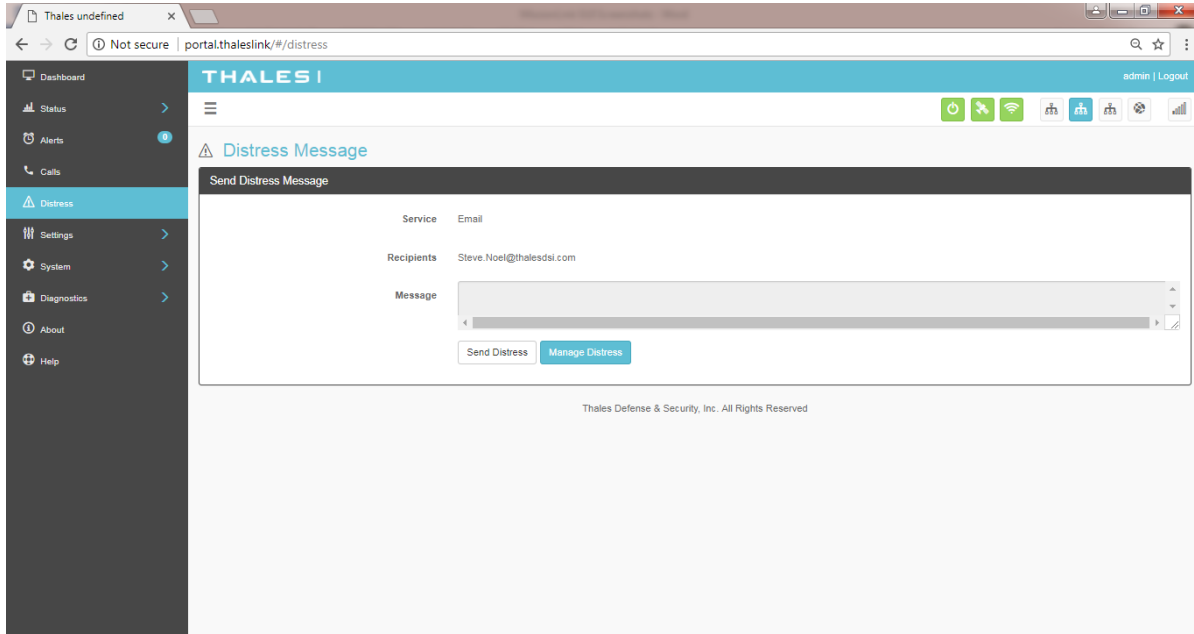
DISTRESS, the user will see icon, indicating this function is not available.

The Distress menu item allows for enabling and sending a distress email message.

Selecting MANAGE DISTRESS will open the SETTING → DISTRESS SIGNAL screen. From here, set up the Distress Message by selecting Email from the drop down box. Once the required email information has been entered, including the message to be sent, select APPLY. For additional information, refer to SETTING → DISTRESS SIGNAL.



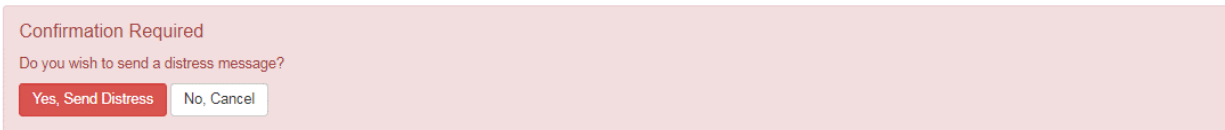
*Figure 3-17 DISTRESS (Disabled View)*



*Figure 3-18 DISTRESS (Enabled View)*

### Sending a DISTRESS MESSAGE:

To send a DISTRESS MESSAGE, press SEND DISTRESS. A pop-up screen will appear asking you to confirm that you want the message to be sent. Select YES, SEND DISTRESS to send or NO CANCEL to abort the message.



*Figure 3-19 Confirmation Required – Send a Distress Message*



### **NOTE**

No external indication is given when distress is activated. This discretion is for user safety in emergency situation. The only indication of distress will be in management portal under Distress menu item.

## Settings

The Settings tab of the portal is the most important section for customizing user configurations and feature settings. It is also advised that only experienced personnel change these settings as they may adversely affect functionality if not set correctly. These settings are under password control to prevent unauthorized personnel from making changes to the system.

### General

From the General page, the user can set the Language and Time Zone, and also change passwords as shown in Figure 3-20 and Table 3-3.

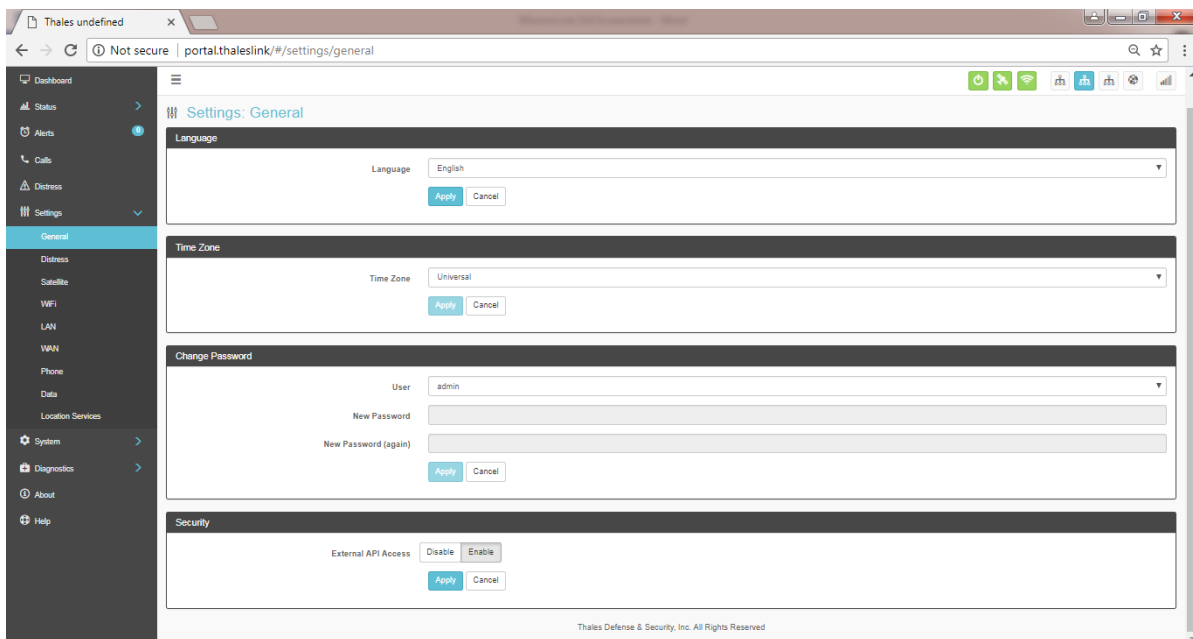
There are four access levels to the system. Three of them are under password control. The passwords are managed in the Change Password section:

- GUEST: User only account, no password, read only access
- WAN USER: Password capability, read only access to some API data remotely via WAN port or over the Iridium network.
- WAN ADMIN: Password capability, FULL access to all data and settings remotely via WAN port or over the Iridium network.
- ADMIN: Password capability, FULL access through the Thales Management Portal via local LAN (or wireless) connection.



### NOTE

It is always recommended that passwords be changed from defaults for added protection and security.



*Figure 3-20 Settings → General Screen*

*Table 3-3 Settings → General Settings*




Section	Parameters
Language	Select either <b>English</b> , French, German, or Spanish. ( <b>English</b> is the default setting)
Time Zone	Select the desired time zone setting from the drop down menu. ( <b>Universal</b> is the default setting)
Change Password	<ul style="list-style-type: none"> <li>Select User, Currently there are 3 choices (Admin, WAN_Admin, and WAN_User)</li> <li>Enter NEW Password and confirm the new password</li> </ul>
Security	Enable / Disable the external API Access. ( <b>Enable</b> is the default setting)

## Distress



### NOTE

Distress calls can only be configured by the administrator. If the user is not logged in as ADMIN and selects MANAGE DISTRESS, the user will see this  icon, indicating this function is not available. Login in as the ADMIN to continue.

On the Distress page, the admin can set up a Distress message. Select EMAIL from the pull down list (Figure 3-21). Enter the required information shown in Table 3-4 (example data shown in Figure 3-22) along with the message to be sent and select APPLY. NOTE: Selecting APPLY does not send a distress message. It saves the settings and message. Sending the distress message is done through the “Distress” menu item.

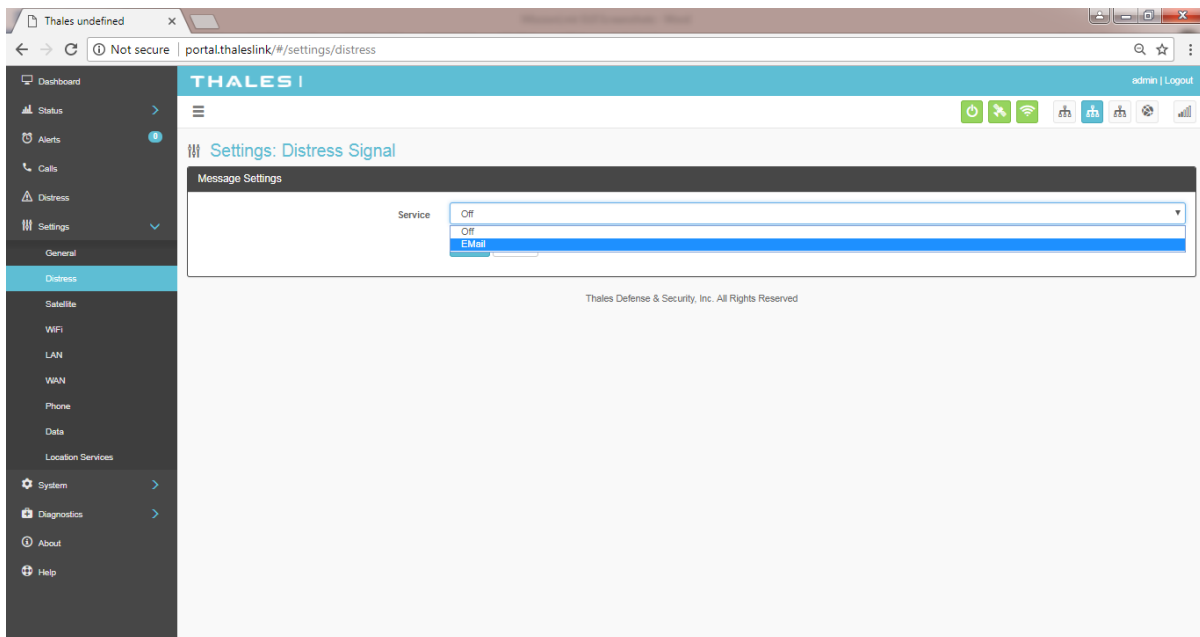


Figure 3-21 Settings → Distress (Initial Screen)

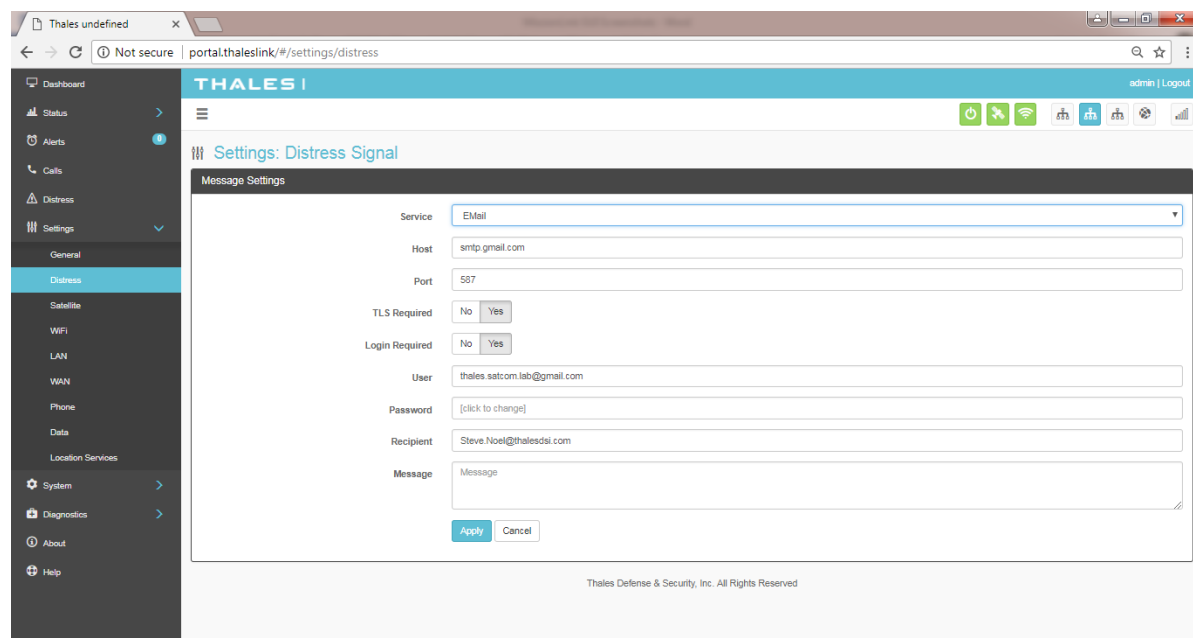









Figure 3-22 Settings → Distress

Table 3-4 Settings → Distress

Section	Parameters
Service	Select either Email or OFF (OFF is the default settings)
Host	Enter the host name (example: smtp.gmail.com)
Port	Enter the port number (example: 587)
TLS Required	Select either <b>YES</b> or NO (Default setting is YES)
Login Required	Select either <b>YES</b> or NO (Default setting is YES)
User	Enter the user email address
Password	Enter the user name password
Recipient	Enter the recipient's email address
Message	Enter the Distress message to be sent.

## Satellite

The Satellite page, shown in Figure 3-23, allows configuration of the data service. The configuration includes configuring whitelists and blacklists for domains, configuring port blocking and port whitelists, setting data limits for information purposes, and enabling and disabling network compression.

When adding a Domain to a Black/Whitelist it is always necessary to first select the  button BEFORE selecting the  button. After selecting the  button, the domain can always be edited or deleted using the   buttons BEFORE selecting the  button to save. If the  button is not selected before leaving the Satellite menu item, the data will not be saved.

The screenshot shows the THALES portal interface for configuring satellite settings. The browser address bar indicates the URL is `portal.thaleslink/#/settings/satellite`. The left sidebar contains navigation options: Dashboard, Status, Alerts, Calls, Distress, Settings (selected), General, Distress, Satellite (selected), WiFi, LAN, WAN, Phone, Data, Location Services, System, Diagnostics, About, and Help.

The main content area is titled "Settings: Satellite" and contains four configuration sections:

- Domain Whitelist & Blacklist:**
  - Domain Blocking Mode: Off (selected), Blacklist, Whitelist
  - Blacklisted Domains: A table with columns "Domain" and "Actions". The "Domain" column has an input field, and the "Actions" column has a "+" button.
  - Whitelisted Domains: A table with columns "Domain" and "Actions". The "Domain" column has an input field, and the "Actions" column has a "+" button.
  - Buttons: Apply, Cancel
- Port Management:**
  - Port Blocking: Disabled (selected), Enabled
  - Port Whitelist: A table with columns "Starting Port", "Ending Port", "Protocol", and "Actions". The "Starting Port" and "Ending Port" columns have input fields. The "Protocol" column has a dropdown menu showing "TCP & UDP". The "Actions" column has a "+" button.
  - Buttons: Apply, Cancel
- Data Limits:**
  - System Limit: -1 (input field). Below it, text reads: "Data limit in kB (1000 bytes). 0 means no data permitted and -1 allows unlimited data."
  - Reset Day: 0 (input field). Below it, text reads: "Day of the month when usage should be reset. 0 means no reset."
  - Buttons: Apply, Cancel
- Satellite Configuration:**
  - TCP PEP: Disabled (selected), Enabled
  - Header Compression: Disabled (selected), Enabled
  - Payload Compression: Disabled (selected), Enabled
  - Buttons: Apply, Cancel

At the bottom of the page, the text "Thales Defense & Security, Inc. All Rights Reserved" is displayed.

