Thales MissionLINK®

User Manual for Certus 350 and Certus 200 Systems

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

Rev	Date	Description of Change	Author
Rev A	June 2018	Initial Release	SJacques
Rev B	Sept 2018	ECN: 42153 • Updates from Beta testing feedback	SJacques
Rev C	March 2019	ECN: 42531 • Update based on user feedback	SJacques
Rev D	Oct 2019	ECN 42906 • Update based on s/w updates	SJacques
Rev E	Jan 2020	ECN 43092 • Update based on user feedback and references to 700 kbps	SJacques
Rev F	May 2020	ECN: 53374 • Update based on new software rel. 2.1	SJacques
Rev G	Oct 2020	ECN: 53663 • Update based on new software rel. 2.2	SJacques
Rev H	Feb 2021	ECN: 53826 • Updated to include Certus 200	SJacques
Rev J	May 2021	ECN: 54064 • Industry Canada Cert – fixed typo	SJacques
Rev K	Dec 2021	ECN: 54409 • Added Certus 200 Mount • Added Portuguese Statement • Version 2.2.2 Updates	SPeters
Rev L	May 2022	ECN 54670 • Added Mexico, Japan, Korea and Brazil Certs • Updates pictures • Added new features – VLAN tagging, Satellite connection monitoring	SPeters
Rev M	Sep 2022	ECN 54855 • Handset updates: PTT & App support • GPIO feature addition	SPeters
Rev N	March 2023	ECN 55134 • Updated based on new SW release • New Alerts • Graceful Shutdown • System Stability Improvements	SPeters

Rev P	April 2024	ECN 55735 • Updated based on new SW release 3.0 • Iridium Messaging Transport® (IMT®) • Configurable Users	LCampbell

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®, Thales MissionLINK®, 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.

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.

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 Subject Line: Thales MissionLINK® User Manual (PN 84468/84468-IETM).

THALES

Table of Contents

List of Figures

List of Tables

SAFETY

The Thales MissionLINK® system should only be installed by a qualified installer of Land Mobile 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 Thales MissionLINK® system. Each chapter may have other specific warnings and cautions.

SHOCK HAZARD

WARNING

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 (TU) and Broadband Active Antenna (BAA) to maintain the warranty terms. Make sure the system is correctly grounded and power is off when installing, configuring and connecting components.

DO NOT OPERATE IN AN EXPLOSIVE ATMOSPHERE

WARNING

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.

LITHIUM ION BATTERIES

CAUTION

The TU contains a small Li-ion battery. Li-ion batteries have a very high energy density. Exercise precaution when handling and testing. Do not short circuit, overcharge, crush, mutilate, nail penetrate, apply reverse polarity, expose to high temperature or disassemble. High case temperature resulting from abuse of the cell could cause physical injury.

THALES

ANTENNA RADIATION HAZARDS

To comply with FCC Radio Frequency radiation exposure limits, the MissionLINK antennas must be installed at a minimum safe distance as shown below.

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 from the antenna. The antenna should be mounted in an area that prevents the possibility of close exposure to the antenna's radiation.

For the Certus 350 antenna, please remain at least 1.0m (3.3 feet) from the antenna while in operation.

For the Certus 200 antenna, please remain at least 0.8m (31 inches) from the antenna while in operation.
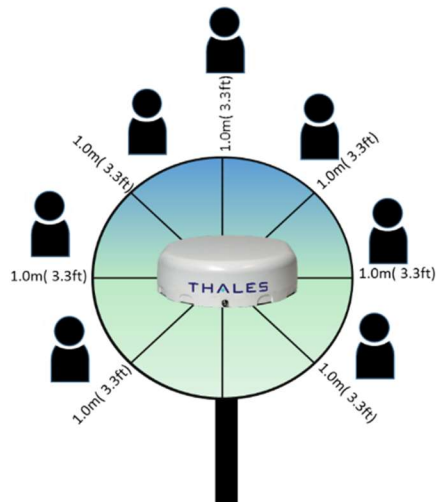
Certus 350   **Certus 200**
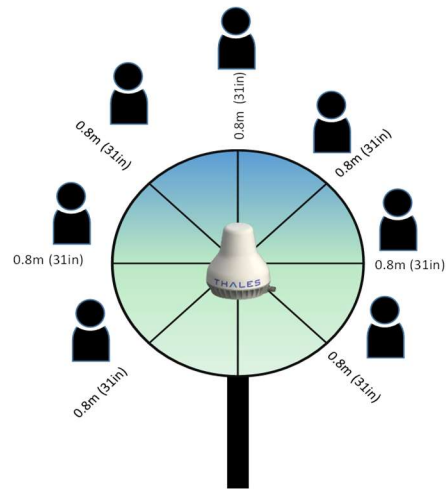
NOTE

Este Equipamento não tem direito à proteção contra interferencia prejudicial e não pode causar interferência em Sistemas devidamente autorizados

THALES

FCC Information

> **NOTE**
> Certus 350
> FCC Identifier: OKCMF350BV
> Contains FCC ID: OKCWROOM32U

> **NOTE**
> Certus 200FCC Identifier: OKCMF200BV
> Contains FCC ID: OKCWROOM32U

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Note:
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

THALES

Industry Canada Information

NOTE
Certus 350
Industry Canada: 473C-MF350BV
Contains IC: 473C-WROOM32U

NOTE
Certus 200
Industry Canada: 473C-MF200BV
Contains IC: 473C-WROOM32U

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter (473C-MF350BV or473C-MF200BV) has been approved by Industry Canada to operate with the antenna listed in Table 7-1 with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (473C-MF350BV ou 473C-MF200BV) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

THALES

Z571 Limited

Statement of Compliance

Document No. 11633_NZ

Based on documentation provided by the manufacturer Thales Communication Inc. the product listed below complies with the requirements of the **General User Radio Licence for Satellite Services** dated 21 April 2015.

Low (MHz)	High (MHz)	Reference Frequency (MHz)
399.9	400.5	400.2
1610	1660.5	1635.25
14000	14500	14250

Trade Name   Thales; Thales MissionLINK
Model Number   MF350BV
Description   Broadband Certus Satellite Terminal and Antenna

Gordon Slimmon
Director
Date: 21 September 2018

THALES

THALES DEFENSE & SECURITY,INC.

Declaration of Conformity with Radio Equipment Directive

The undersigned of this letter declares that the following equipment complies with the specifications of Radio Equipment Directive (2014/53/EU) concerning Radio & Telecommunications Equipment.

Equipment included in thisdeclaration

VF350BM Certus 350 VesseLINK Broadband Maritime Satellite Terminal and Antenna

VF200BM Certus 200 VesseLINK Broadband Maritime Satellite Terminal and Antenna

MF350BV Certus 350 MissionLINK Broadband Maritime Satellite Terminal and Antenna

MF200BV Certus 200 MissionLINK Broadband Maritime Satellite Terminal and Antenna

Equipment Applicability
The VesseLINK and MissionLINK provide voice and high speed data communication over 100% of the globe through the Iridium Certus broadband Satellite system.
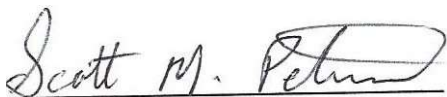
Declaration
The health requirement is met by conforming to EU standard EN 623 11. The safety requirement is met by conforming to EN 60950-1:2006 w/A2:2013 (for Certus 350) and to EN 62368-1:2014 (for Certus 200). The electromagnetic compatibility as set out in Directive 2014/30/EU is met by conforming to the EU standards ETSI EN 301-489-1 and ETSI EN 301-489-17. Effective and efficient use of radio spectrum in order to avoid harmful interference is met by conforming to the ETSI EN 301-441 standard.

Manufacturer
Thales Defense & Security, Inc.   22605 Gateway Center Drive
                                       Clarksburg, Maryland 20871 U.S.A.