Figure 3-23 Settings → Satellite Screen

Table 3-5 Settings → Satellite

Section	Value
<b>Domain Whitelist &amp; Black List</b>	
Domain Blocking Mode	<b>OFF</b> / Blacklist / Whitelist (OFF is the default setting)
Blacklisting	Enabling <u>allows ALL</u> websites EXCEPT those listed (very little restriction)
Whitelisting	Enabling <u>blocks ALL</u> websites EXCEPT those listed (the most restriction)
<b>Port Management</b>	
Port Blocking	<b>Disabled</b> / Enabled (Disabled is the default setting)
Port Whitelist	Enter the Starting Port and Ending Port number.
	Select the applicable protocol ( <b>TCP &amp; UDP</b> or TCP only or UDP only) (TCP & UDP is the default setting)
<b>Data Limits</b>	
System Limit	Data limit in kB (1000 bytes), 0 means no data and -1 means unlimited data. Setting data limits is for information purposes only. No data restrictions will occur by setting limits.
Reset Day	Enter the day of the month when usage should be reset, 0 means no reset
<b>Satellite Configuration</b>	
TCP PEP	Disabled / <b>Enabled</b> (Default setting is ENABLED)*
Header Compression	Disabled / <b>Enabled</b> (Default setting is ENABLED)*
Payload Compression	Disabled / <b>Enabled</b> (Default setting is ENABLED)*
	*NOTE: Compression enabled to increase throughput but could be a problem for some less common and older devices



## NOTE

Setting data limits is for information purposes only. Data will not be restricted if the limit is reached or exceeded. An alert will be generated saying that the limit has been reached.

## Wi-Fi

The Wi-Fi page shown in Figure 3-24 allows setup of the Wi-Fi service.

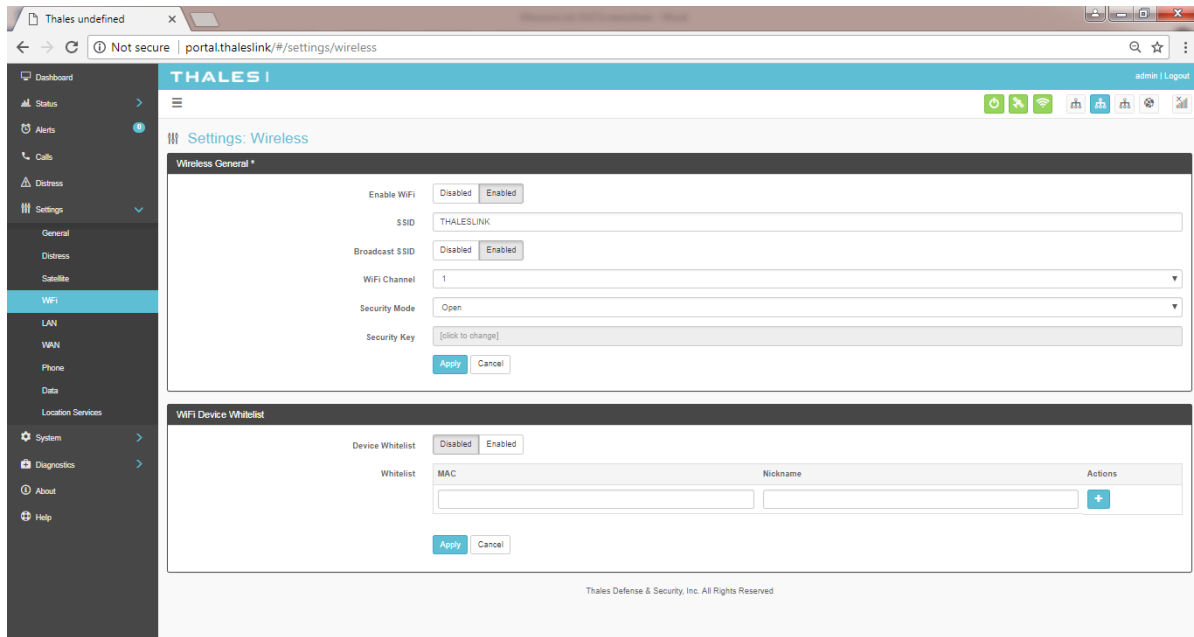


Figure 3-24 Settings → Wi-Fi Screen

Table 3-6 Settings → Wi-Fi

Section	Value
<b>Wireless General</b>	
Enable Wi-Fi	Disabled / <b>Enabled</b> (Enabled is the default setting)
SSID	Enter the name of the SSID. THALES LINK is default.
Broadcast SSID	Disabled / <b>Enabled</b> (Enabled is the default setting)
Wi-Fi Channel	Set the Wi-Fi Channel 1 – 11
Security Mode	Set the security mode for the channel – OPEN or WPA2. OPEN is default and does not require a Security Key (password).
Security Key	When WPA2 is selected as the security mode, a security key must be entered. It can be any length and any combination of characters, numbers, etc. Once enabled, any device accessing the ThalesLINK Wi-Fi will have to enter the password.
Device Whitelist	<b>Disabled</b> / Enabled (Disabled is the default setting)
Whitelist	This allows specific devices to access the system's Wi-Fi. If Enabled, only the devices entered in the Whitelist are allowed on the Wi-Fi network. This is done by entering the MAC address of the device (example: 01:23:45:67:89:ab). All others are prevented from accessing it. See below note for finding a device's MAC address
	Assign a Nickname to the MAC Address

**NOTE**

Once the initial Wi-Fi WPA2 Security Key is entered, it can be changed at any time by just overwriting the current Security Key in the Settings → Wi-Fi → Wireless General area.

**NOTE**


To identify a device's MAC address for whitelisting, you should be able to find it in your device's Settings menu. Sometimes it is called the Wi-Fi Address. If it can't be found, a simple way is that while the Device Whitelist is **DISABLED**, connect the device to be whitelisted to the Wi-Fi system by selecting the correct Wi-Fi Network (SSID) and typing in the Security Code if WPA2 is enabled. Once connected, go to Status → Current Devices menu item and find the device Hostname in the list of Allocated IPs. The MAC address will be in the left column.



## LAN



### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

The LAN page, shown in Figure 3-25, allows POE to be enabled or disabled on the three LAN ports and DHCP to be enabled and configured or disabled. See Table 3-7 for more information on the information that is entered.

Figure 3-25 Settings → LAN Screen

Table 3-7 Settings → LAN


Section	Value
<b>POE</b>	
Enable PoE 1	Disabled / <b>Enabled</b> (Enabled is the default setting)
Enable PoE 2	Disabled / <b>Enabled</b> (Enabled is the default setting)
Enable PoE 3	Disabled / <b>Enabled</b> (Enabled is the default setting)
<b>DHCP</b>	
Enable DHCP	Disabled / <b>Enabled</b> (Enabled is the default setting)
IP Address	Enter the IP Address
Mask	Enter the Mask Number
Start	Enter the starting value for the octet
End	Enter the ending value for the octet
Lease Time	Enter the Lease Time being allotted (in seconds)

Section	Value
<b>DHCP Reservations</b>	
Name	Enter the name of the DHCP Reservation
Duration	Enter the length of time (in seconds)
MAC	Enter the MAC address
Address	Enter the last digits of the IP Address
Enabled/Disabled	Disabled / <b>Enabled</b> (Enabled is the default setting)








## WAN



### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

The WAN page, shown in Figure 3-25, allows configuration of the WAN data service. The settings include configuring whitelists and blacklists for domains, configuring port blocking and port whitelists.

When adding a Domain to a Black/Whitelist it is always necessary to first select the  button BEFORE selecting the  button. After selecting the  button, the domain can always be edited or deleted using the   buttons BEFORE selecting the  button to save. If the  button is not selected before leaving the WAN menu item, the data will not be saved.

Additional details about these settings are described in Table 3-8.

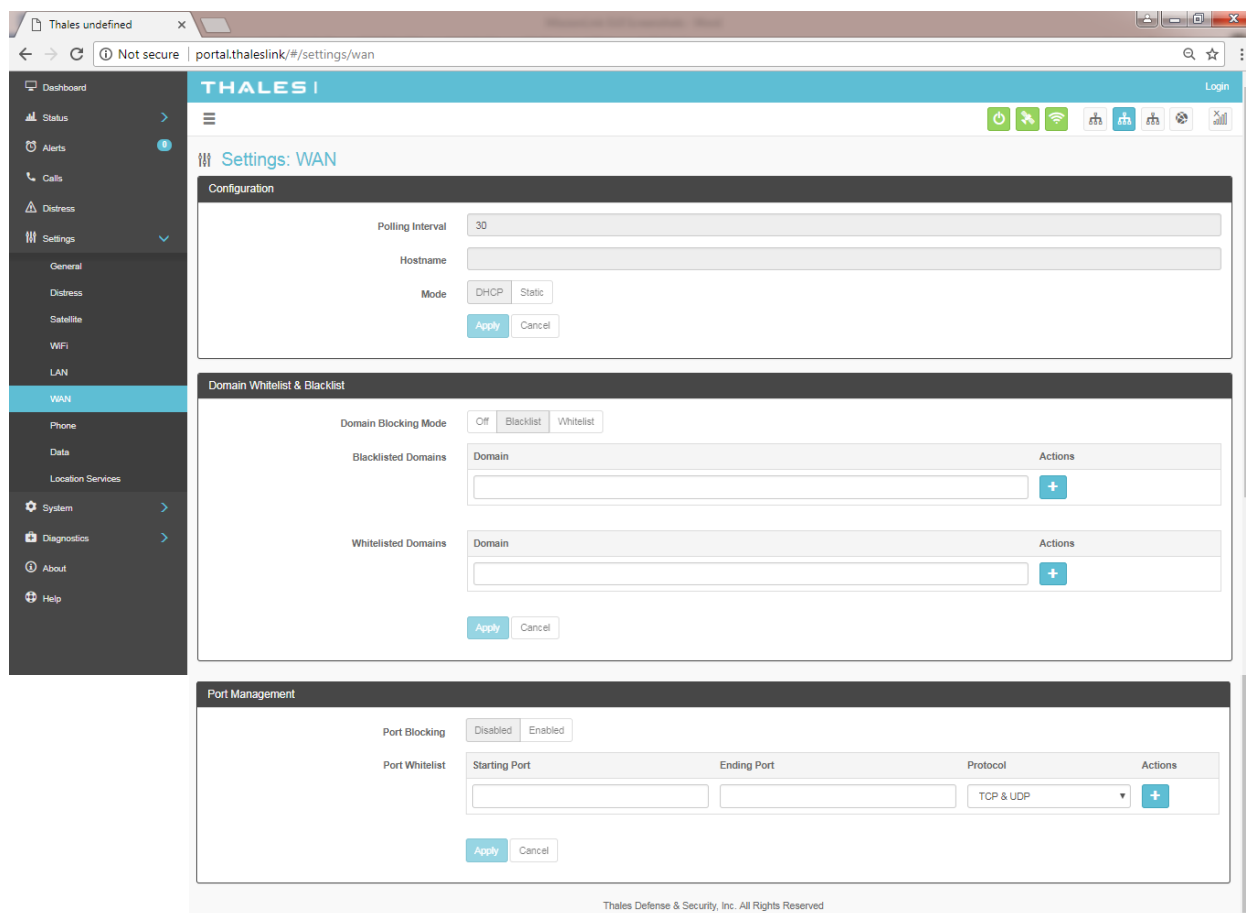


Figure 3-26 Settings → WAN Screen


Table 3-8 Settings → WAN

Section	Value
<b>Configuration Management</b>	
Polling Interval	
Hostname	
Mode	<b>DHCP</b> or <b>STATIC</b> (DHCP is the default setting)
<b>Domain Whitelist &amp; Black List</b>	
Domain Blocking Mode	<b>OFF</b> / Blacklist / Whitelist (OFF is the default setting)
Blacklisting	Enabling <u>allows ALL</u> websites EXCEPT those listed (very little restriction)
Whitelisting	Enabling <u>blocks ALL</u> websites EXCEPT those listed (the most restriction)
<b>Port Management</b>	
Port Blocking	<b>Disabled</b> / Enabled (Disabled is the default setting)
Port Whitelist	Enter the Starting Port and Ending Port number.
	Select the applicable protocol ( <b>TCP &amp; UDP</b> or TCP only or UDP only) (TCP & UDP is the default setting)

## Phone



### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

The Phone Settings page, shown in Figure 3-28, allows configuration of phone extensions and mapping of those extensions to the outbound Iridium phone lines as well as which extension rings for each inbound Iridium line. Each extension can be mapped to one, two, three or none of the Iridium phone lines for outbound calls by checking the box next to the corresponding Line in the Outbound Lines column. By selecting the “pencil” icon, a password can be entered for each extension if desired. An extension can be deleted by selecting the “trashcan” icon. All changes are saved only after the APPLY button is selected.

Each of the three Iridium phone lines (Inbound) can be mapped to ring only one extension. The extension is selected from the pull-down menu. Configuration of analog devices such as the POTS phones and the Radio Gateway are configured on this page. Each of these devices can be mapped to an extension.

Finally, in the Phone Configuration area, call logs can be enabled or disabled and the POTS phone impedance can be selected for optimal performance.










When adding an extension, it is always necessary to first select the  button BEFORE selecting the  button. Several extensions can be added by selecting the  button multiple times, and then selecting the  button. After selecting the  button, the extension can always be edited or deleted selecting the   buttons BEFORE selecting the  button to save. If the  button is not selected before leaving the Phone menu item, the data will not be saved.

Table 3-9 describes the settings in more detail.

Thales Defense & Security, Inc. All Rights Reserved

Figure 3-27 Settings → Phone Screen


Table 3-9 Settings → Phone

Section	Value
<b>Extension Mapping</b>	
1-88888	Phone extensions are set up here and mapped to out bound Iridium phone lines. Extension numbers cannot begin with 0 or 9.
1001-1003	Default extensions that map to the three Iridium phone lines. The default has each extension mapping to all three outbound Iridium lines.
<b>Inbound Iridium Lines</b>	
1-88888	Maps each inbound Iridium line to a single extension previously set up.
1001 - 1003	Default extensions 1001, 1002 and 1003 are mapped to Line 1, Line 2 and Line 3 respectively
<b>Device Mapping</b>	
POTS	Assigns extensions to POTS 1 and POTS 2 phones
Radio GW	Assigns extension to the Radio Gateway
<b>Phone Configuration</b>	
Enable Call Log	Disabled / <b>Enabled</b> (Enabled is the default setting). Call logs display Active Calls and Call History when the Calls menu item is selected.
POTS Impedance	Sets the dynamic output of the POTS system to match regional Phone types ( <b>USA</b> , Australia, Europe, UK, USA-Loaded) (USA is the default setting)

## Data



### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

From the Data page, shown in Figure 3-28, data is enabled or disabled and the routing is configured. The data can be configured to always go through the Iridium satellite system, always go through the WAN port or go through both, depending on availability of the WAN network.

- For the automatic data routing feature, the WAN network takes precedence over the Iridium satellite network.
- When the Data Route is set to ANY, and with a WAN device attached (i.e. cellular modem), the system automatically switches to the WAN attached network when signal is available. The system will ping the internet to determine if the WAN device is in range, and if so switches the data path from Satellite to WAN. If the signal drops out, the data path switches back to Satellite.
- Selecting ANY will cause all data to go through the Iridium satellite network if no WAN device is attached or if the WAN device is not powered.



## NOTE

The WAN port does not have Power of Ethernet (PoE) capability, so any device plugged into the WAN port needs to provide its own power source. The TU does not provide power.



## NOTE

The automatic data routing feature does not apply to voice calls. All voice calls are routed through the Iridium satellite system 100% of the time. The WAN port is only for data.

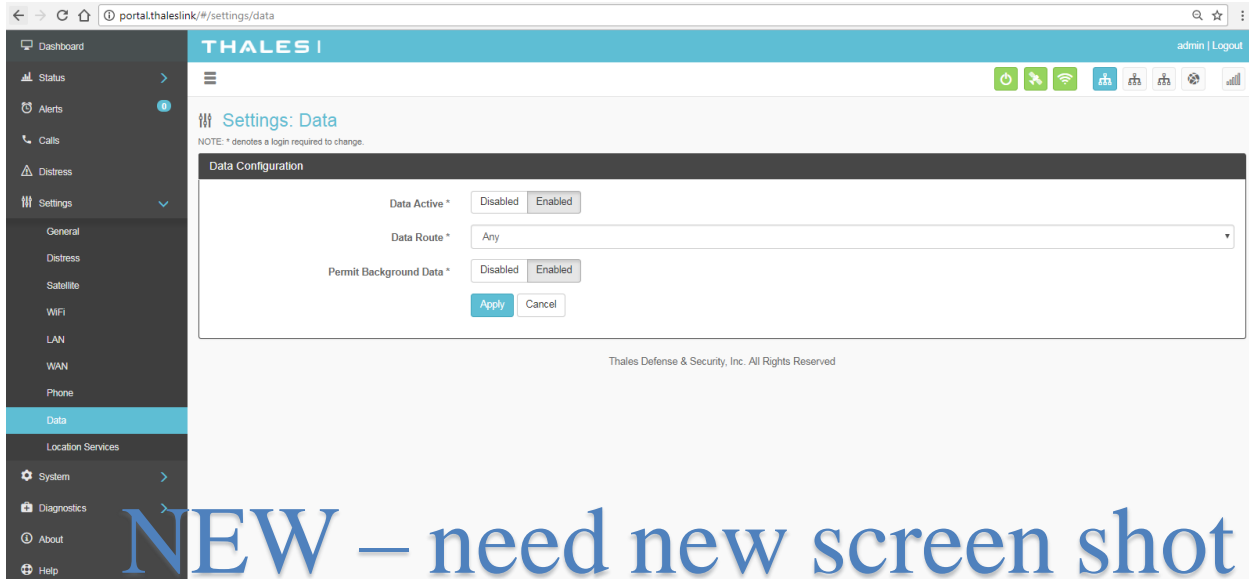


Figure 3-28 Settings → Data Screen

Table 3-10 Settings → Data

Section	Value
<b>Data Configuration</b>	
Data Active	Disabled / <b>Enabled</b> (Enabled is the default setting)
Data Route	Select the desired data route ( <b>Any</b> , Satellite, or WAN Port) ( <b>Any</b> is the default setting). The automatic data routing feature requires <b>Any</b> be set.
Permit Background Data	Disabled / <b>Enabled</b> (Enabled is the default setting). If Enabled, this setting allows for GPS location information to be transmitted even when data is disabled. This is valuable if location services are being used.
Disable Data on Boot	<b>NO</b> / YES ( <b>NO</b> is the default setting). Determines the default data operations state when the system is restarted.





## NOTE

Since the system default for “Satellite Data Sessions” is OFF, the “Disable Data on Boot” configuration has been added so that when the system is turned off and on frequently, it comes up in a known state each time for data. This allows the unit to start up with data sessions turned on each time or to be off.

## Location Services

From the Location Services page, shown in Figure 3-29, Location Services are enabled and disabled and the settings are configured (when enabled). Thales offers ClearSIGHT as the preferred tracking service. This requires an account and service subscription. More information can be found at [www.clrSight.com](http://www.clrSight.com).

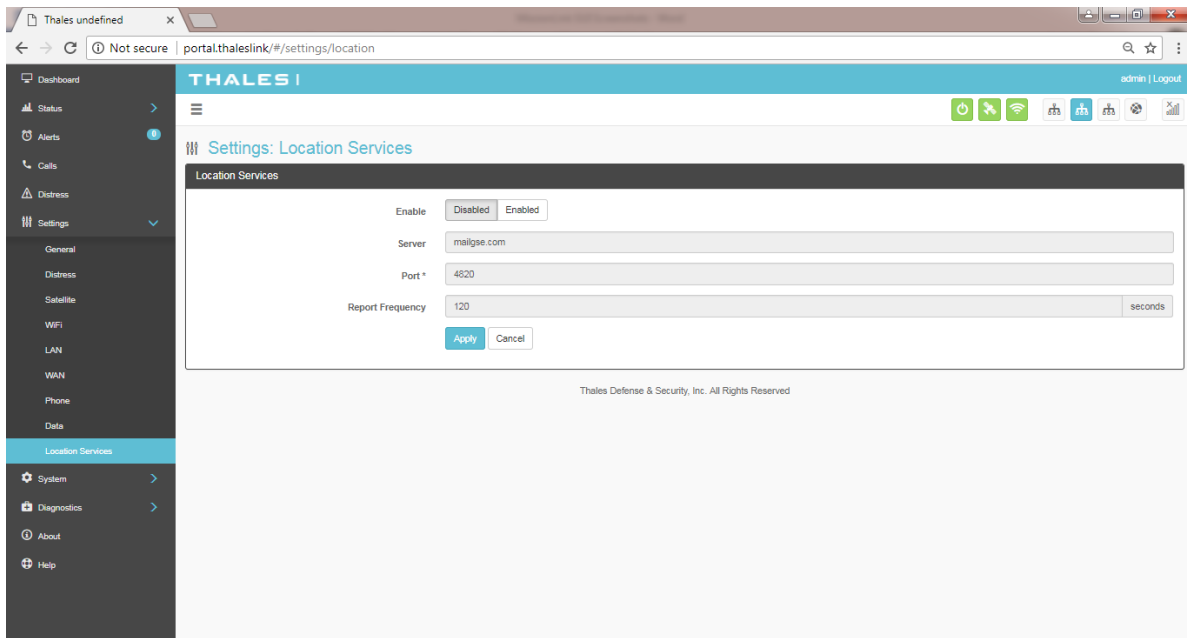


Figure 3-29 Settings → Location Services Screen

Table 3-11 Settings → Location Services

Section	Value
<b>Data Configuration</b>	
Enable	<b>Disabled</b> / Enabled (Disabled is the default setting)
Server	Enter the name of server. Get this information from <a href="http://www.clrSight.com">www.clrSight.com</a>
Port	Enter the port number of the service from <a href="http://www.clrSight.com">www.clrSight.com</a>
Report Frequency	Default setting is 120 seconds. When DISTRESS is set to enabled, frequency will be every 5 minutes.


## System

The System menu item allows for backing up a configuration and restoring it, monitoring of system data usage (unofficial), performing a system reboot, restoring factory default settings, and provides information on the system firmware versions.

### Backup



#### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

Refer to Figure 3-30. Before performing a firmware update, replace a TU, cloning information for multiple systems or just as good practice periodically, the system configuration file should be backed up to prevent loss of custom configuration settings in the event that an issue should occur. Backup can occur on devices that have a file system where the configuration file can be downloaded and saved (personal computer, laptop, Android). Backing up the current configuration is a simple process detailed below.

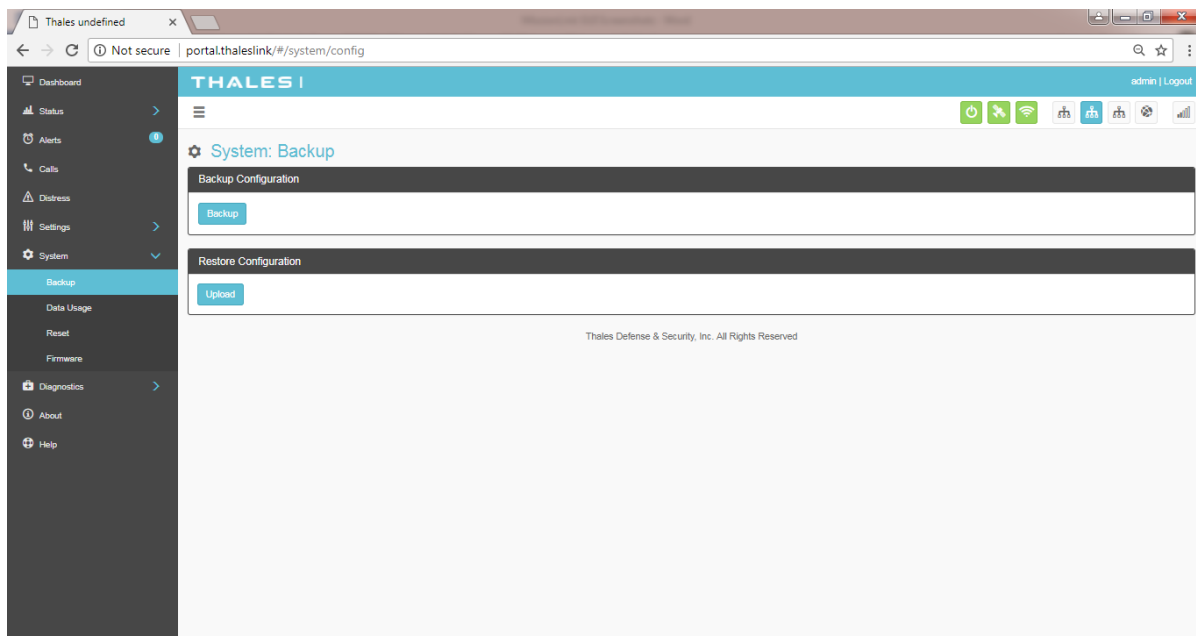


Figure 3-30 System → Backup Screen


- Backup Configuration
    - Connect a computer to the TU either through Ethernet or Wi-Fi
    - Select BACKUP, will automatically backup the data contained in the Management Portal.
    - The backup file can be renamed as long as the file extension is “.json”
- NOTE: This is very useful for restoring setting to a replacement unit or cloning setup for multi-unit fleet service

- Restore Configuration
  - In the event the configuration file needs to be reloaded, RESTORE CONFIGURATION will enable you to reload a previous saved configuration file.
  - Select RESTORE CONFIGURATION
  - Navigate to the file that was saved.
  - Open the file to Upload

## Data Usage



### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

Refer to Figure 3-31. Data usage is shown for information purposes only. If there is a data limit set, that is shown as well. The system data usage can be reset to restart the data count. Select RESET and then YES, RESET to confirm. Otherwise, select NO, CANCEL.



### NOTE

This is an estimate of data used and does not accurately represent the billable data total. It also does not limit or restrict data usage even if the Data Usage exceeds the Data Cap. To get accurate data usage, please contact your service provider.

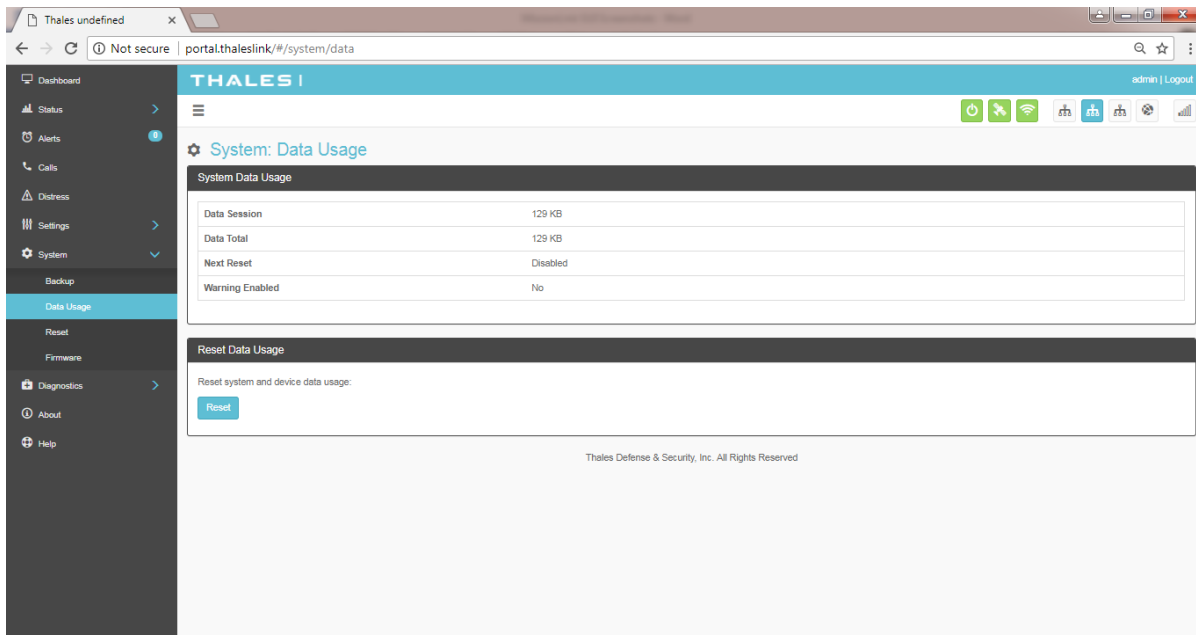



Figure 3-31 System → Data Usage Screen

## Reset



### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

Refer to Figure 3-32. In the event the system is not responding correctly, a system reboot can be performed. Select REBOOT to restart the system.

If there is a larger issue such as a corruption or if configuration settings have made the system non-operational, a Factory Reset can be performed. Select FACTORY RESET. This resets all the configuration settings to the default settings.