Place and Date
Clarksburg, MD, 14 January 2021

Scott Peters

Director, Program Management

(Translation)

Type Approval Certificate

TÜVRheinland ®

Classification	Certification Ordinance Article 2-1-28-2 Earth Station for Portable Mobile Satellite (non-geostationary/Iridium)
Type of emission, frequency and antenna power	41K7 Q7W 1618.395833～1625.895833MHz(125kHz 間隔 61 波), 1618.3125～1625.9375MHz(125kHz 間隔 62 波), 1618.354167～1625.979167MHz(125kHz 間隔 62 波) 3.91W 83K4 Q7W 1618.5416665～1625.7916665MHz(250kHz 間隔 30 波), 1618.375～1625.875MHz(250kHz 間隔 31 波), 1618.4583335～1625.9583335MHz(250kHz 間隔 31 波) 4.7W 334K Q7W 1618.5～1625.5MHz(1000kHz 間隔 8 波), 1618.8333335～1625.8333335MHz(1000kHz 間隔 8 波), 1619.1666665～1625.1666665MHz(1000kHz 間隔 7 波) 15W 667K Q7W 1619～1625MHz(2000kHz 間隔 4 波), 1619.6666665～1625.6666665MHz(2000kHz 間隔 4 波), 1620.3333335～1624.3333335MHz(2000kHz 間隔 3 波) 15W
Model Name	MissionLINK MF200BV
License Holder	Thales Defense & Security, Inc.
Manufacturer	Thales Defense & Security, Inc.
Certificate number	005-102888
Certification date	2021-10-29

Approval as mentioned above is granted under the provisions of Article 38-24-1 of the Radio Law.

THALES

Type Approval Certificate

TÜVRheinland®

Classification	Certification Ordinance Article 2-1-28-2 Earth Station for Portable Mobile Satellite (non-geostationary/Iridium)
Type of emission, frequency and antenna power	41K7 Q7W 1618.395833～1625.895833MHz(125kHz 間隔 61 波), 1618.3125～1625.9375MHz(125kHz 間隔 62 波), 1618.354167～1625.979167MHz(125kHz 間隔 62 波) 0.35W 83K4 Q7W 1618.5416665～1625.7916665MHz(250kHz 間隔 30 波), 1618.375～1625.875MHz(250kHz 間隔 31 波), 1618.4583335～1625.9583335MHz(250kHz 間隔 31 波) 0.37W 334K Q7W 1618.5～1625.5MHz(1000kHz 間隔 8 波), 1618.8333335～1625.8333335MHz(1000kHz 間隔 8 波), 1619.1666665～1625.1666665MHz(1000kHz 間隔 7 波) 1.3W 667K Q7W 1619～1625MHz(2000kHz 間隔 4 波), 1619.6666665～1625.6666665MHz(2000kHz 間隔 4 波), 1620.3333335～1624.3333335MHz(2000kHz 間隔 3 波) 2.75W
Model Name	MissionLINK MF350BV
License Holder	Thales Defense & Security, Inc.
Manufacturer	Thales Defense & Security, Inc.
Certificate number	005-102915
Certification date	2022-02-18

Approval as mentioned above is granted under the provisions of Article 38-24-1 of the Radio Law.

2022-02-18

TÜV Rheinland Japan Ltd.

JRF-005-102915-001

User Manual PN 84468 Rev N

THALES

Federative Republic of Brazil
Telecommunications National Agency

Certificate of Equipment Authorization

(Not Transferable)

Nº **18490-21-12044**

Expires: **Indeterminada**

Date of Certificate: **06/05/2022**

Applicant:
CNPJ: 01.773.463/0001-59
OMNISYS ENGENHARIA LTDA

Manufacturer:

THALES DEFENSE & SECURITY, INC.,
22605 GATEWAY CENTER DRIVE, CLARKSBURG, MD, 20871
Nº

20871

ESTADOS UNIDOS DA AMÉRICA

This document approves, in accordance with the Telecommunication Rules and Regulations, the Certificate of Conformity number UL-BR 22.0312, issued by **UL do Brasil Certificações**. This approval is issued on behalf of the applicant here identified and is valid only for the product described below for use under the Anatels Rules and Regulations.

Type - Category:
Transceptor Móvel por Satélite - III

Model - Comercial Name (s)
MF350BV (MissionLink) /MF200BV (MissionLink)

Basic technical characteristics:

Potência Máxima de Saída (W)	Designação de Emissões	Faixa de Frequências Tx (MHz)
314,992	590KG1D	1.616,0 a 1.626,5

O produto incorpora Transceptor de Radiação Restrita com as características informadas no respectivo Certificado de Conformidade Técnica;
Ensaio de SAR não aplicável;
Módulos de interfaces disponíveis: FXS.
Comments

Na sua utilização o produto deve estar ajustado na(s) potência(s) e frequência(s) autorizadas pelo órgão técnico competente.

This certificate replaces the certificate of the same number issued in 31/03/2022

Constitutes an obligation of the manufacturer or supplier of the product in Brazil to identify all approved products with Anatel's mark before its distribution to the market, as well as observe and maintain the technical characteristics which motivated the original certification.

The information in this Approval Certificate can be confirmed in the Certification and Approval Management System - SCH, available on Anatel's website. (www.anatel.gov.br).

Davison Gonzaga da Silva
Gerente de Certificação e Numeração

THALES

UNIDAD DE CONCESIONES Y SERVICIOS
DIRECCIÓN GENERAL DE AUTORIZACIONES
Y SERVICIOS

ift
INSTITUTO FEDERAL DE
TELECOMUNICACIONES

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

CERTIFICADO DE HOMOLOGACIÓN
Clase: PROVISIONAL
Número: RCSTHMF20-0842
Vigencia: 4 de mayo de 2021

JORGE LUIS GONZÁLEZ BELTRÁN
REPRESENTANTE LEGAL DE
THALES MÉXICO, S.A. DE C.V.
Blvd. Miguel de Cervantes Saavedra No. 301, piso 16
Col. Ampliación Granada
C.P. 11520, Miguel Hidalgo, Ciudad de México.

Fecha de emisión: **4 de mayo de 2020**	Oficio respuesta a solicitud: **IFT/223/UCS/DG-AUSE/ 2246 / 2020**
Equipo: **Terminal satelital (Thales MissionLINK)**	
Marca: **THALES**	Modelo: **MF350BV**
Perito(s) en Telecomunicaciones: **Ing. José Luis Pérez Baez (IFT-P-0065-2017)**	

CARACTERÍSTICAS TÉCNICAS

Bandas de frecuencias	1616 – 1626.5 MHz (Banda "L")
Potencia isotroípica radiada efectiva (PIRE)	9 dBW (voz), 18.2 dBW (datos)
Tipo de modulación	DQPSK, QPSK, 16 APSK
Antena:	
Tipo	IP66 matriz escalonada
Diámetro	35.6 cm
Polarización	RHCP
Ganancia	9.5 dBi
Ancho del haz	31° típico

Autorizó
El Director General

GERARDO LÓPEZ MOCTEZUMA

Insurgentes Sur 1143,
Col. Nochebuena, C.P. 03720
Demarcación Territorial Benito Juárez,
Ciudad de México.
Tels. (55) 5015 4000

El presente Certificado está sujeto a las condiciones y notas descritas al reverso de la hoja 1.

hoja 1 de 1

A9D5-7D5B-9EC8-715B

방송통신기자재등의 적합인증서

Certificate of Broadcasting and Communication Equipments

상호 또는 성명 Trade Name or Applicant	아리온통신 주식회사
기자재명칭 Equipment Name	위성휴대통신용 무선설비의 기기
기본모델명 Basic Model Number	MF350BV
기기부호/추가 기기부호 Equipment code /Additional Equipment code	GMPCS / LARN8
파생모델명 Series Model Number	MissionLink
인증번호 Certification No.	R-C-YPP-MF350BV
제조자/제조국가 Manufacturer /Country of Origin	Thales Defense & Security, Inc. / 미국
인증연월일 Date of Certification	2022-03-18
기타 Others	

위 기자재는 「전파법」 제58조의2 제2항에 따라 인증되었음을 증명합니다.

It is verified that foregoing equipment has been certified under the Clause 2, Article 58-2 of Radio Waves Act.

2022년(Year) 03월(Month) 23일(Day)

국립전파연구원장

Director General of National Radio Research Agency

※ 인증 받은 방송통신기자재는 반드시 **"적합성평가표시"** 를 부착하여 유통하여야 합니다.
위반시 과태료 처분 및 인증이 취소될 수 있습니다.