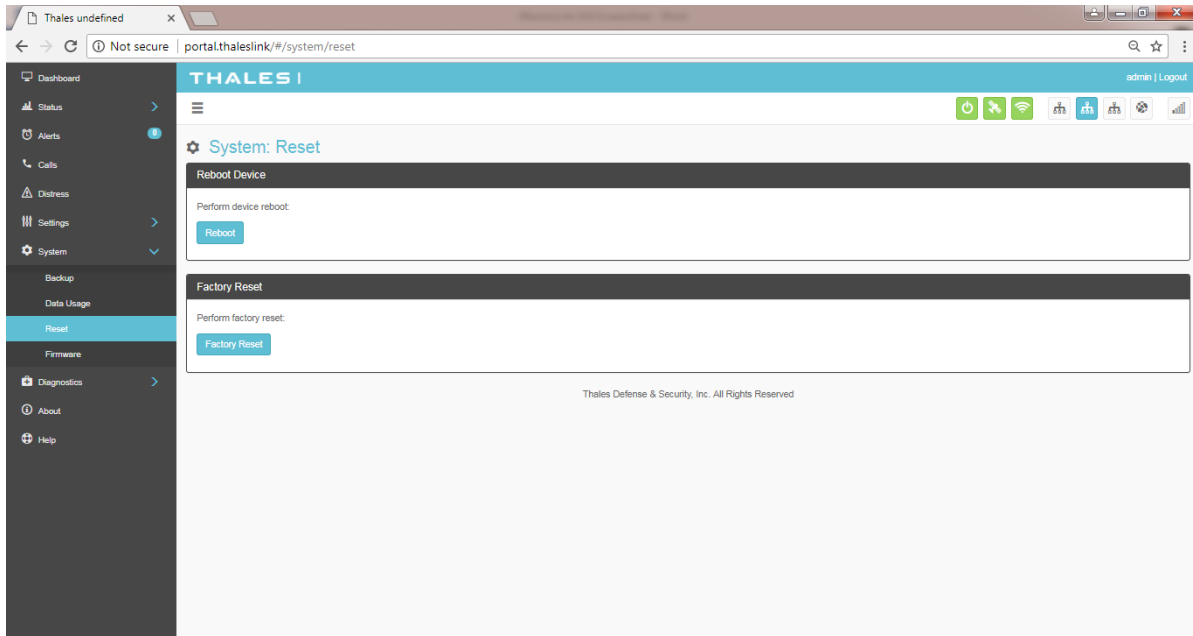


Figure 3-32 System → RESET

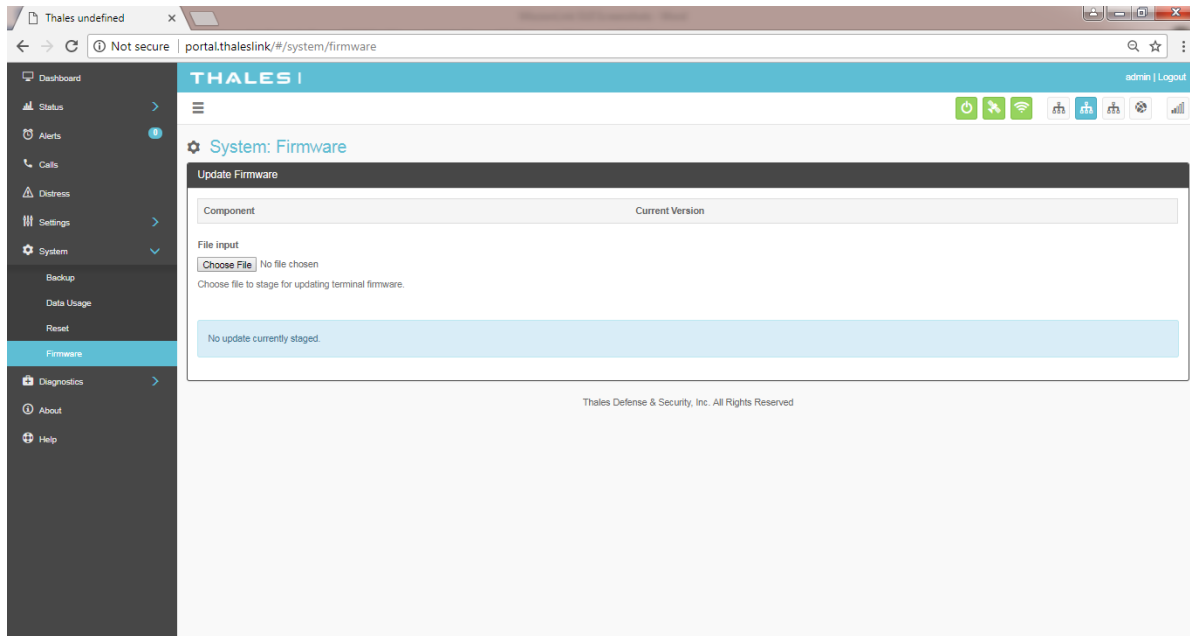


### NOTE

Factory Rest will restore factory defaults and all users' customized settings will be lost.

## Firmware

Refer to Figure 3-33. The Firmware page displays the current firmware version numbers. These may be helpful if customer service is contacted to resolve an issue.



*Figure 3-33 System → Firmware Screen*



### NOTE


For detailed instructions on updating Firmware on the TU please reference chapter 5 of this manual.

## Diagnostics

### Self-Test



#### NOTE

This is an ADMIN functional only. If the user sees this  icon, login as the ADMIN to continue. Otherwise this is a view only screen.

The Self-Test diagnostics page, users will be able to run a diagnostic test of the system and results will be available in the diagnostic logs page for debug.

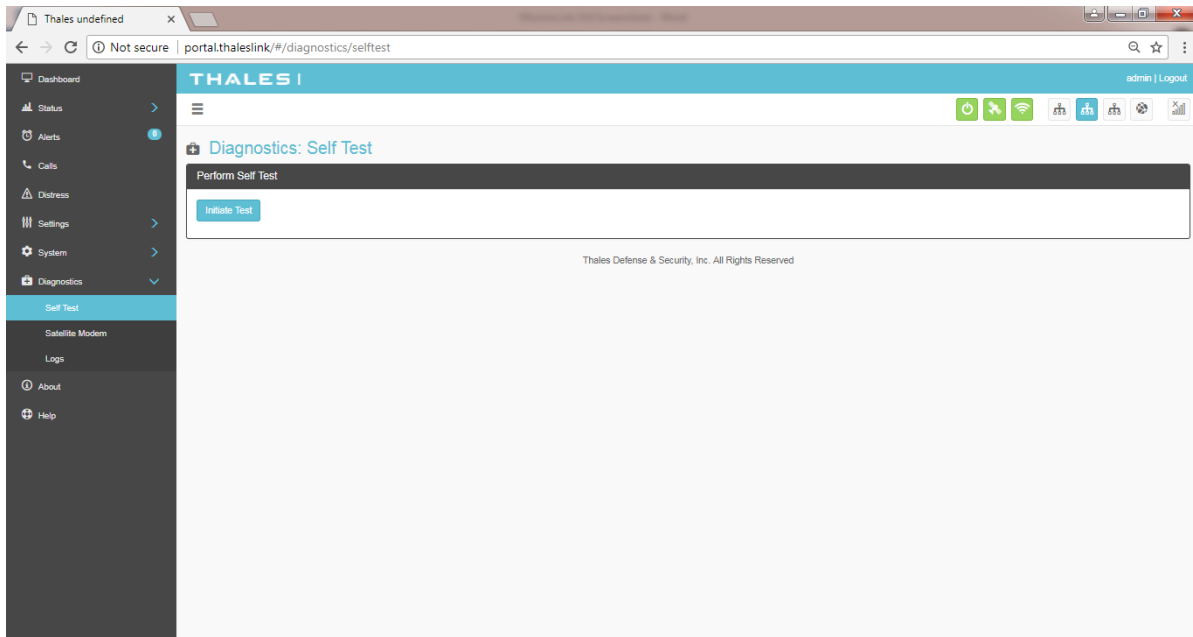


Figure 3-34 Diagnostics → Self-Test Screen

Refer to Figure 3-35. Select INITIATE TEST and then confirm by selecting YES, TEST to perform the self-diagnostics test.



Figure 3-35 Perform Self-Test Confirmation

**NOTE**

Once the Self-Test is complete, a pop-up screen will appear indicating that the Self-Test is complete, and to check the logs for details.

## Satellite Modem

**NOTE**

This is a view only page.

The Satellite Modem diagnostics page provides information that will aide in the debugging of the system.

The Satellite Modem page is divided into the following sections as shown in Figure 3-35:

- System Status
- Constellation Status
- Static Config
- System Diagnostics

Thales undefined

portal.thaleslink/#/diagnostics/modem

admin | Logout

Dashboard

Status

Alerts

Calls

Distress

Settings

System

Diagnostics

Self Test

Satellite Modem

Logs

About

Help

THALES I

Diagnostics: Satellite Modem

System Status

L Band Frame

1301904015

EBBS LL Access Denial Cause

0000: NONE

EBBS LL Connection State

idle

SBD LL Access Denial Cause

0000: NONE

SBD LL Connection State

idle

TMSI Valid

true

Up Time

20255

Connection Bandwidth Status

Download Bitrate

0

Download Carriers

0

Upload Bitrate

0

Upload Carriers

0

Modmod

DEQPSK

GPS Location

Fix

true

Altitude

197

Latitude

39.2293

Longitude

-77.279583

Space Vehicle Constellation Status

Time

1510980344.66

L Band Frame Number

1301987909

Space Vehicles

Space Vehicle ID	X km	Y km	Z km	XYZ Age	EBBS Enabled						
82	1544	-6224	3000	129	false						
	Beam ID	ACQ Classes	ACQ Classes Age	BCCH Slot	BCCH SubBand	SV Blocking	SV Blocking Age	X km	Y k	Z km	XYZ Age
	1	65535	32	5	7	false	32	1536	-4812	3880	80
80	-132	-5912	4020	12	false						
	Beam ID	ACQ Classes	ACQ Classes Age	BCCH Slot	BCCH SubBand	SV Blocking	SV Blocking Age	X km	Y k	Z km	XYZ Age
	23	65535	316	2	9	false	316	1088	-4724	4128	59
	23	65535	316	2	9	false	316	1088	-4724	4128	59
	40	0	286	5	13	false	286	852	-5180	3600	93
	40	0	286	5	13	false	286	852	-5180	3600	93
	28	65535	356	2	21	false	356	592	-4900	4072	74
	28	65535	356	2	21	false	356	592	-4900	4072	74
93	3828	-3624	4828	7	false						
	Beam ID	ACQ Classes	ACQ Classes Age	BCCH Slot	BCCH SubBand	SV Blocking	SV Blocking Age	X km	Y k	Z km	XYZ Age
	38	65535	356	5	21	false	356	2300	-4292	4104	54
	38	65535	356	5	21	false	356	2300	-4292	4104	54
	38	65535	356	5	21	false	356	2300	-4292	4104	54
	34	0	274	5	15	false	274	2176	-4128	4336	81
	34	0	274	5	15	false	274	2176	-4128	4336	81
	34	0	274	5	15	false	274	2176	-4128	4336	81

Static Config

Frequency Reference

Internal

Permit Antennaless

false

Permit Software Upgrade

true

RF Cable Loss

80

TX Ind Lag Time

10

TX Ind Lead Time

10

System Diagnostics

IMEI

300008080004130

IMSI

901037050000313

MAC Address

74da:aa:3c:c2:13

Component	Hardware Version	Software Version	Serial #
5042-PCB-01	REV B/C		
BCX			IRD0000ST
BuildSystem		Job #855319	
CS		CX 1.5.8-1985	
DSP		v7.12.12377 (Release) (#988255)	
DSP IBL		CCL P1387 (IBL Version 5.0.11210) (Release) (#751030) DSP Clk speed:850MHz HW support:PCIETH	
FPGA		HW: Dv1387 SW: Dv2000	

Thales Defense & Security, Inc. All Rights Reserved

Figure 3-36 Diagnostics → Satellite Modem Screen

3-38

User Manual PN 84468 Rev 1



## Diagnostics Logs

Refer to Figure 3-37. The Diagnostics Logs provide the operator with the results of all recent diagnostic tests. This information can be used in debugging / troubleshooting the system.

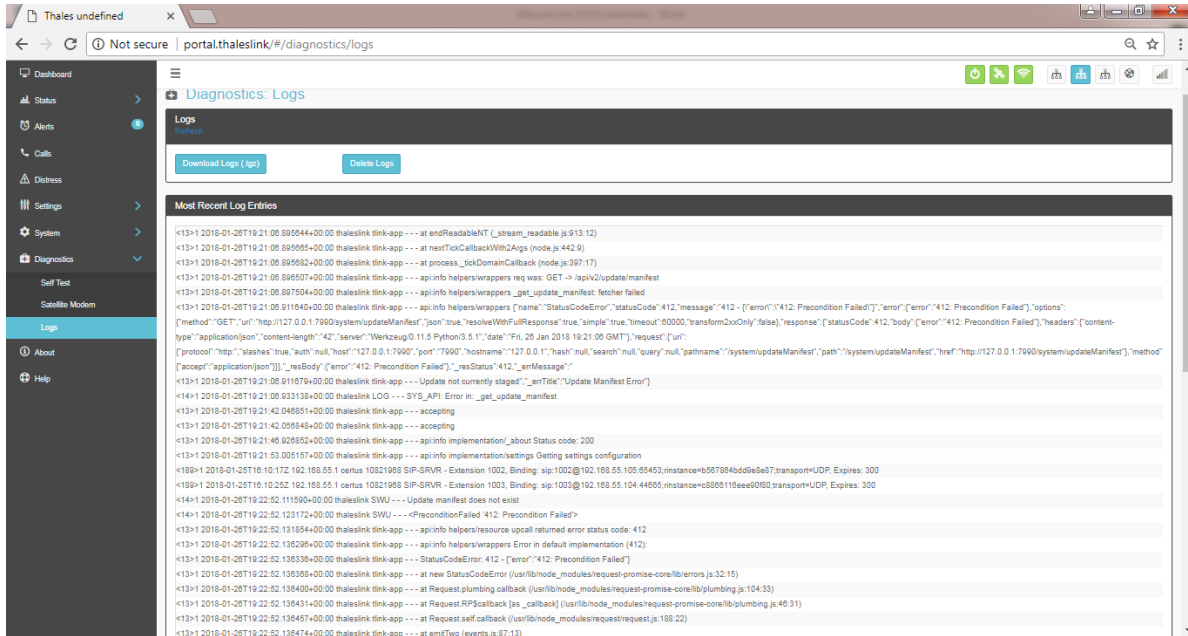


Figure 3-37 Diagnostics → Logs Screen



### NOTE

The “Most Recent Log Entries” only shows the last 100 log entries. For additional information, select **DOWNLOAD LOGS** (.tgz) for additional information.

## About

Refer to Figure 3-38. This page provides detailed information relating to the equipment, including unique HW information and its current software version.

This includes,

- Antenna
- Satellite Modem
- Power Supply
- System
- VOIP Module
- Wi-Fi

The screenshot displays the 'About' page of the Thales portal.thaleslink/#/about interface. The page features a sidebar menu on the left with options: Dashboard, Status, Alerts, Calls, Distress, Settings, System, Diagnostics, About (selected), and Help. The main content area is titled 'THALES |' and contains several sections of system information:

- Antenna**

Software Version	34
Hardware Version	3
Antenna Type	H2
Model	4
Serial #	81700411
- Satellite modem**

Software Version	CX 1.5.8-1055
Hardware Version	5042-PCB-01 REV B/C
Serial #	IRD0005T
IMEI	30000800004130
- Power Supply**

Software Version	17
------------------	----
- System**

Software Version	d0.0.21.251038
• Application	00.00.21.0001-r1
• OS	4.1.35-fsic+gfeb20fb
• Portal	24
Hardware Version	5
Model	
Serial #	
Info	
System MAC Address	18:39:19:00:00:04
- VOIP Module**

Software Version	0.1.x.20180119
Hardware Version	5.2.x
Serial #	InvalidSerialNo
LAN MAC Address	18:39:19:00:00:04
WAN MAC Address	18:39:19:40:05:8E
- WIFI**

Software Version	1.4.0.55357
Hardware Version	5
WIFI MAC Address	88:8B:0F:05:CE:54

At the bottom of the page, the text 'Thales Defense & Security, Inc. All Rights Reserved' is visible.

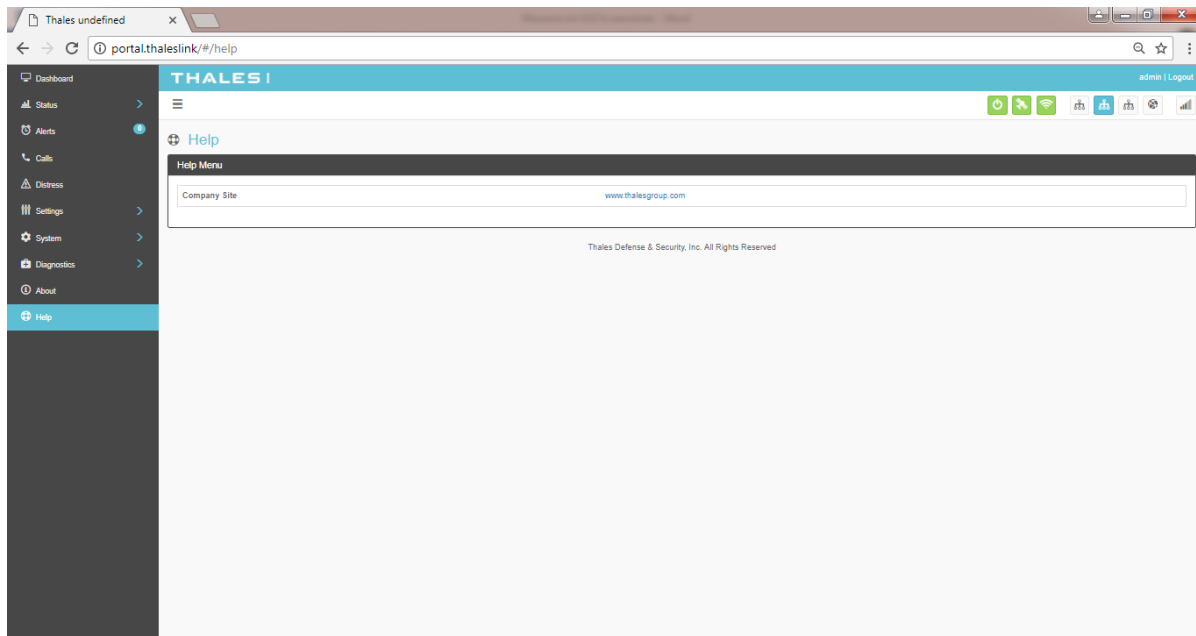
Figure 3-38 About Screen

## Help

This Help page, shown in Figure 3-39, provides access to all manuals and links to customer support.

This section includes:

- User Manual
- Installation Manual
- Quick Reference Guide
- Links to customer support



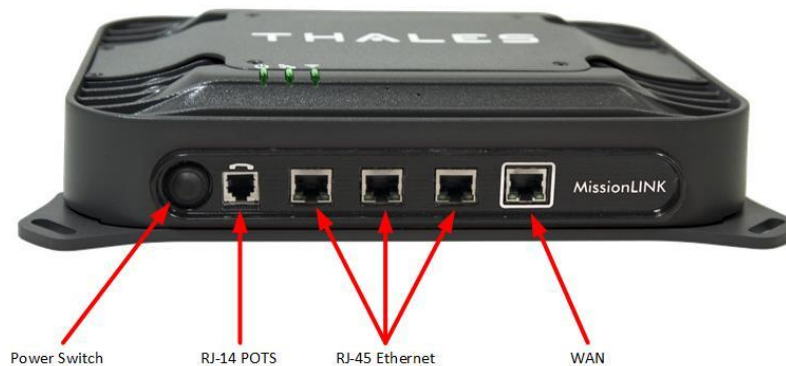
*Figure 3-39 Help Screen*

## CHAPTER 4 GETTING STARTED

### GETTING STARTED

#### **STEP 1: Connect Phone (standard POTS handset) or Ethernet VOIP Phone to Terminal Unit (TU).**

The TU front has a main power switch, one RJ-14 port for POTS (Plain Old Telephone Service), three PoE (Power over Ethernet) RJ-45 ports for VoIP phones or Computers, and one WAN (Wide Area Network) port. Refer to Figure 4-1 for location of ports.



*Figure 4-1 Terminal Unit Front Panel Detail*

#### POTS Phone connection

By default a POTS Phone can simply be plugged into the RJ-14 port using a standard phone cord (not provided) without any setup.

Up to 2 POTS Phones can be connected to the TU using a RJ-14 Splitter (not provided). Using a RJ-14 Splitter, the two POTS phones can each have a separate phone line (not two phones using the same phone line).

#### VoIP or Thales IP Phone connection

By default the TU has (3) lines preconfigured for use with the Thales IP handsets. If using a VoIP phone, Thales recommends CISCO SPA504G and Grand Stream GXP2140 models for ease of use with MissionLINK. Other brands and models may be supported but functionality cannot be guaranteed.

Follow your VoIP phone configuration guide to setup the VoIP phone and connect to the TU using the following parameters.

A typical VoIP phone configuration is shown below:

VoIP 1: (receives calls on line 1 of your SIM)	User: "1001" Password: "1001" Host: "sip.thaleslink" Protocol: udp or tcp
VoIP 2: (receives calls on line 2 of your SIM)	User: "1002" Password: "1002" Host: "sip.thaleslink" Protocol: udp or tcp
VoIP 3: (receives calls on line 3 of your SIM)	User: "1003" Password: "1003" Host: "sip.thaleslink" Protocol: udp or tcp

## STEP 2: Know your MissionLINK

It may be necessary to know details about your MissionLINK system when calling for help or service.

IMEI is unique to each unit and can be found on the bottom plate of the TU. This IMEI can also be found in the <http://portal.thaleslink> under the ABOUT tab.

IMSI is a unique identifier to each SIM card. This IMSI can also be found in the <http://portal.thaleslink> under the STATUS→ SIM tabs. (SIM must be inserted)

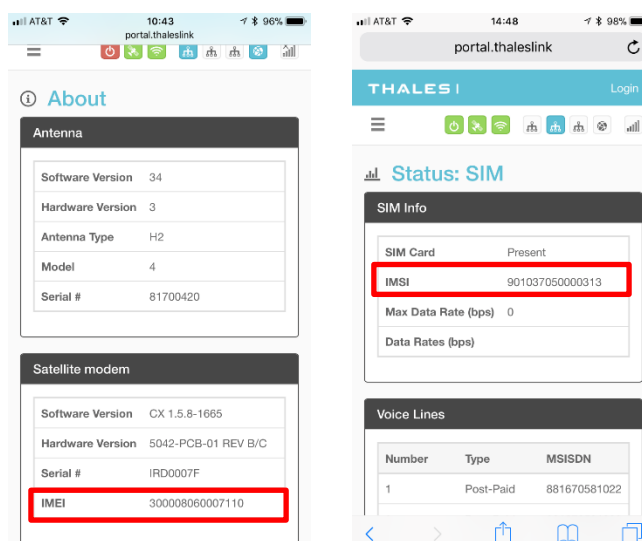
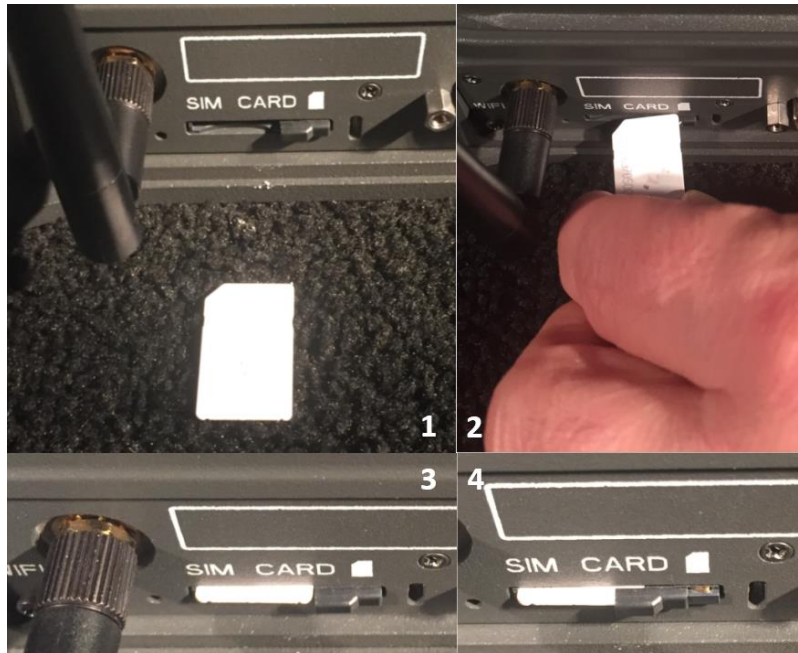


Figure 4-2 MissionLINK IMEI and IMSI from Mobile Device

## STEP 3: Install SIM

Install SIM card from Air-time provider as below. Insert card with contacts down as shown until it clicks into place. Be sure to engage the lock for the SIM Card



*Figure 4-3 Installing SIM Card and engaging the lock*




## STEP 4: Power the MissionLINK unit.

Press and release the power button on the TU. NOTE: After the button is pressed and released, a few seconds pass before the power LED (left) starts flashing. It may take a few minutes on initial startup for all 3 LED's on the unit top to turn solid **GREEN** or **BLUE**. You may see an occasional red LED during power up. This is normal as long as after it has fully booted, it stays green or turns blue. Refer to Table 4-1 for more information on the status LEDs.



*Figure 4-4 System, Satellite and Wi-Fi Status LED's*

Table 4-1 Terminal Unit LED Status

Indicator	Description
 <b>System</b>	
Solid GREEN	System functioning properly
Flashing GREEN	System busy (Booting up)
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)
 <b>Satellite</b>	
Solid BLUE	Connected and passing data (over satellite)
Solid GREEN	System functioning properly
Flashing GREEN	Acquiring satellite
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)
 <b>Wi-Fi</b>	
OFF	Wi-Fi OFF
Flashing GREEN	Wi-Fi busy
Solid Green	System functioning properly
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)

## STEP 5: Connect to MissionLINK portal to configure system.

Reference Figure 4-5. There are a couple options to login to the Management Portal.

### Option A: Via Wi-Fi.

1. Power on the MissionLINK TU and let it boot up (may take a couple minutes)
2. On the wireless device, find and select THALES LINK as an available Wi-Fi access point.
3. Open a browser and type: <http://portal.thaleslink> (do not type .com or any other extension)
4. The Management Portal appears in “guest” mode.
5. To make any changes, log in as an administrator by selecting LOGIN at the top of the window
6. When prompted, enter the default Username (admin) and Password (admin)
7. Immediately change the Password for added security (SETTINGS → GENERAL)

### Option B: Via (PC, Mac or Linux) Ethernet connection

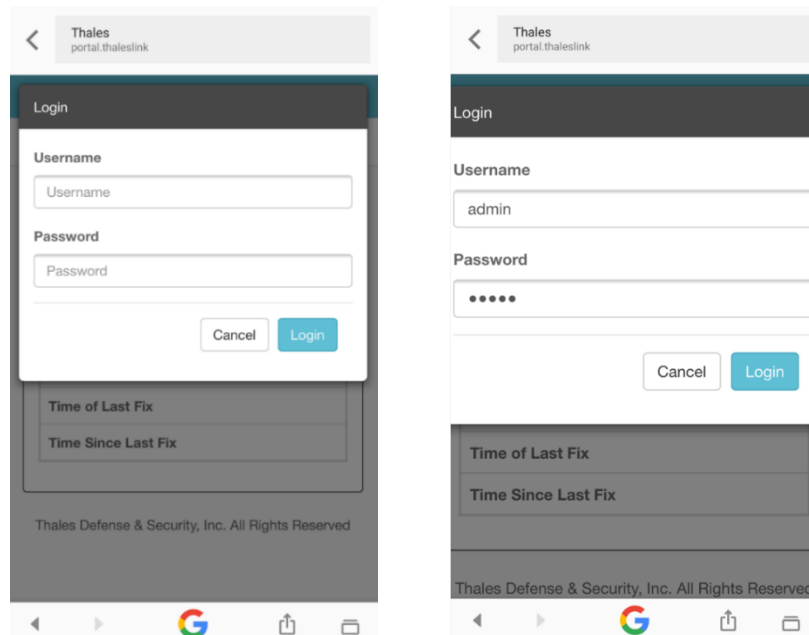
1. Power on the MissionLINK TU and let it boot up (may take a couple minutes)
2. Open a web browser
3. Type: <http://portal.thaleslink> (do not type .com or any other extension)
4. The Management Portal appears in “guest” mode.
5. To make changes, log in as an administrator by selecting LOGIN at the top of the window
6. When prompted, enter the default Username (admin) and Password (admin)

## 7. Immediately change the Password for added security (SETTINGS→GENERAL)



### NOTE

If you forget the password, press and hold the reset pin on the back of the box (while powered on) in order to reset the system to factory settings.



*Figure 4-5 MissionLINK User Interface Login*

### STEP 6: Place a phone call.

1. Lift the handset from the base and listen for a dial tone.
2. Call a known number to test call and voice clarity  
Dial Country code, area code and phone number #

**FOR EXAMPLE: (do not dial this number): 001-234-567-8900**



## **STEP 7: Access the Internet.**

Once your device has successfully connected to the TU, open the management portal <http://portal.thaleslink> to verify the satellite connection.

Verify:

- No active alerts (DASHBOARD or ALERTS page on the Management Portal)
- Satellites detected (go to STATUS → SERVICE), signal strength bars (top right of screen) should show more than 1 bar as available.

Try loading a small website such as [www.google.com](http://www.google.com) to verify your internet connection. If the page loads successfully you are ready to browse the internet.

## CHAPTER 5 FIRMWARE UPGRADE

On occasion it may be necessary to update MissionLINK software to add features or fix issues found in the software. This section will step through the process of those updates. Firmware updates are large files (75MB or more) and it is not recommended to do firmware updates over the Iridium satellite network. For best results use an external high speed internet connection. It is possible to use the WAN port on the MissionLINK if an LTE modem is connected and the network is available. The firmware file will contain updates for both the TU and the antenna if needed, so a single load automatically updates both. It is important to make sure the system is connected powered up and operational before attempting a firmware update. Do not remove power from the TU or remove the antenna connection while an update is in process. This may cause a corruption to occur and force a revert to the previous software version.



### NOTE

For SW reset or returning to factory defaults please refer to Chapter 6 → RESETS.

### DOWNLOADING THE FIRMWARE FROM THE THALES WEBSITE

**Connect via PC or Mobile device to the Internet.**

1. With a PC or laptop, connect to website [www.Thalesdsi.com/IRIDIUM](http://www.Thalesdsi.com/IRIDIUM) using a high speed internet connection
2. Go to THALESLINK Firmware Update link.
3. Enter required information such as the MissionLINK IMEI.



### NOTE

If downloading a firmware version for 700 kbps performance upgrade, addition information and payment verification may be required.

4. Download file to device and note its location on the computer



### NOTE

In order to complete the Firmware update, the user must be logged in as the ADMIN.