CHAPTER 1   INTRODUCTION

INTRODUCTION

Thank you for your recent purchase of a Thales MissionLINK® product. Powered by the Iridium global satellite network, it is the only system with truly pole-to-pole coverage for voice and data communications. This USER MANUAL will cover a basic overview as well as advanced features for the Thales MissionLINK® systems including the Certus 350 MissionLINK and the Certus 200 MissionLINK.

Additional information can be found in the following documents:

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

> **i**
> **NOTE**
> Some figures in this manual depict a representative antenna that may be either a Certus 350 antenna or a Certus 200 antenna. Functionally, either antenna can be used for the operation described in the figures.

ABOUT THIS MANUAL

This user manual is intended for anyone who intends to operate and configure the MissionLINK system. It covers both the Certus 350 and the Certus 200 system operation and features. It, however, cannot cover all topics and advanced features. For questions or topics that are not covered in this manual, please contact your service provider or Thales at www.Thalesdsi.com.

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.

This 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 replaced the legacy Iridium satellite constellation with 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 to a Ground Station or Gateway. 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).
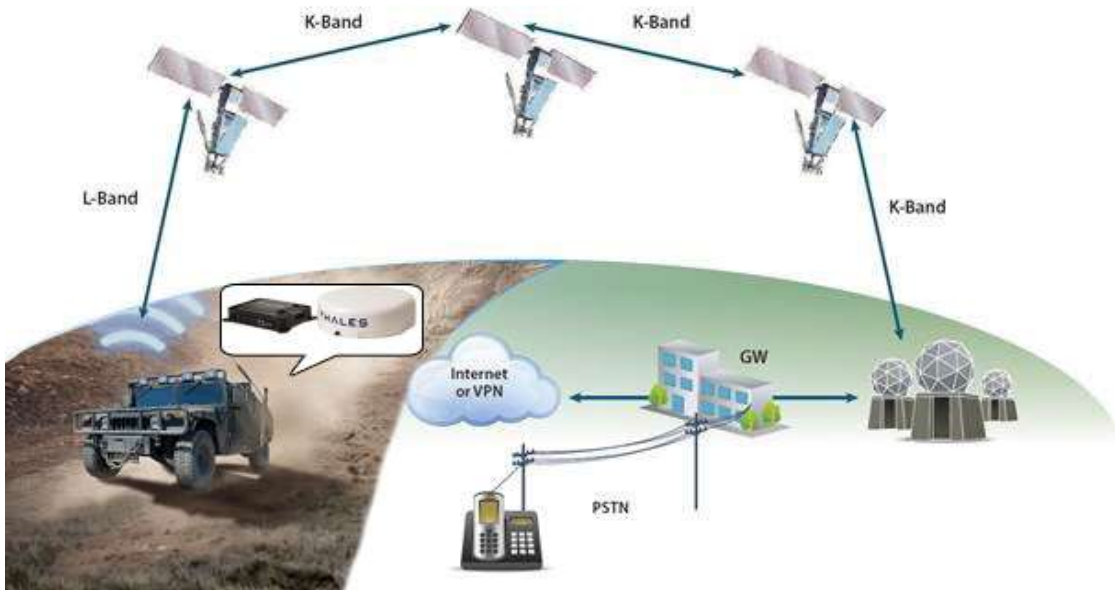
Figure 1-2 Typical Iridium Network Flow of a Voice or Data Call.

CHAPTER 2   SYSTEM OVERVIEW

SYSTEM DESCRIPTION

The MissionLINK system operates using Iridium Certus™ 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™ Multi-Services Platform

- Satellite data sessions up to 352kbps uplink and 704kbps downlink for Certus 350 systems and 176kbps uplink and 176kbps downlink for Certus 200 systems
- Up to 3 high quality Iridium voice lines

Satellite Voice
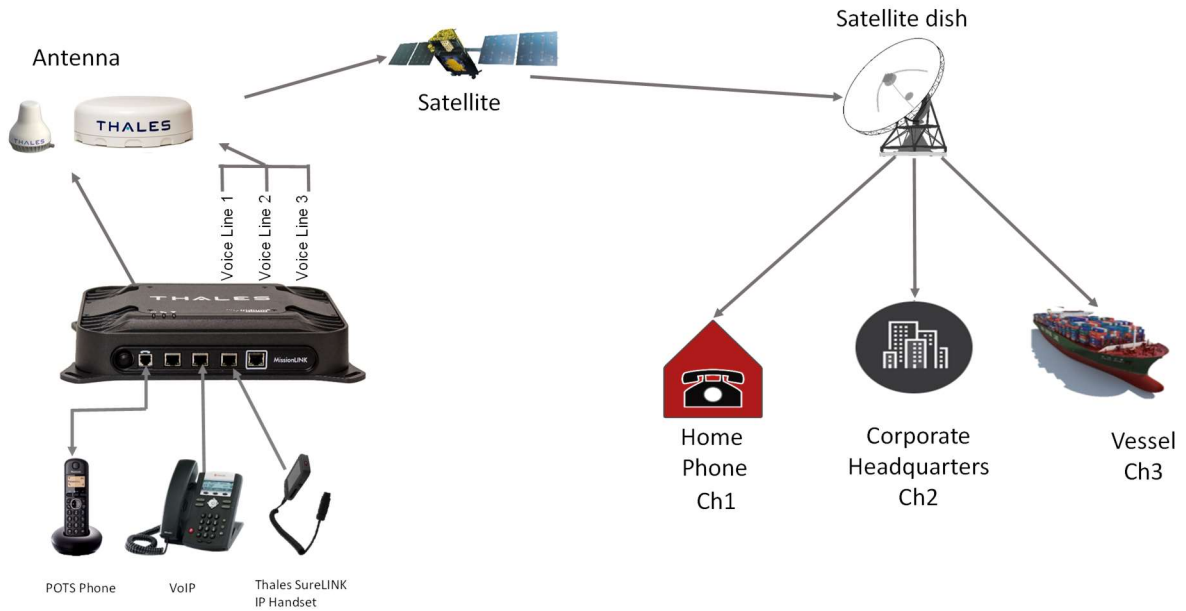
Figure 2-1 Calling Overview for Three Voice Lines

Primary System Features (for both Certus 350 and Certus 200 systems)

- Embedded 802.11b/g/n Wi-Fi access point with up to three (3) simultaneous users.
- Intuitive Management Portal user interface for configuration, monitoring and system status.
- Application Programming Interface (API) for local and remote management and issue resolution.
- Private Branch Exchange (PBX) functionality provides extensions for free local calling through the terminal. (Figure 2-2).
- Least Cost Routing automatically routes the data to an optional, lower cost network (i.e., cellular, Wi-Fi, etc.).
- Iridium Messaging Transport® (IMT®) for subscription-based IoT messaging over the Iridium network.
- Secondary Data Flows (SDF) maps specialized data services to physical ports
- GNSS capability allows configuration of multiple satellite constellations including GPS, GLONASS, Galileo and Beidou for precise autonomous geo-spatial positioning
- Low profile, IP66/IP67 (Certus 350/Certus200) rated antenna with single RF cable to the Terminal Unit (TU).
- Magnetic mount kit for easy antenna installation.
- Radio Gateway feature enables Land Mobile radios to access the satellite voice network.
- Ruggedized tethered Thales SureLINK IP Handset provides reliable, remote system configuration, monitoring and voice calls (optional).
- Supported WEB Browsers:
  - Chrome
  - Safari
  - Firefox
  - Android
  - iOS (Safari)

Microsoft WEB Browsers are not supported.