## INSTALLING THE FIRMWARE ON MISSIONLINK

### Via Computer or Mobile device.

1. With PC or Mobile Device connect to “THALES LINK” on Wi-Fi or via Ethernet (RJ-45) port.
2. Open a web browser and type: <http://portal.thaleslink> (do not type .com or any other extension)
3. Once prompted enter Username and Password.
4. Navigate to the SYSTEM → Firmware (Figure 5-1)

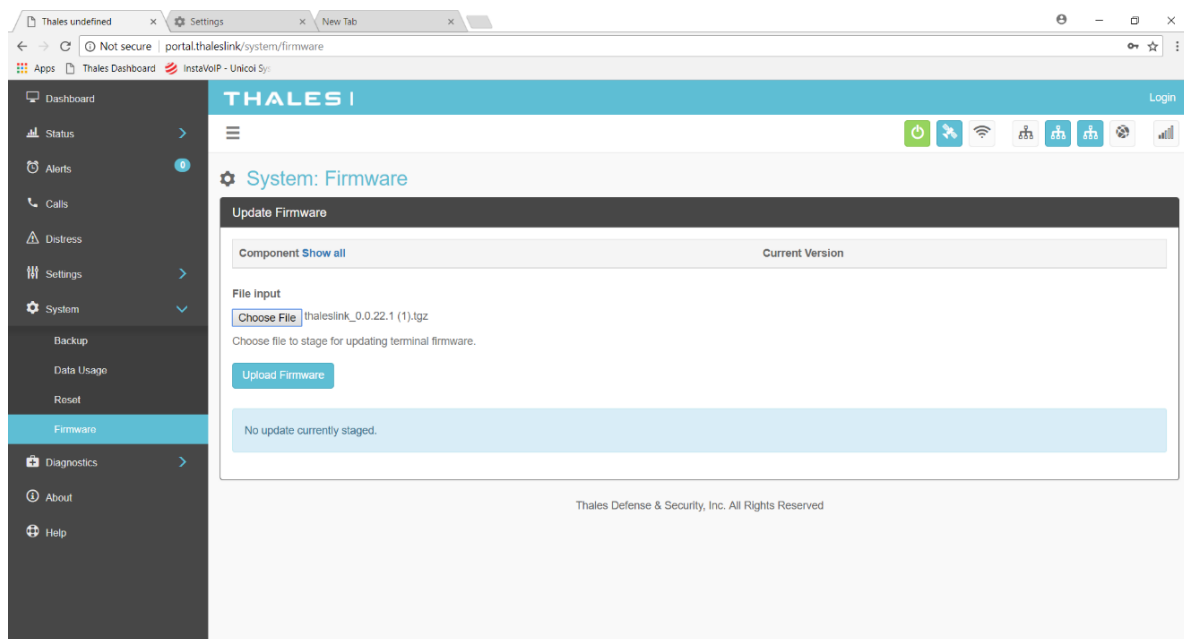
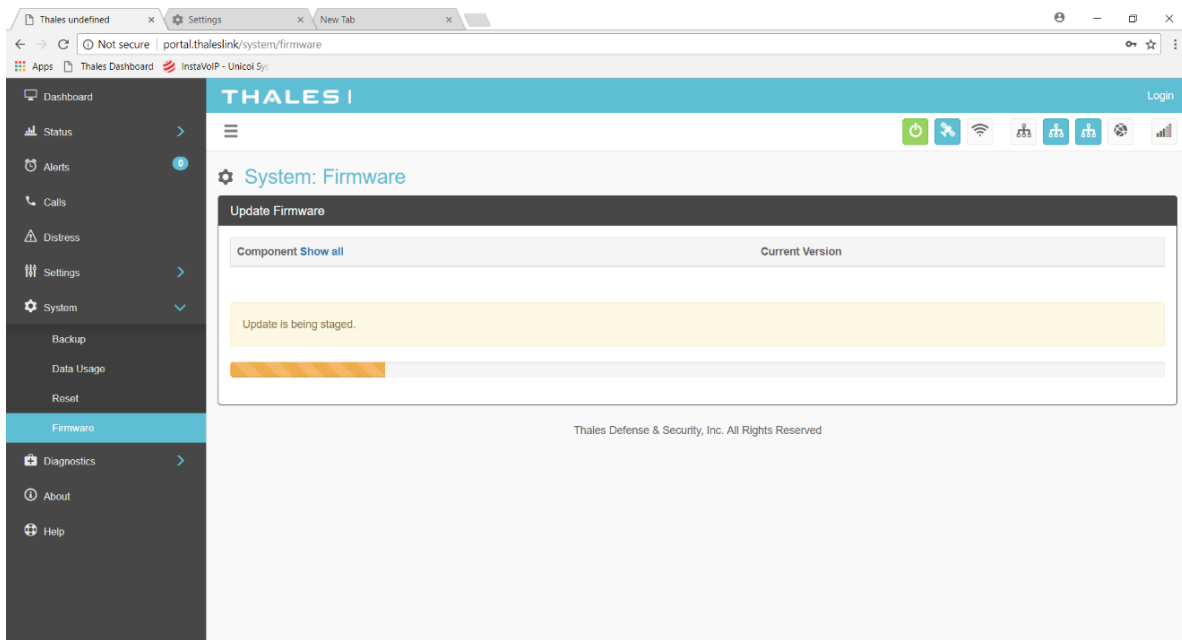


Figure 5-1 System → Firmware

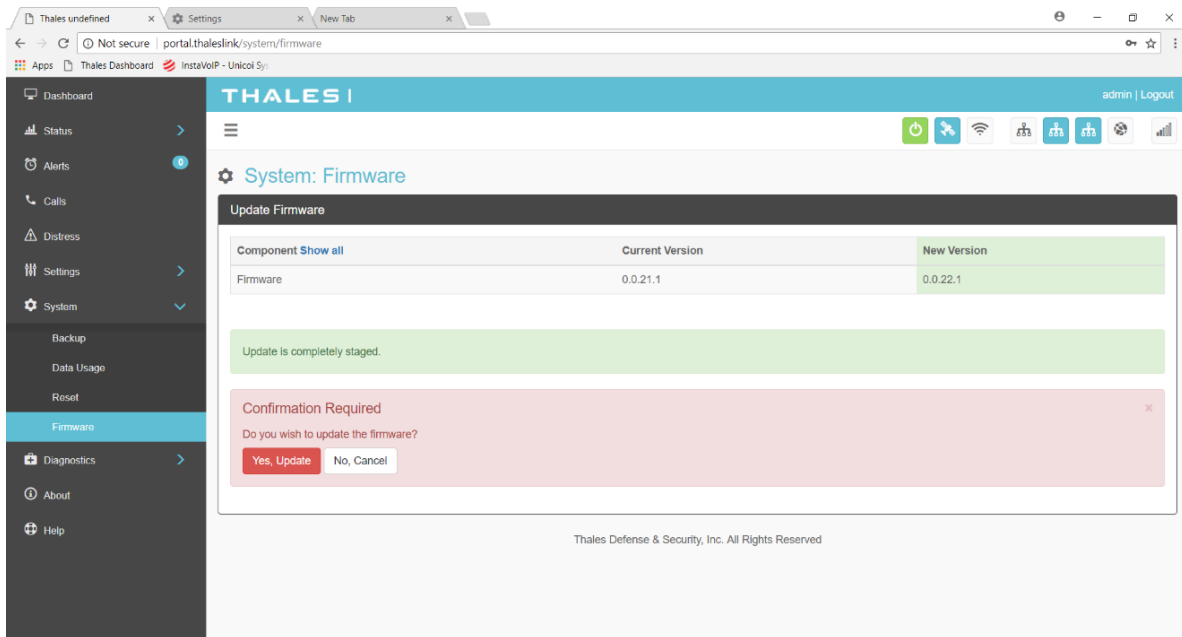
5. Select CHOOSE FILE.
6. Go to File Input and select the Browse button.
7. Navigate to location of downloaded file (See Page 5-1). This file should have “FW revision.tgz” as the file extension
8. Select the “SELECT” button
9. After file has been selected return to the Firmware page.
10. Select “UPLOAD FIRMWARE” button. This may take a few seconds as a progress bar moves across the page (see Figure 5-2).



*Figure 5-2 Firmware Being Staged*

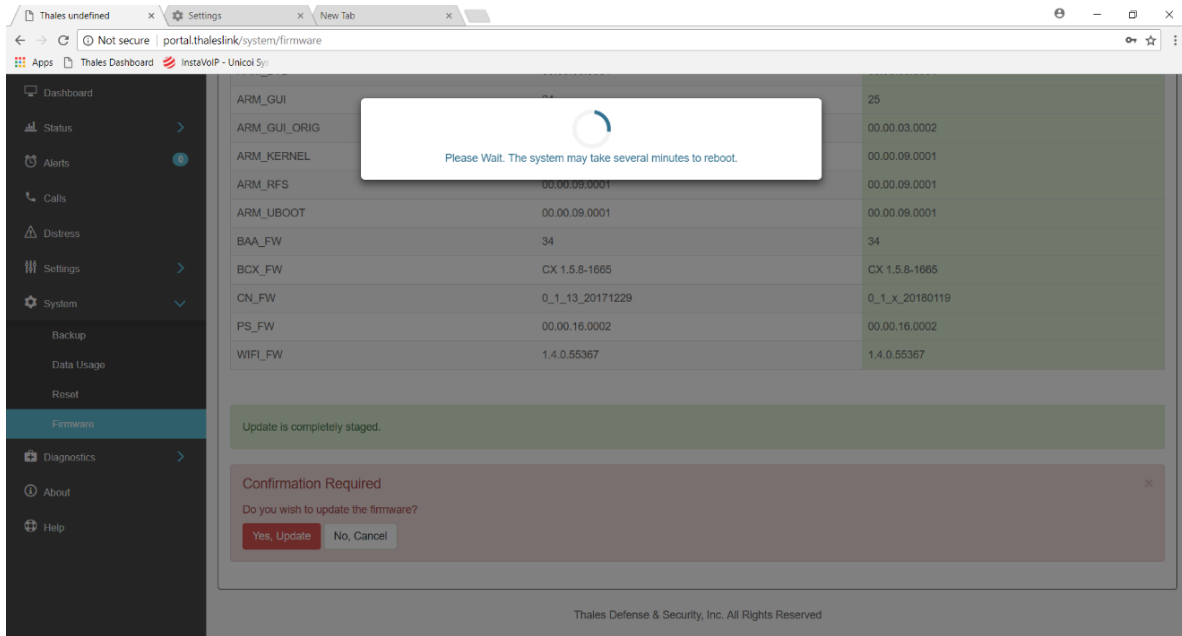
11. Once staged the Firmware page will display “UPDATE STAGED” (At this point user will be able to see Current and New Versions side by side on the Firmware page)

12. Select “RUN”



*Figure 5-3 System → Firmware Update Confirm*

13. Once YES, UPDATE is selected, the process to Update Firmware has begun and will take several minutes to complete. **\*DO NOT REMOVE POWER DURING THIS PHASE\***



*Figure 5-4 Firmware Update in Process*

14. Once completed system will reboot, wait for all the Status LEDs to go Solid Green and/or Blue. This may take a couple minutes.
15. Verify Firmware Update by connecting to “THALES LINK” on Wi-Fi or Ethernet port.
16. Open a web browser and type: <http://portal.thaleslink> (do not type .com or any other extension).
17. Once prompted enter the admin Password (this will not change from before the firmware update).
18. Navigate to the SYSTEM → Firmware to view updates. (Software version can also be found in the ABOUT menu item.)

System: Firmware

Update Firmware

Component	Current Version	New Version
Firmware	00.00.18.0015	
ARM_APP	00.00.17.0016	
ARM_DTB	00.00.08.0010	
ARM_GUI	21	
ARM_GUI_CRIG	00.00.03.0002	
ARM_KERNEL	00.00.08.0010	
ARM_RFS	00.00.08.0010	
ARM_UBOOT	00.00.08.0010	
BAA_FW	34	
BCX_FW	CX 1.5.7-1167-engA	
CN_FW	0_1_11_20171011	
PS_FW	00.00.14.0009	
WIFI_FW	1.4.0.87	

File input

Choose File

No file chosen

Choose file to stage for updating terminal firmware.

No update currently staged.






Thales Defense & Security, Inc. All Rights Reserved

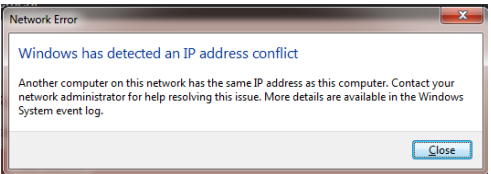
Figure 5-5 System → Firmware Update Completed

## CHAPTER 6 TROUBLESHOOTING

### TROUBLESHOOTING

Table 6-1 Troubleshooting

PROBLEM	SOLUTION
 Satellite LED Flashing GREEN	<ul style="list-style-type: none"> <li>Flashing GREEN light indicates that it is acquiring the satellite. If it continues to flash for more than 5 minutes, check that the antenna has a clear view of the sky.</li> <li>Reboot TU.</li> </ul>
 Satellite LED Flashing RED	<ul style="list-style-type: none"> <li>Critical Fault Detected. Open management portal <a href="http://portal.thaleslink">http://portal.thaleslink</a> and check Alerts. Make any adjustments. (For example: check antenna connection, or GPS not acquired.)</li> <li>Turn unit off and on again. If same result, contact your service provider.</li> </ul>
 System LED Flashing Green	<ul style="list-style-type: none"> <li>Start-up in progress. Wait until unit has run diagnostics and completed start procedure. This may take more time than usual when acquiring satellites for the first time</li> <li>Switch power off and back on if the light doesn't turn solid green after 5 minutes.</li> <li>Connect the management portal, type in <a href="http://portal.thaleslink">http://portal.thaleslink</a> and check for any system alerts</li> </ul>
 System LED Flashing RED	<p>Fault Detected. Open management portal <a href="http://portal.thaleslink">http://portal.thaleslink</a> and check for alerts. Make any adjustments. (For example: Common alerts include, but not limited to, are the SIM Card not installed, SIM Card not provisioned. Power-Up Test (POST) failure.)</p> <ul style="list-style-type: none"> <li>Turn unit off and on again. If same result, contact your service provider.</li> </ul>
 Wi-Fi LED	<p>OFF – Turn Wi-Fi ON using the Management Portal. THALESLINK &gt; SETTINGS &gt; WIFI</p> <p>Solid RED – Reboot the TU.</p> <p>Flashing GREEN – Check NO OR WEAK WI-FI</p>
Call Logs are not appearing	<p>Call logs must be enabled. Verify call logs are enabled (SETTING → PHONE → PHONE CONFIGURATION)</p>

PROBLEM	SOLUTION
Cannot connect to the Management Portal	<ul style="list-style-type: none"> <li>• Ensure Terminal Unit is powered ON</li> <li>• Ensure Wi-Fi is enabled and connected to ThalesLINK. If not, ensure Cat 5 cable is connected to one of the three Ethernet ports (NOT WAN or POTS Port). If Ethernet connection, replace the cable and re-check connection</li> <li>• Open web browser and type <a href="http://portal.theseslink/#">http://portal.theseslink/#</a>. Ensure network settings are correct on the connected device.</li> <li>• Device's browser may be incompatible. Update or try different browser.</li> <li>• Verify IP address is correct – 172.33.16.2</li> <li>• You may need to reconnect via Ethernet or Wi-Fi to the TU.</li> <li>• Check to make sure the correct address is typed in <a href="http://portal.theseslink">http://portal.theseslink</a></li> </ul>
Cannot connect to Wi-Fi service	<ul style="list-style-type: none"> <li>• Check to see if there's an available connection by checking the devices that are connected in Status → Current Devices page.</li> <li>• Only 5 simultaneous devices can connect to the Wi-Fi. Any additional connection attempts are blocked.</li> <li>• Remove one or more devices from the Wi-Fi and try again to connect.</li> <li>• Use the Wi-Fi Device Whitelist to limit access to specific wireless devices.</li> </ul>
Network Error	<p>If you receive a message similar to this, another user is attempting to use the same IP Address as your computer. Only 1 administrator can be logged on at a time.</p> 
No or Weak WI-FI Signal	<ul style="list-style-type: none"> <li>• Connect Wi-Fi antenna and ensure it is secured tightly</li> <li>• If walls or metal obstructions are between the TU and the Wi-Fi device, move closer to the TU or move the TU to a better location with less obstructions</li> <li>• Check to make sure Wi-Fi device is connected to the TU's Wi-Fi and verify that you are connected to the ThalesLINK.</li> <li>• Check the Management Portal to make sure the Wi-Fi device is registered as a user</li> </ul>
ThalesLINK is not obtaining a satellite signal (Satellite LED is red)	<ul style="list-style-type: none"> <li>• Check signal bars at the top of the Management Portal. If no bars are highlighted, the satellite is not being detected. Wait a few minutes to see if the signal strength improves as another satellite comes into view.</li> <li>• Check antenna connection at the TU and antenna. Make sure no corrosion has occurred on the cable connections to the antenna and that the connectors are screwed in tightly.</li> <li>• Check antenna for a clear view of the sky with no obstructions. Relocate antenna if needed.</li> </ul>



PROBLEM	SOLUTION
	<ul style="list-style-type: none"> <li>• Check for interferers in the area that could be affecting the signal such as active radars, VSAT systems and other radio antennas. Turn those off and retest.</li> <li>• Move vessel to a new location and retest if other interfering vessels are in the area</li> <li>• Reboot TU and check the Alerts.</li> <li>• Call Service Provider if the satellite connection is still not working.</li> </ul>
ThalesLINK management portal does not work	<p>Ensure Terminal Unit is powered ON            Ensure Wi-Fi is enabled and connected to MissionLINK            If not ensure Cat 5 cable is connected to one of the three Ethernet ports (NOT WAN or POTS Port)            Open web browser and type <a href="http://portal.thaleslink">http://portal.thaleslink</a>            May have to disable LTE or Wireless data to ensure connection is to MissionLINK on mobile devices.            Device's browser may be incompatible. Update or try a different browser.</p>
Terminal Unit does not power-ON	<ul style="list-style-type: none"> <li>• Check TU for Green lights, If green light is on Unit has Power</li> <li>• Push Power Button on front of TU.</li> <li>• Check that the power source is providing 10-32V (optional accessory)</li> <li>• Check Power 10-32V DC cable polarity is correct</li> <li>• Check to ensure Ignition line is connected to switched line or connected to Red (Positive line) for continuous operation (optional accessory)</li> <li>• Check that ignition or remote switch is turned on if ignition line is connected (optional accessory)</li> </ul>
Terminal Unit has power but accessories not working	<ul style="list-style-type: none"> <li>• Remove power from accessories and disconnect from TU. Restart TU using the Power button or remove power from TU for 10 seconds. After TU has rebooted re-attach accessories</li> <li>• If POE accessory not receiving power, make sure POE is enabled for that port.</li> <li>• POE is not available on WAN port. Any device on WAN port needs its own power source.</li> <li>• Check VoIP phone manuals for proper configuration. Each phone may have a different configuration method.</li> </ul>

PROBLEM	SOLUTION
Terminal Unit is not responding	<ul style="list-style-type: none"> <li>• Check LED status on TU or on Management Portal. Make sure there are no RED LEDs. Check for Alerts in Management Portal by selecting the Alerts menu item</li> <li>• Reboot the system.</li> <li>• Check for any Alerts that have been generated</li> <li>• As a last resort, use the manual reset button, located below Wi-Fi antenna port, using a straightened paper clip or similar sized article insert into port and push reset button.</li> <li>• Call Service Provider if the TU is still not responding</li> </ul> <p><u>NOTE:</u> This is not recommended as a routine troubleshooting measure. All user data and debug information will be lost and factory defaults returned.</p>
Terminal Unit not connecting to Management Portal	<ul style="list-style-type: none"> <li>• System LED is flashing GREEN, wait until it turns solid GREEN, then try reconnecting to the portal.</li> </ul>
Terminal Unit does not power-ON	<ul style="list-style-type: none"> <li>• Check Terminal Unit for Green lights, If green light is on Unit has Power</li> <li>• Push Power Button on front of Terminal Unit</li> <li>• Check that the AC/DC or the 10-32V DC cable is connected</li> <li>• Check that the power source is providing 10-32V (optional accessory)</li> <li>• Verify that the power supply is plugged into the power source</li> <li>• Check Power 10-32V DC cable polarity is correct</li> <li>• Check to ensure Ignition line is connected to switched line or connected to Red (Positive line) for continuous operation (Optional Accessory)</li> <li>• Check that ignition or remote switch is turned on if ignition line is connected (optional accessory)</li> </ul>

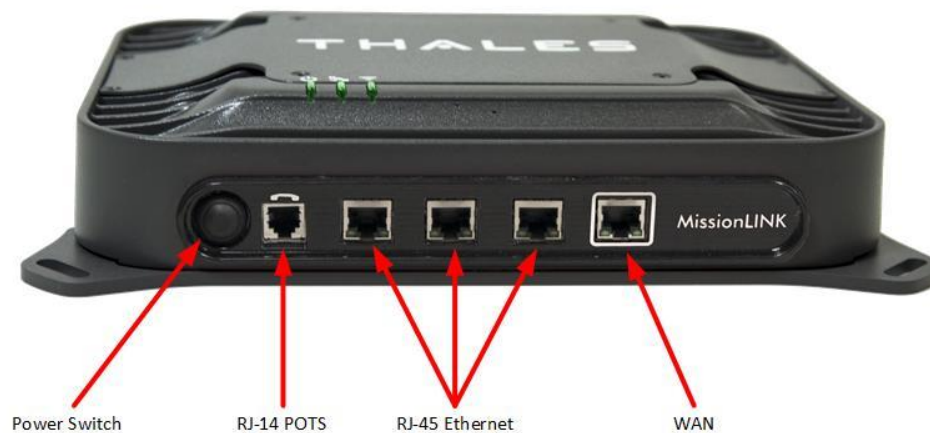
## System Resets

When ThalesLINK is not responding or operating properly it may be necessary to rest the system. There are varying levels of system resets and are explained below:

### Power Cycle

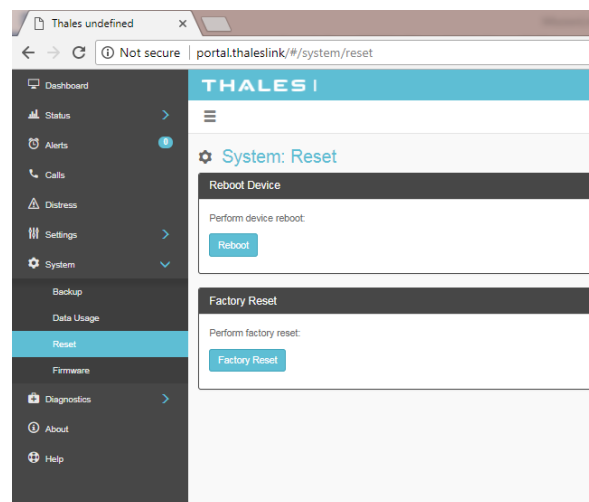
There are 3 ways to power cycle the system:

- If power is already on (LEDs are illuminated), press and release the Power Switch on the unit to power the unit off. Again, press and release the Power Switch to power the unit on. It will take a couple minutes before the boot-up cycle completes.



*Figure 6-1 Location of Power Button on Terminal Unit (TU)*

- From the Management Portal, select SYSTEM → RESET → REBOOT DEVICE. Press REBOOT. It will take a couple minutes before the boot-up cycle completes.



*Figure 6-2 Management Portal - SYSTEM → RESET*

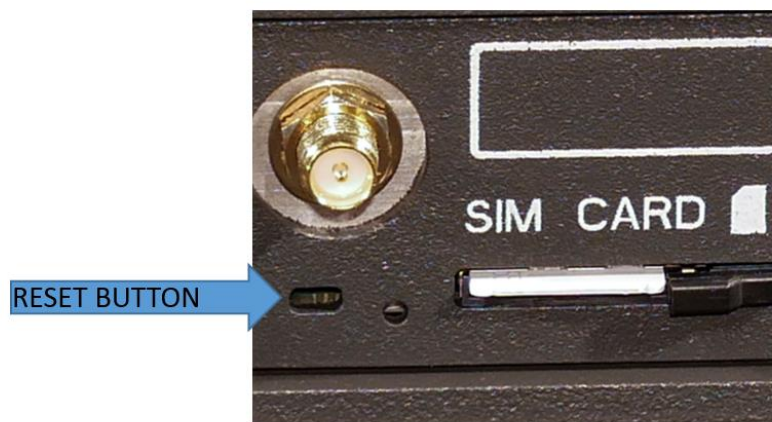
- If neither of these work, then unplugging the system from the power source may be necessary. Note: Always wait at least 10 seconds for power inside the unit to dissipate before reconnecting the input power.

## Factory Reset

As its name implies this restores the factory defaults (passwords will return to “admin”). This is particularly helpful when a system has been wrongly configured and starting over is the easiest option. If an admin password is customized and is forgotten, the only way to reset it is to use the factory reset option.

Factory Reset can be accomplished by either of these two actions:

- Remove the SIM card cover exposing the reset hole. Using a straightened paperclip, insert it into the round hole just to left of the SIM card as shown in Figure 6-3. Push in until the paperclip causes the switch to click. A factory reset will occur.



*Figure 6-3 RESET BUTTON*

- From the Management Portal select SYSTEM → RESET → FACTORY RESET. Confirm by selecting YES, FACTORY RESET. A factory reset will occur.

## Firmware Revert



### **NOTE**

FIRMWARE REVERT should only be used when a system has a serious issue and all other troubleshooting tips have been tried. Call your Service Provider before doing a firmware revert to make sure all other troubleshooting steps have been exhausted.

This restores the previous version FIRMWARE used on the system.

This can be accomplished by following these steps:

- Remove the SIM card cover exposing the reset hole. Using a straightened paperclip, insert it into the round hole just to left of the SIM card as shown in Figure 6-3. Push in until the paperclip causes the switch to click. At the same time hold the power button in until the LEDs blink and then release.

## Alerts

*Table 6-2 ALERTS / Error Messages*

Alert Name	Description	Level	Additional Information	Corrective Action
ANT_CABLE	Cable loss excessive; check system	Critical	Cable loss may exceed the system spec of 9 dB	Check Antenna cable for damage or loose connections. Replace if necessary.
ANT_CABLE	Cable loss high; performance maybe degraded	Fault	Cable loss may exceed the system spec of 9 dB	Check Antenna cable for damage or loose connections.
ANT_MISSING	Unable to detect antenna	Fault		Check Antenna for damage. Check cable for loose connections. Replace if necessary.
BCX-denial	Failed to connect to pass data, reason – location	Fault		Restart TU. Contact representative if problem persists.
BCX_SIM	Modem failed to read SIM card	Warning		Remove, clean and re-insert SIM. Contact service provider if problem persists.
CN_OFF	CN is powered off, restart required	Critical	CN is noticed to be unexpectedly off.	Restart TU. Contact representative if problem persists.
CN_REBOOT	CN Reboot has occurred, full system restart is required.	Critical	CN Module restarts while the system is up and running.	Restart TU U. Contact representative if problem persists.
MODEM_ACT	Modem returned an unknown error – cannot activate	Fault		Restart TU. Contact representative if problem persists.

Alert Name	Description	Level	Additional Information	Corrective Action
MUX_PLL_UNLOCKED	Antenna mux out-of-lock	Critical	PLL failed to acquire	Restart TU. Contact representative if problem persists.
PWR_IBIT_FAILURE	The power has failed “Initiated Built In Self Test” View Logs for details.	Fault		Open <a href="http://portal.thaleslink">http://portal.thaleslink</a> and review Self-Test logs. Contact representative.
SIM_MISSING	SIM card not detected	Fault	SIM Card is physically missing	Replace SIM card

**THIS PAGE INTENTIONALLY LEFT BLANK**



## CHAPTER 7 TECHNICAL SPECIFICATIONS

### TECHNICAL SPECIFICATIONS

Table 7-1 Technical Specifications

Description		Parameters
<b>Technical</b>		
Frequency of Operation	TX	1616 to 1626.5 MHz
	RX	1616 to 1626.5 MHz
Channelization	FDMA spacing	41.667 KHz
	TDMA Timing	8.3 mS Slot in a 90 mS window
	Channels Available	240 channels
EIRP (Weighted Average)	Voice	9 dBW
	Data (Block 1)	11.7 dBW
	Data Certus <sup>SM</sup> 1xC8 16 APSK	15.2 dBW
	Data Certus <sup>SM</sup> 2xC8 16 APSK	18.2 dBW
Modulation	Block 1 Voice/Data	DQPSK
	Certus <sup>SM</sup> C1, C8 Voice/Data	QPSK
	Certus <sup>SM</sup> C8 APSK Data	16 APSK
Antenna	Type	Electronically steered phased array
	Polarization	RHCP
	Gain	9.5 dBi
	Beam Width	31° typical per beam
	MissionLINK coverage	8° to 90 elevation
	MissionLINK coverage	provides useful link margin up to roll = 20°
<b>Power</b>		
DC Input	Voltage	10-32 VDC
	Max Current	12 Amps
	Max Power	120 Watts
Ethernet	3x PoE	PSE Class 2 (6.5 Watts each)

## TEMPERATURE

*Table 7-2 Operating and Storage Temperatures*

Description		Temperature Range
Broadband Active Antenna	Operating Temp	-30°C to +55°C
	Storage Temperature	-40°C to +85°C
Terminal Unit	Operating Temp	-30°C to +55°C
	Storage Temperature	-40°C to +85°C

## PHYSICAL CHARACTERISTICS

*Table 7-3 Physical Characteristics*

Description		Parameters
Broadband Active Antenna	Dimensions	14" D x 4" H (35.6 cm x 10.2 cm)
	Weight	7 lbs (3.2 kg)
Terminal Unit	Dimensions	12" L x 9" W x 3" H (30.5 cm x 23 cm x 7.6 cm)
	Weight	< 7.5 lbs (3.4 kg)

## CONNECTOR DETAILS:

### General Purpose Inputs / Outputs (GPIO)

The GPIO has 4 main functions. Refer to Table 7-2 for the pin descriptions of the GPIO connector.

1. **1-Wire SOS/Distress** → This is activated when Pin 5 has been connected to GND signal (ANY of the pins 1, 8 or 12) for more than 3 seconds.

Once set, it sends an automated message stating SOS has been triggered. This message contains Latitude, Longitude, Altitude and predefined user message (setup in management portal) to a message recipient.

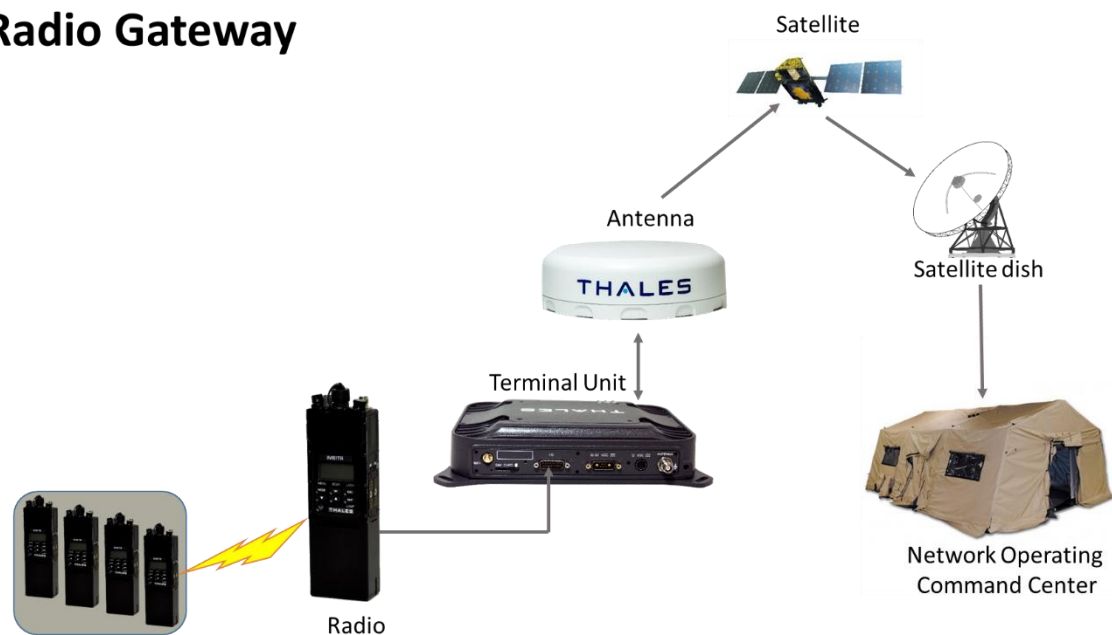
**IF Location Services are turned on the distress signal will increase frequency of transmission to every 5 minutes.**

### **NOTE: THERE IS NO EXTERNAL INDICATION OF SOS/DISTRESS**

This security feature is for user protection. **The ONLY way to remove active SOS is to enter management portal under DISTRESS TAB**

2. **Radio Gateway** → advanced users can connect Land Mobile Radio I/O to send and receive voice calls over the ThalesLINK. This feature is for advanced users familiar with Land Mobile Radio systems and requires custom cable connections between GPIO and Radio NOT offered by TDSI. Because each radio system will require a unique setup is highly advised to contact your TDSI representative for help in setup of this advanced user feature.