NOTE
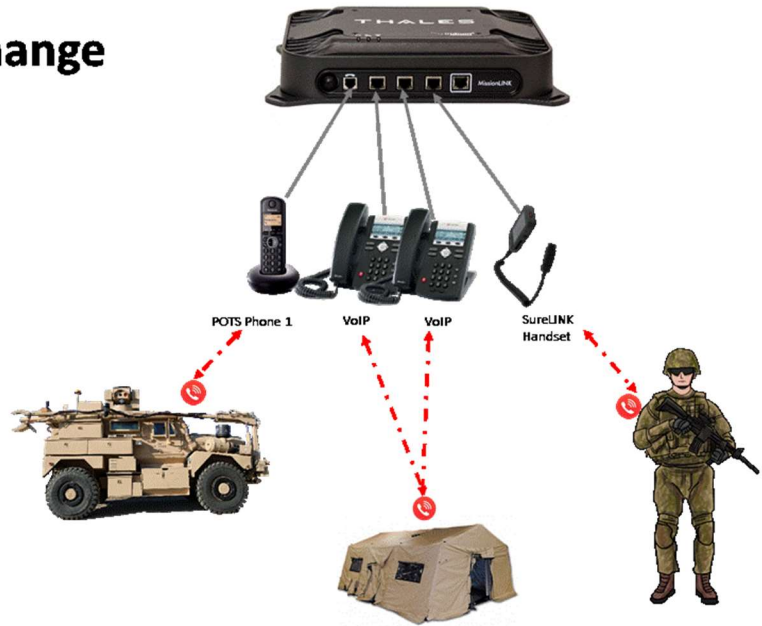
Figure 2-2 Local Communications via PBX Functionality

A typical user setup that includes standard kit items, accessories and user provided items such as a POTS phone, VoIP phones and a computer is shown in Figure 2-3. A cellular modem or other network modem can be connected to the WAN port for data least-cost routing operations. Voice calls are always routed through the Iridium satellite system and not the WAN port.
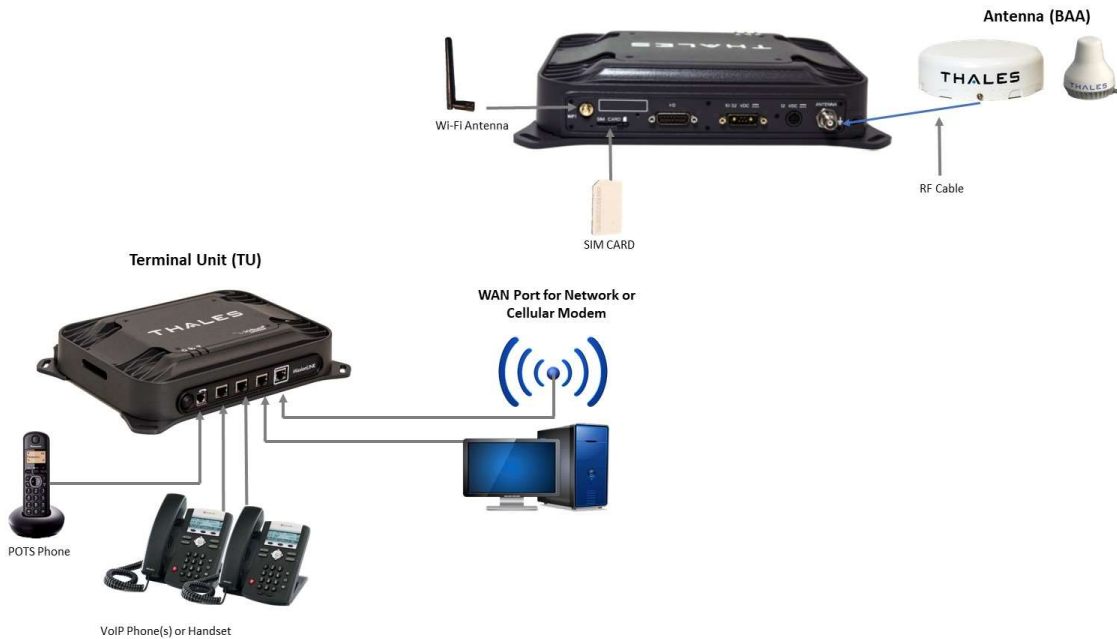
Figure 2-3 MissionLINK System with Connected Hardware

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 and Voice over IP (VoIP) calls. Three RJ-45 Ethernet connectors and one RJ14 connector 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 either a DC power cable with a 10-32V input range and remote start wire or an AC/DC power supply, accommodating all types of vehicles, applications and power sources.

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.
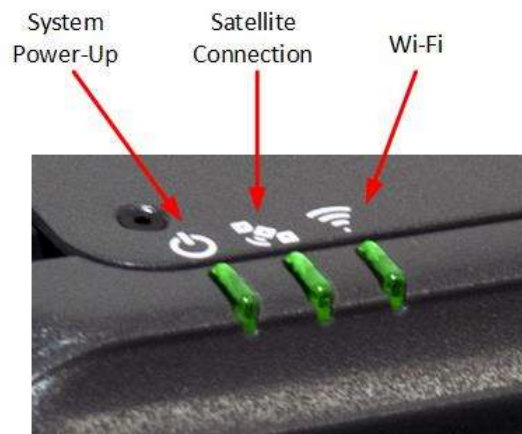
Figure 2-5 Terminal Unit (TU) LEDs

Table 2-1 Terminal Unit LED Status

Indicator	Description
⏻ **System**	
Solid GREEN	System functioning properly
Flashing GREEN	System busy (Booting up)
Solid YELLOW	Warning (functioning but minor issue)
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)
Solid MAGENTA	Defective System
Satellite	
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)
Wi-Fi	
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: Operational
Flashing Green: Start-up or in progress of configuring or acquiring service
Solid Yellow: System is operational but a minor issue should be addressed
Solid Red: Fault requires user attention (Open Management Portal for Alerts)
Flashing Red: Critical fault requiring immediate attention. For additional information, refer to Chapter 6 Troubleshooting
Solid Magenta: Defective system. For additional information, refer to Chapter 6 Troubleshooting.

The Terminal Unit front panel (left to right) has a main power button, one RJ-14 connector for POTS (Plain Old Telephone Service) Phone(s), three PoE (Power over Ethernet) RJ-45 connectors for VoIP phones or Ethernet-based devices, and one WAN (Wide Area Network) connector primarily used to connect an external cellular modem or VSAT.
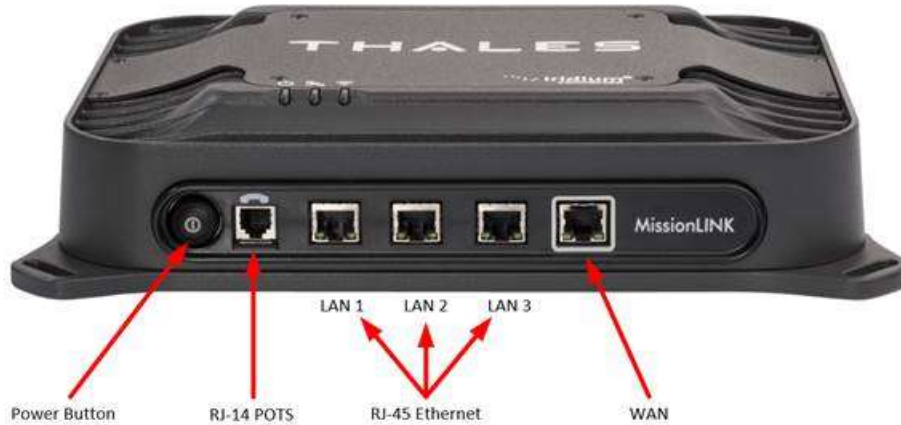
Figure 2-6 Terminal Unit (TU) Front Panel Detail

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

Figure 2-7 Terminal Unit (TU) Back Panel Detail

Broadband Active Antenna (BAA)

The BAA is a separate 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 through the single coaxial cable.

Figure 2-8 Broadband Active Antenna (BAA) Unit for Certus 350 and Certus 200 Systems

RF COAXIAL CABLE INSTALLATION CONSIDERATIONS

Good quality RF coaxial cable is recommended. Several considerations must be taken into account concerning the cable when installing a MissionLINK system. These include:

- **RF Cable loss** - The MissionLINK system is designed to operate with an RF cable loss of 10 dB or less in the L-band frequency of operation (1616-1626 MHz). Thales accessory cables listed below have been selected to meet this criteria.

- **DC losses due to cable resistance (inner conductor and shield)** - The MissionLINK system is designed to work with a maximum total RF cable ohmic resistance of 1.10 Ohms round-trip (inner conductor and shield). Thales accessory cables listed below meet this criteria.

- **Cable length** - The maximum cable length that the MissionLINK can operate with is 50 meters due to the delay requirements of the system. The maximum Thales cable length accessory cable is 50 meters in length.

Table 2-2 Coaxial Cable List

Cable	TDSI Part Number
10 foot TWS-240	855021-010
20 foot TWS-240	855021-020
30 foot TWS-250	855021-030
50 foot TWS-240	855021-050
100 foot TWS-240	855022-100
25 meters LMR-300 FR	855023-082
50 meters LMR-400 FR	855033-164

NOTE The last two cables are Fire Rated (FR) providing resistance to fire and continued operation in the presence of fire, improving safety when being used.

CHAPTER 3   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 button, one RJ-14 connector for POTS (Plain Old Telephone Service), three PoE (Power over Ethernet) RJ-45 connectors for VoIP phones or Computers, and one WAN (Wide Area Network) connector. Refer to Figure 3-1 for location of the connectors.
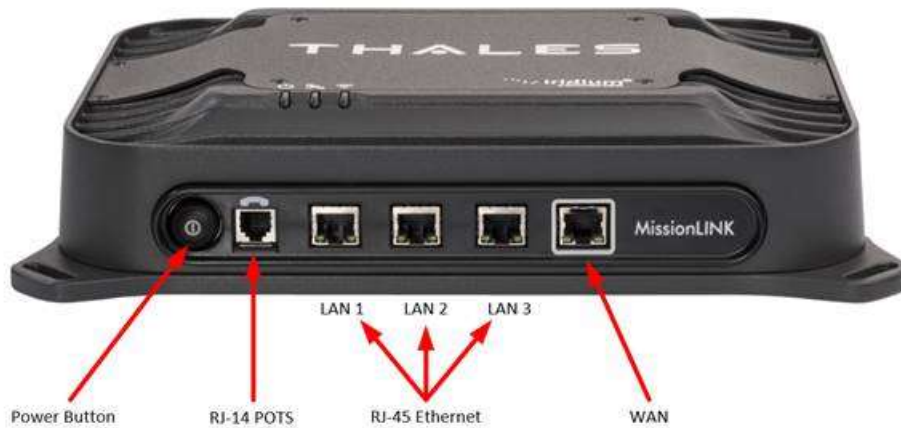
Figure 3-1 Terminal Unit (TU) Front Panel Detail

POTS Phone connection
By default, the POTS Phone(s) are pre-configured to use the first two Iridium voice lines without any additional configuration.

The TU can accept up to two (2) POTS Phones connected with 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). Note that single, molded plastic piece RJ-14 Splitters (triplex jacks) will not fit into the POTS phone connector. It is recommended that a POTS Splitter be used that includes a short phone cord that fits into the TU POTS connector.

VoIP or Thales SureLINK IP Phone connection
By default the TU has three (3) extensions preconfigured for use with POTS phones, VoIP phones, or Thales SureLINK IP Handsets, as shown in Table 3-1.

If using a VoIP phone, Thales recommends CISCO SPA504G and Grand Stream GXP2140 models for use with Thales MissionLINK. Other brands and models may work but have not been tested by Thales.

Follow your VoIP phone configuration guide to setup the VoIP phone and connect to the TU using the following parameters. For detailed VoIP phone setup see Chapter 4, VoIP Phone Settings.

Table 3-1 Typical VoIP Phone Configuration

Extension 1: (will make and receive calls on line 1 of your SIM)	User: "1001" Password: "1001" Host: "sip.thaleslink" Protocol: udp
Extension 2:(will make and receive calls on line 2 of your SIM)	User: "1002" Password: "1002" Host: "sip.thaleslink" Protocol: udp
Extension 3:(will make and receive calls on line 3 of your SIM)	User: "1003" Password: "1003" Host: "sip.thaleslink" Protocol: udp

NOTE By default, extensions 1 and 2 are mapped to POTS phone connections and Extension 3 is flexible. A VoIP phone can be configured to any extension even those assigned to the POTS lines. The SureLINK IP Handset will have a default of 1002 or extension 2, so it will automatically work the same as the first POTS line.

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 back plate of the TU. This IMEI can also be found in the http://portal.thaleslink (or https://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 (or https://portal.thaleslink)under the STATUS→ SIM tabs. (SIM must be inserted).

NOTE Using https:// allows for secure connections between the TU and the computer viewing the Thales Management Portal.

3-1
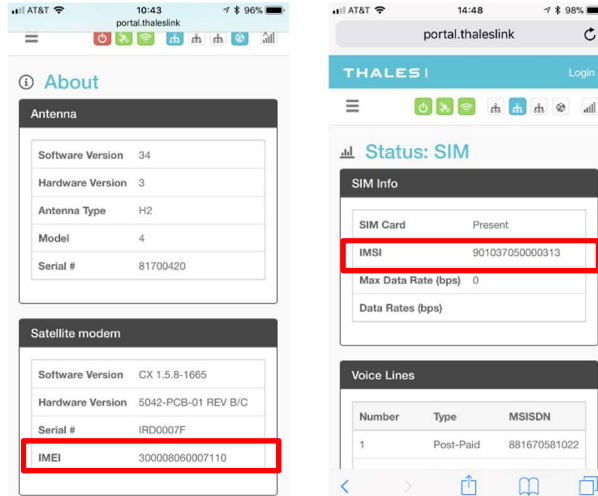
Figure 3-2 MissionLINK IMEI and IMSI from Mobile Device

STEP 3: Install SIM

1. Open the SIM Card protective cover by pulling it away from the TU, exposing the SIM card slot. (Figure 3-3).

Figure 3-3 SIM Card with Cover Opened

2. Install SIM card from Air-time provider (1, Figure 3-4), by inserting the card with contacts down (2) until it clicks into place (3).

3. Be sure to engage the lock for the SIM Card (4).

Figure 3-4 Installing SIM Card and Engaging the Lock

4. Secure the SIM Card cover once the SIM Card has been locked into place to prevent moisture or dust intrusion. (Figure 3-5)

Figure 3-5 Secure the SIM Card Cover

STEP 4: Power the MissionLINK unit.

Before powering the unit, make sure the DC power cable is connected to a 10-32VDC source, the polarity is correct, and the DC cable is securely connected to the TU. If using the AC/DC power supply, connect one end to the terminal's 12V DC input and connect the power cord to a 120 or 240V AC outlet. The antenna must also be connected per the corresponding system installation manual. Power the unit by pressing and releasing the power button on the TU (Figure 3-1). NOTE: After the button is pressed and released, a few seconds pass before the System LED (left) starts flashing. It may take a few minutes on initial startup for all three LED's on the unit top to turn solid GREEN (middle LED may turn BLUE). You may see an occasional red LED during power up. This is normal. Refer to Table 3-2 for more information on the status LEDs.
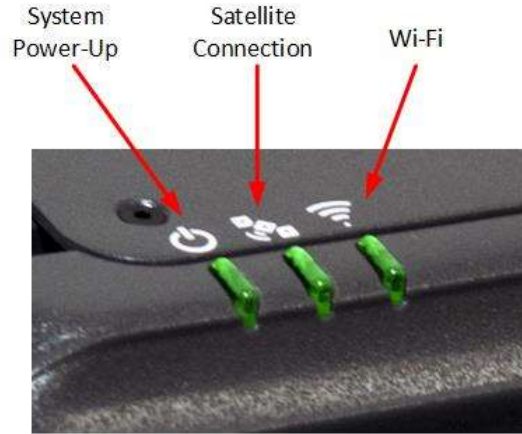
Figure 3-6 System, Satellite and Wi-Fi Status LEDs

Table 3-2 Terminal Unit LED Status

Indicator	Description
⏻ **System**	
Solid GREEN	System functioning properly
Flashing GREEN	System busy (Booting up)
Solid YELLOW	Warning (functioning but minor issue)
Solid RED	Fault (minor issue)
Flashing RED	Critical fault (major issue)
Solid MAGENTA	Defective System
Satellite	
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)
Wi-Fi	
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.