## Radio Gateway



*Figure 7-1 Radio Gateway for Advanced Land Mobile Services*

3. **2- Wire RS232→** Reserved for future use.  
Contact your service provider or Thales Customer Service for help in setting up of this advanced user feature.
4. **User defined GPIO→** Reserved for future use.  
Contact your service provider or Thales Customer Service for help in setting up of this advanced user feature.

## Connector location

D-SUB 15 Pin Standard shown in Figure 7-2.

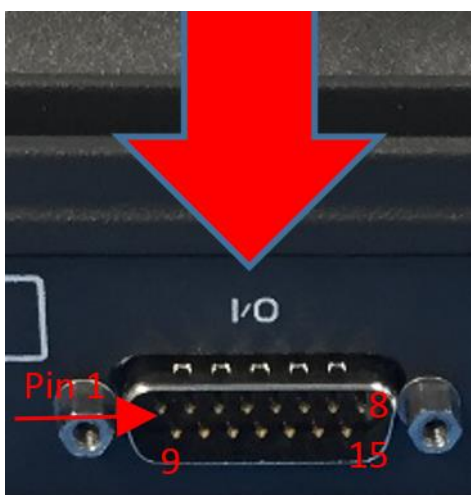


Figure 7-2 GPIO Connector Pin Detail

Table 7-4 GPIO Connector Pin Definition

Pin No	Name	Description
1	GND1	Ground
2	Audio_In +	Radio Gateway functionality, differential (+) Hi-Z Audio Input from external Radio
3	Audio_Out +	Radio Gateway functionality, Differential (+) Low-Z Audio Output to external radio (mic input)
4	RadioCOR	Radio Gateway functionality, Radio initiated voice into terminal (optional)
5	SOS_IN	SOS remote functionality, Ground pin to activate internal SOS
6	GPI01	Software configurable GPIO pin #1 (future)
7	RS232_TD	RS232 Output (future)
8	GND2	Ground
9	Audio_In -	Radio Gateway functionality, differential (-) Hi-Z Audio Input from external Radio
10	Audio_Out -	Radio Gateway functionality, Differential (-) Low-Z Audio Output to external radio (mic input)

Pin No	Name	Description
11	RadioPTT	Radio Gateway functionality, Putput PTT from terminal to external radio, short to ground for PTT enabled, Open drain requires external 10k pullup resistor
12	GND3	Ground
13	GPI02	Software configurable GPIO pin #2 (future)
14	RS232_RD	RS232 Input (future)
15	12V	=12V output, 100mA

## TU 12V Connection Detail

Type: KPPX-4x connector (or similar) shown in Figure 7-3.

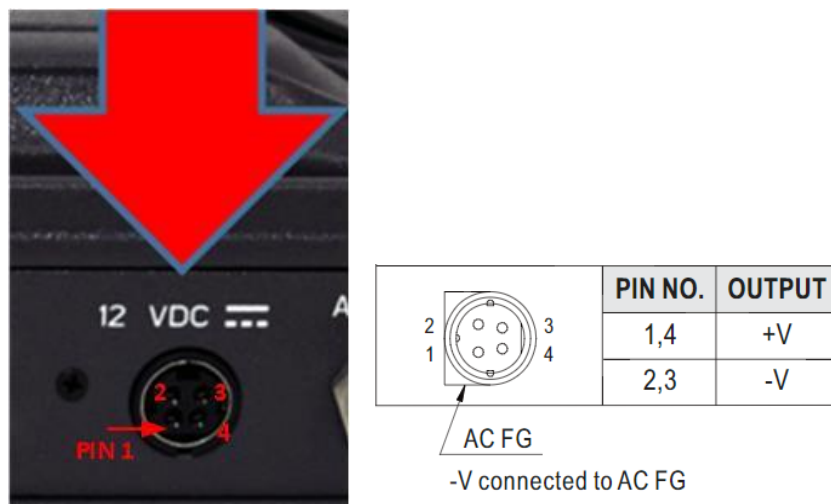


Figure 7-3 12V Input and Mating Connector Detail

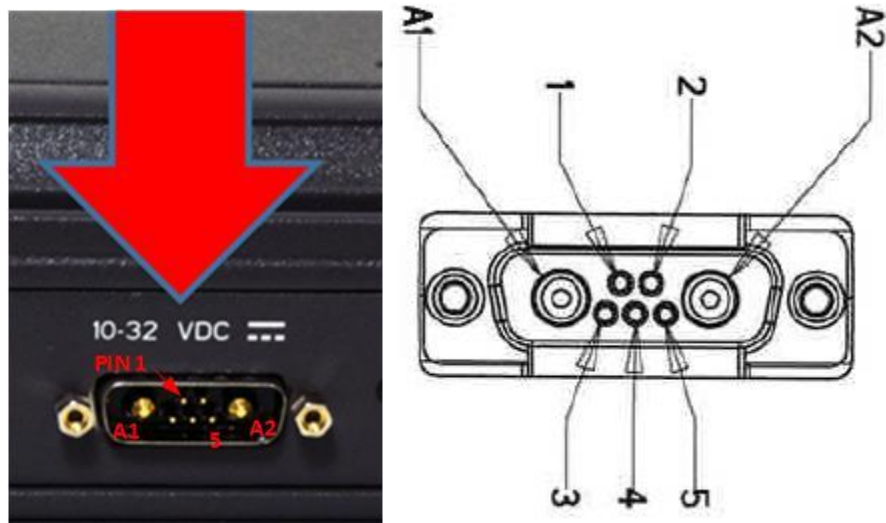
## TU 10-32VDC Connection Detail

Type: 684M7W2103L201 connector (or similar) shown in Figure 7-4.

A1 = V+ /10-32VDC

A2 =V- /GND

Pin 5 = Ignition



*Figure 7-4 10-32 VDC and Mating Connector Detail*

## CHAPTER 8 ACRONYMS / GLOSSARY

### ACRONYMS / GLOSSARY

*Table 8-1 List of Acronyms*

Acronym	Description
AC	Alternating Current
API	Application Programming Interface
BAA	Broadband Active Antenna
BAE	Broadband Application Electronics
BCX	Broadband Core Transceiver
BIT	Built In Test
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DTMF	Dual Tone Multi-Frequency
EBB	Enhanced Broadband
ETSI	European Telecommunications Standards Institute
GPIO	General Purpose Inputs/Outputs
GPS	Global Positioning System
HGA	High Gain Antenna
HRLP	High Speed Radio Link Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ITU	International Telecommunications Union
LAN	Local Area Network
LED	Light Emitting Diode
LEO	Low Earth Orbiting
LGA	Low Gain Antenna
LOS	Line of Site
MO	Mobile Originated
MT	Mobile Terminated
NAS	Network Attached Storage
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
POE	Power Over Ethernet
POST	Power On Self-Test
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QSG	Quick Start Guide
R/W	Read/Write
RF	Radio Frequency

Acronym	Description
SBC	Smart Battery Charger
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMBus	System Management Bus
SV	Satellite Vehicle
TCP	Transmission Control Protocol
TDSI	Thales Defense & Security, Inc.
TLS	Transport Layer Security
TU	Terminal Unit
UDP	User Datagram Protocol
UL/DL	Uplink/Downlink
VLAN	Virtual Local Area Network
VOIP	Voice of Internet Protocol
WAN	Wide Area Network
WI-FI	Wireless Network
WPA2-PSK	Wi-Fi Protected Access 2 – Pre-Shared Key

*Table 8-2 List of Definitions*

Acronym	Description	
API	Application Programming Interface	The management portal provides API to allow for the connection to the terminal remotely.
BAA	Broadband Active Antenna	The antenna and supporting electronics that interface an Iridium satellite terminal with the Iridium constellation
BAE	Broadband Application Electronics	Hardware and software platform resident in the TU that interfaces with the BCX, BAA and user devices
BCX	Broadband Core Transceiver	Hardware designed for an Iridium satellite terminal to interface end-user equipment with an Iridium BAA
BIT	Built In Test	Diagnostic testing for system integrity check and error reporting
DHCP	Dynamic Host Configuration Protocol	The Dynamic Host Configuration Protocol (DHCP) is a system used in computer networking to automatically assign networking information to a client.
DTMF	Dual Tone Multi-Frequency	Signals generated from phone keypad
EBB	Enhanced Broadband	EBB Mode is Iridium NEXT phase 1 EBBS (Enhanced Broadband Service)
ETSI	European Telecommunications Standards Institute	Organization that maintains standards for Information and Communications applicable to fixed and mobile radio platforms
GPIO	General Purpose Inputs/Outputs	General use pins



Acronym	Description	
HGA	High Gain Antenna	External antenna that connects to the TU via a coaxial cable. The HGA2 (also called BAA-H2) provides 352 kbps uplink and downlink capability
HRLP	High Speed Radio Link Protocol	Management of In-band signaling on broadband channels
HTTP	Hypertext Transfer Protocol	Protocol to exchange or transfer hypertext
ICMP	Internet Control Message Protocol	Protocol by network devices that typically send error messages and is used for diagnostics
ITU	International Telecommunications Union	Agency of the United Nations responsible for issues concerning information and communications technologies
LED	Light Emitting Diode	Semiconductor that emits colored light
LGA	Low Gain Antenna	External antenna that connects to the TU via a coaxial cable. The LGA1 and LGA2 support the future Certus <sup>SM</sup> 100 and Certus <sup>SM</sup> 200 capabilities
Management Portal		Management Portal: A web page served from the Terminal Unit that brings together the diverse status and configuration information of the TU in one place.
MO	Mobile Originated	Calls originating from the terminal
MT	Mobile Terminated	Calls terminating at the terminal
NAS	Network Attached Storage	Ability to store and retrieve files to/from a physical memory storage device attached to the network
PBX	Private Branch Exchange	Telephone connection between local users not requiring external phone connection
POST	Power On Self-Test	BIT Test performed at the turn-on of the TU
POTS	Plain Old Telephone Service	A voice-grade telephone service that utilizes analog signal transmission over copper loops
PSTN	Public Switched Telephone Network	The world's collection of interconnected voice-orientable public telephone networks, both commercial and government owned.
R/W	Read/Write	Capability
SIM	Subscriber Identification Module	Iridium provided method to authenticate and identify subscriber
SIP	Session Initiation Protocol	An Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, and chat
SMBus	System Management Bus	Two-wire bus for communications between devices such as a Terminal and a Smart Battery
SV	Satellite Vehicle	Iridium Satellite
TCP	Transmission Control Protocol	Core internet protocol that provides reliable delivery and error-checking
TLS	Transport Layer Security	TLS is on the standard way that computers on the internet transmit information over an encrypted channel.
TU	Terminal Unit	Electronic equipment that contains the BCX and the BAE

Acronym	Description	
UDP	User Datagram Protocol	Connectionless transmission model with minimum , no-handshaking protocol
UL/DL	Uplink/Downlink	To and from satellite communications
VLAN	Virtual Local Area Network	For context within this document, VLAN more specifically designates an Ethernet VLAN. A VLAN is establishes a broadcast domain that is partitioned
WPA2-PSK	Wi-Fi Protected Access 2 – Pre-Shared Key	Method of securing a Wi-Fi network

## CHAPTER 9 SPARE PARTS

### SPARE PARTS

The following list of equipment can be purchased as a kit or separately, depending on your requirements and/or needs.

*Table 9-1 List of Equipment*

IRIDIUM System Part Number				Description
MF700BV				Kit, MissionLINK Vehicular High Gain 700**
MF350BV				Kit, MissionLINK Vehicular High Gain 350**
	Qty	Part Number	Description	
✓	✓	1	1100789-501	Kit, Terminal Unit, Mounting Hardware
✓	✓	1	1100790-501	Kit, Antenna Magnetic Mount
✓	✓	1	1100792-501	Kit, Antenna Mounting Hardware Land
✓	✓	1	1600899-1	Broadband Active Antenna (BAA)
	✓	1	4102947-502	Terminal Unit 350, IRIDIUM CERTUS Land
✓		1	4102947-504	Terminal Unit 700, IRIDIUM CERTUS Land
✓	✓	1	855021-010	Cable TNCM-TNCM Coax TWS (LMR) 240 Mat 10Ft
✓	✓	1	855024-020	Cable, Vehicle Power Harness 20Ft
✓	✓	1	855026-010	Cable Cat-5e Patch RJ45M-RJ-45M Blue 10ft
✓	✓	1	85728-001	Antenna 2.4 GHz Dipole 2dBi Rev Pol SMA 50 OHM
✓	✓	1	3900011	Template, Terminal Unit Mount
✓	✓	1	3900013	Template, Land BAA Mount
✓	✓	1	3402174-1	MissionLINK Quick Reference Guide

\*\* The MF700BV kit includes the future software upgrade for 700 kbps downlink speeds whereas the MF350BV does not. The MF350BV is capable of the 700 kbps downlink speeds and the option can be purchased separately.

**Note:** The SIM card is provided by the airtime service provider and may be packaged separately from this kit.

*Table 9-2 MissionLINK Accessories*

Description	Part Number	Qty
Power Supply, AC/DC 12V – 160W	84670-001	1
Cable AC Power USA Plug Type B IEC 60320-C13 Connect Blk 6ft	854024-001	1
Cable AC Power Euro Plug Type E IEC 320-C14 Connect Blk 6ft	854025-001	1
Cable AC Power AUS Plug Type 1 IEC 320-C14 Connect Blk 6ft	854026-001	1
Cable AC Power UK Plug Type G IEC 320-C13 Connect Blk 6ft	854027-001	1
Cable TNCM-TNCM Coax TWS (LMR) 240 Mat 10Ft	855021-010	1
RF Cable TNCM-TNCM COAX TWS (LMR) 240 MAT 30FT	855021-030	1
RF Cable TNCM-TNCM COAX TWS (LMR) 400 MAT 100FT (Fixed Locations)	855022-100	1
Cable, Vehicle Power Harness 20Ft	855024-020	1
Cable Cat-5e Patch RJ45M-RJ-45M Blue 10ft	855026-010	1
Antenna 2.4 GHz Dipole 2dBi Rev Pol SMA 50 OHM	85728-001	1
Male-Male Ethernet Adapter (???)	TBD	1
SS Clip and Knob for IP Handset	TBD	1
IP Handset with 6” Coil Cord	1600913-1	1





Thales Defense & Security, Inc.  
22605 Gateway Center Drive | Clarksburg MD 20871  
Toll-Free 1.800.324.6089 | Phone: 240.864.7000 | Fax: 240.864.7920  
Email: [Customer.Service@thalesdsi.com](mailto:Customer.Service@thalesdsi.com) | Website:  
[www.thalesdsi.com](http://www.thalesdsi.com)