<table>
<tr>
<td>

(i)

NOTE
</td>
<td>
Thales uses a self-signed certificate for encryption between the terminal and the browser when viewing the Management Portal (https://portal.thaleslink). A self-signed certificate is a security certificate that is not signed by a certificate authority (CA). As such, a user will experience a warning in their browser before the keys are exchanged. The warning is different between browser types. Thales recommends you accept the risk posed by the browser. The browser will use HTTPS without warning until the key is either deleted or expires.
</td>
</tr>
</table>

Reference Figure 3-7. 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 few minutes).
2. On the wireless device, find and select the SSID ThalesLINK as an available Wi-Fi access point. No password is required on initial setup and is left to the user to add WPA2 protection with a password during this configuration process.
3. Open a browser and type: http://portal.thaleslink (or https://portal.thaleslink) (do not type .com or any other extension)
4. As a default, no changes to setup are necessary, but advanced users may want to configure their preferred system settings.
5. Once the Management Portal opens, click LOGIN button. Enter "admin" for Login ID and Password.
6. At this time, it is advised that you change the Management Portal admin password. To change password: Go to SETTINGS →GENERAL and change the password for the "Admin" user. A strong password is required that is at least 8 characters with a lowercase letter, an uppercase letter, a number, and a special character.

Option B: Via (PC, Mac or Linux) Ethernet connection
1. With your computer, connect the Ethernet RJ-45 Cable (included) to any of the 3 Ethernet ports on the TU. (Shown on Figure 2-6) (Do not connect to the WAN port identified on the TU with a box around the port.)
2. Via the network settings on your computer's operating system, enable the MissionLINK connection.
3. Open a web browser and type: http://portal.thaleslink (or https://portal.thaleslink) (do not type .com or any other extension)
4. As a default, no changes to setup are necessary, but advanced users may want to configure their preferred system settings.
5. Once the Management Portal opens, click LOGIN button. Enter "admin" for the Login ID and Password.
6. At this time it is advised that you change the Management Portal admin password. To change password: Go to SETTINGS → GENERAL and change the password for the "Admin" User. A strong password is required that is at least 8 characters with a lowercase letter, an uppercase letter, a number, and a special character.

NOTE If you forget the Wi-Fi WPA2 password or the admin 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. All custom configuration settings will be lost.
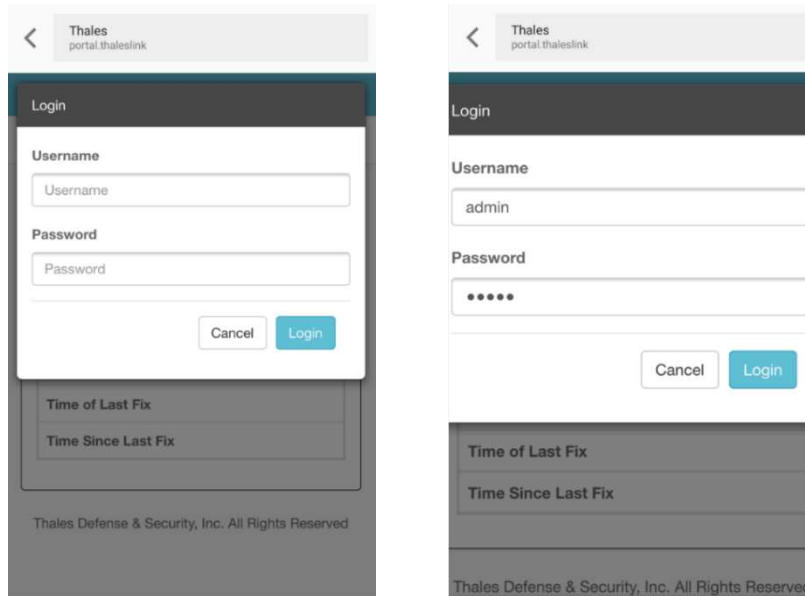
Figure 3-7 MissionLINK User Interface Login

STEP 6: Place a phone call.

NOTE The MissionLINK system contains Private Branch Exchange (PBX) functionality, where both local calls and outside calls can be made. Local extensions can be dialed directly from another local phone, but outside calls require dialing a "9" in order to connect to an outside line prior to dialing the phone number (unless disabled from the Management Portal).

1. Choose either POTS or VoIP handset.

2. Lift the handset from the base and listen for a dial tone.

3. For all calls using the Iridium Voice Services, dial 9 before the phone number. When making a local call, simply dial the extension.

4. Call a known number to test call and voice clarity

Call the Iridium automated message: (9) 1-480-752-5105

STEP 7: Access the Internet.

Once your device has successfully connected to the TU, open the Management Portal http://portal.thaleslink (or https://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.
- Data is defaulted off from the factory. To enable data, login and click the "ACTIVATE" button by enable session on the Dashboard tab.
- Check that the antenna has a clear view of the sky or check the alerts if voice calls or data fail.

Try loading a small website such as www.google.com to verify your internet connection. If the page loads successfully you are ready to browse the internet.

CHAPTER 4   THALES MANAGEMENT PORTAL

NOTE

To access the Management Portal from a laptop:
- Power on the Thales MissionLINK TU and let it boot up (may take a few minutes)
- Open a web browser
- Type: http://portal.thaleslink (or https://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). A strong password is required that is at least 8 characters with a lowercase letter, an uppercase letter, a number, and a special character.

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 few minutes)
- On the wireless device, find and select ThalesLINK as an available Wi-Fi access point.
- Open a browser and type: http://portal.thaleslink (or https://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). A strong password is required that is at least 8 characters with a lowercase letter, an uppercase letter, a number, and a special character.

GETTING TO KNOW THE THALES MANAGEMENT PORTAL

The Thales Management Portal is a Graphical User Interface (GUI) 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, desktop computers, and the optional Thales SureLINK IP Handset. Restrictions apply on browser type and version. 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. There are five access levels to the system. Four of them are under password control.

- 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 third local access is for configurable users who are created by administrators. These users can view data and make configuration changes within the permissions they are given. Configurable users can be created with or without remote access.
- The first remote access level is for remote users who need to monitor 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 opened, 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 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", the remote administrator is denoted by "wan_admin", and any configurable users are denoted by their username. By password control, the local system administrator can enable or prevent any remote access to the system.

Administrators, after initially logging in to the admin account with default 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 for added security and protection. A strong password is required that is at least 8 characters with a lowercase letter, an uppercase letter, a number, and a special character.

The administrator can create and configure up to two users and determine what access groups these users have permissions for. These users, after logging in, can view data and make changes

within the access groups that they are given permissions for. These users can change their own password but no other passwords. A strong password is required. The administrator can delete users when they are no longer needed.

In the following pages, the Thales Management Portal is described in detail. When referring to the administrator/admin, it can include any configurable users that have permissions for the correct access group. 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.

- Dashboard – Provides information relating to any current Alerts and Services.
- Status – Provides status of each of the items listed below. These informational screens cannot be edited.
  - Current Devices
  - GPS
  - LAN
  - Phones
  - Services
  - SIM
- Alerts – Provides a listing of system alerts
- Calls – Provides current calls, call history, and call management.
- Emergency – Allows the operator to send an emergency message.
- Iridium Messaging – Enables the Administrator to send messages via Iridium Messaging Transport® (IMT®).
- Settings – Enables the Administrator to configure the system.
- 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 a self-test, check system status, and view the diagnostics log.
- 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)).

NOTE Depending on the web browser being used, you may see a message that says NOT SECURE. If you type https://, this message will go away. This message does not affect operation of the management portal.

Menu Components

The System Status Icons at the top of the screen, highlighted in Figure 4-1, provide system level information at a glance. When selected, these icons provide addition screen(s) of information and a quick way to make certain configuration setting changes by the administrator.
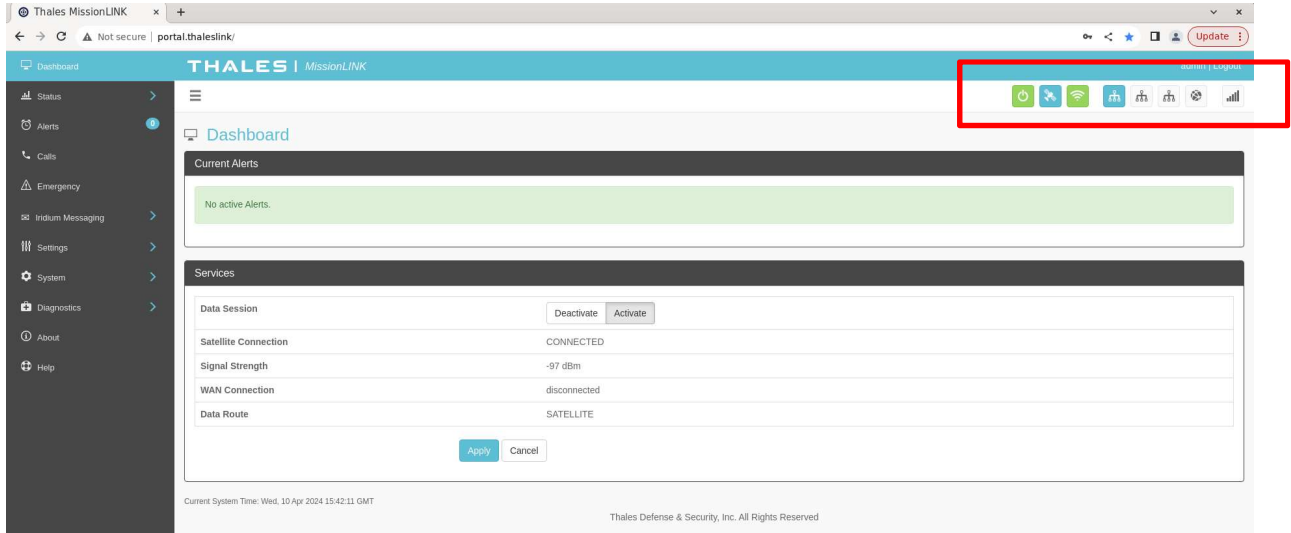
Figure 4-1 Quick Link Icons

> **NOTE** Status icons on the GUI may lag those on the TU, due to the GUI refreshing every 10 to 15 seconds.

Table 4-1 Quick Link Icons

ICON	Description
	System Status
	Satellite Status
	Wi-Fi Status
	LAN 1, 2, and 3 Status
	WAN Status
	Satellite 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 4-2.
    - o STATUS shows the current condition of the system.
    - o UPTIME indicates how long the terminal has been in use.
    - o The RESTART button allows an administrator to reboot the terminal.
    - o The SHUTDOWN button allows and administrator to shut down the TU, but this will require manual action to turn the BDU back on.
    - o Selecting VIEW ALERTS opens the ALERTS window and displays any Current Alerts.
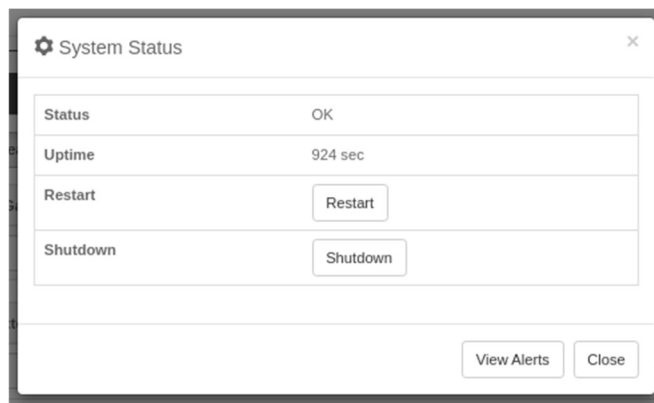
Figure 4-2 Quick Link – System Status

**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 can login to the GUI by reentering 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 4-3, 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.
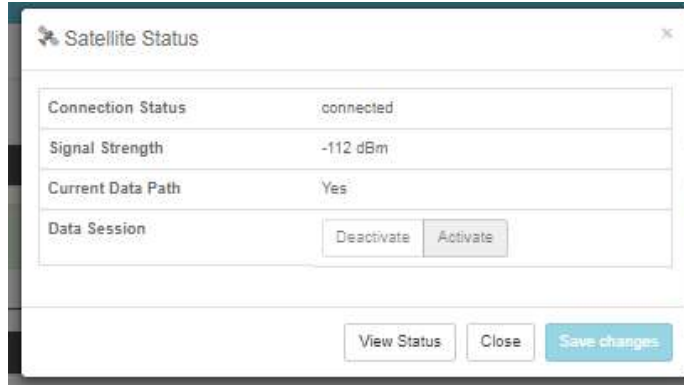
Figure 4-3 Quick Link – Satellite Status

- Wi-Fi Status – The Wi-Fi Status icon (Figure 4-4) 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.

> **i**
> **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.
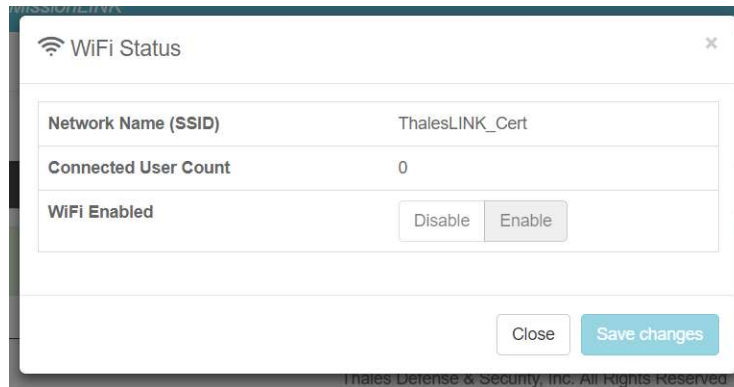
Figure 4-4 Quick Link – Wi-Fi Status

- 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 4-5 is shown, displaying the "Link Status" and allowing for turning the Power over Ethernet (PoE) ON or OFF for that LAN, as well as enabling or disabling the PAN port. Only LAN 2 and 3 can be disabled. LAN port 1 is always enabled to prevent a situation where

the terminal cannot be accessed. Changes will only take effect once SAVE CHANGES is selected.
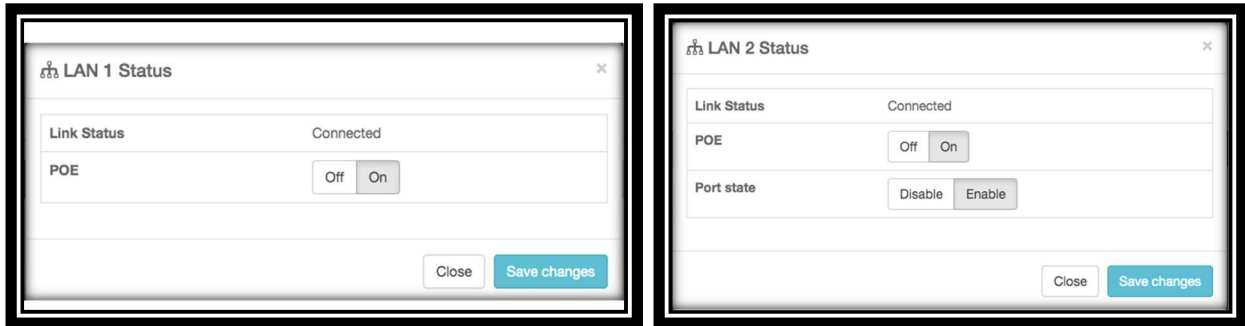
Figure 4-5 Quick Link – LAN 1and Lan 2 Status (LAN 3 similar)

- 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 4-6 is shown. The details provided on this screen are for information only and include WAN PORT STATE, INTERNET CONNECTION, and CURRENT DATA PATH.
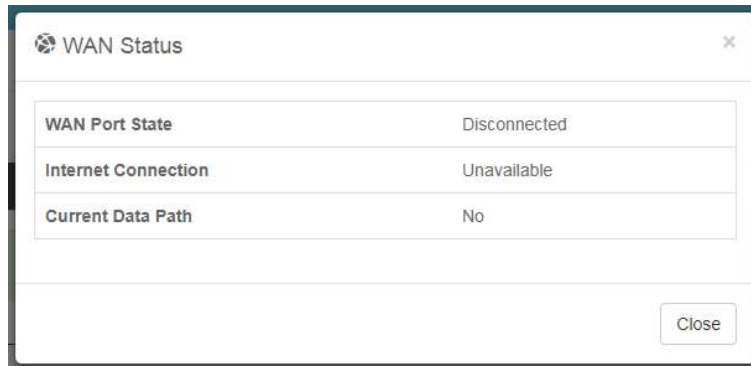
Figure 4-6 Quick Link – WAN Status

- 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 (or https://portal.thaleslink) into a supported web browser, the Dashboard screen comes up by default. The Dashboard can also appear by selecting the top menu item highlighted in blue in Figure 4-7. From the Dashboard, you can see information relating to:

- Current Alerts
- Services
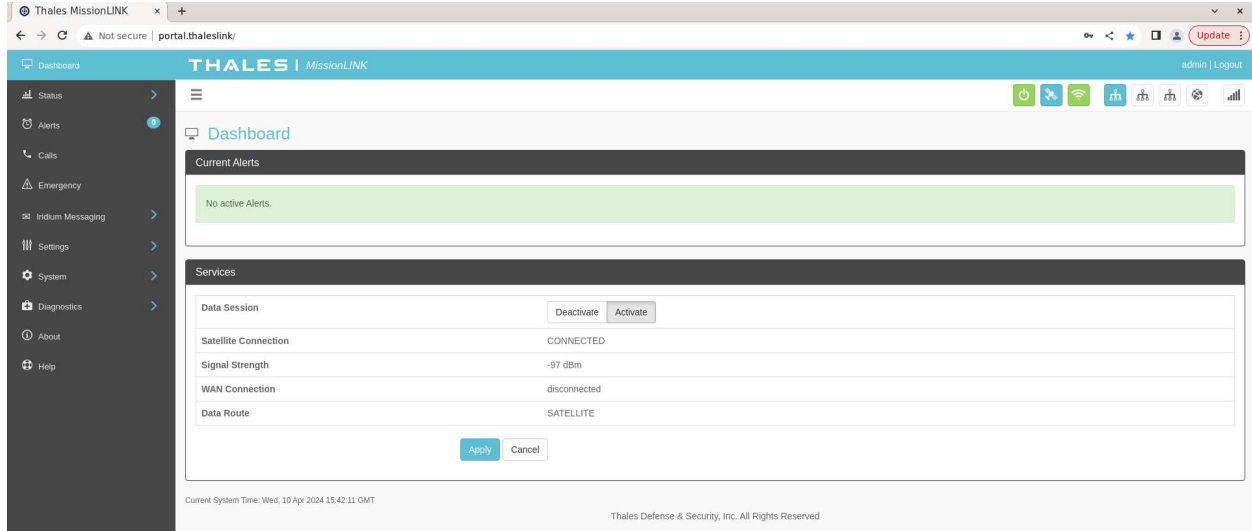
Figure 4-7 Thales MissionLINK Dashboard - Main Screen

Table 4-2 Thales MissionLINK Dashboard - Main Screen

Section	Value	Description
Current Alerts (When shown on dashboard)		
Alert Name	Text	Provides information relating all system issues summarized for easy reporting and debug/troubleshooting. For additional information, refer to Chapter 6 Troubleshooting
Services		
Data Session	Deactivate or Activate	Allows the admin to activate or deactivate the Data Session.
Satellite Connection	Disconnected, Connected, Access, Acquisition, and Idle	Displays the current status of the system when 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
Data Route	Satellite or WAN	Displays the data route

Status

![NOTE icon]

NOTE The STATUS selection screens (CURRENT DEVICES, 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.
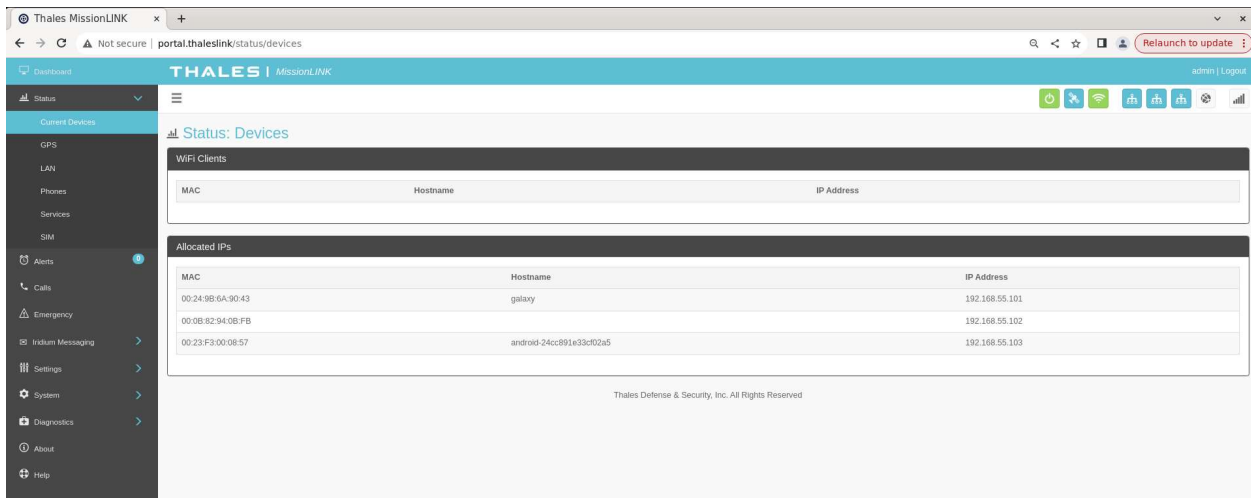
Figure 4-8 Status → Current Devices Screen

GPS

The GPS page provides detailed GPS information as shown in Figure 4-9.
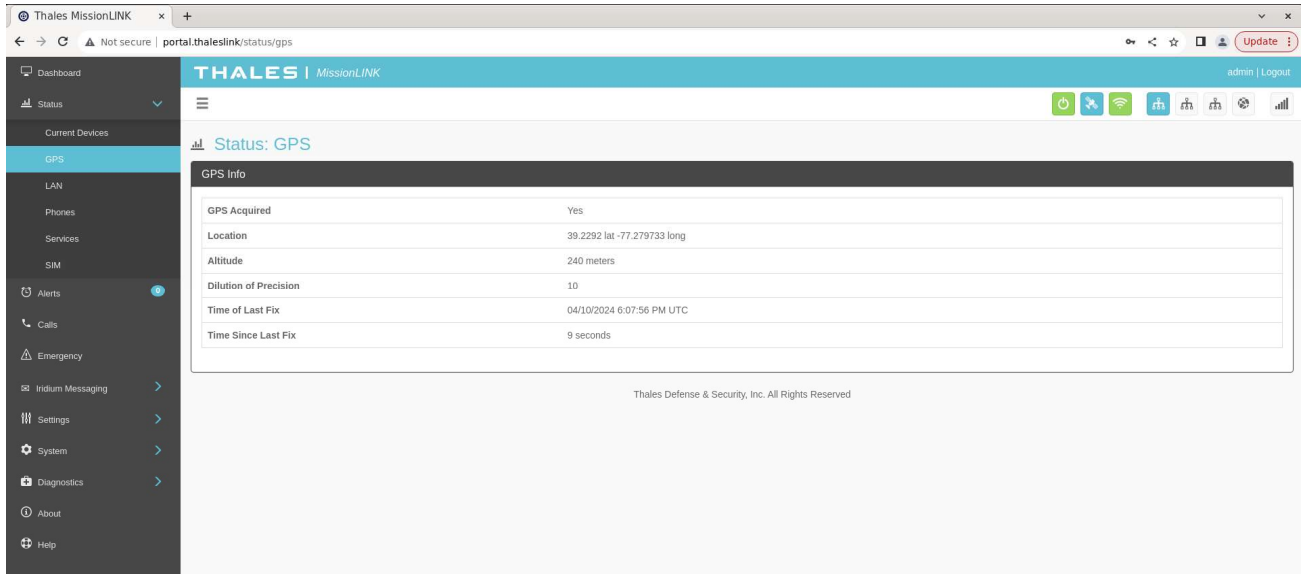
Figure 4-9 Status → GPS Screen

LAN

The LAN page displays the connection status of the built-in Wi-Fi access point and the LAN ports as shown in Figure 4-10.
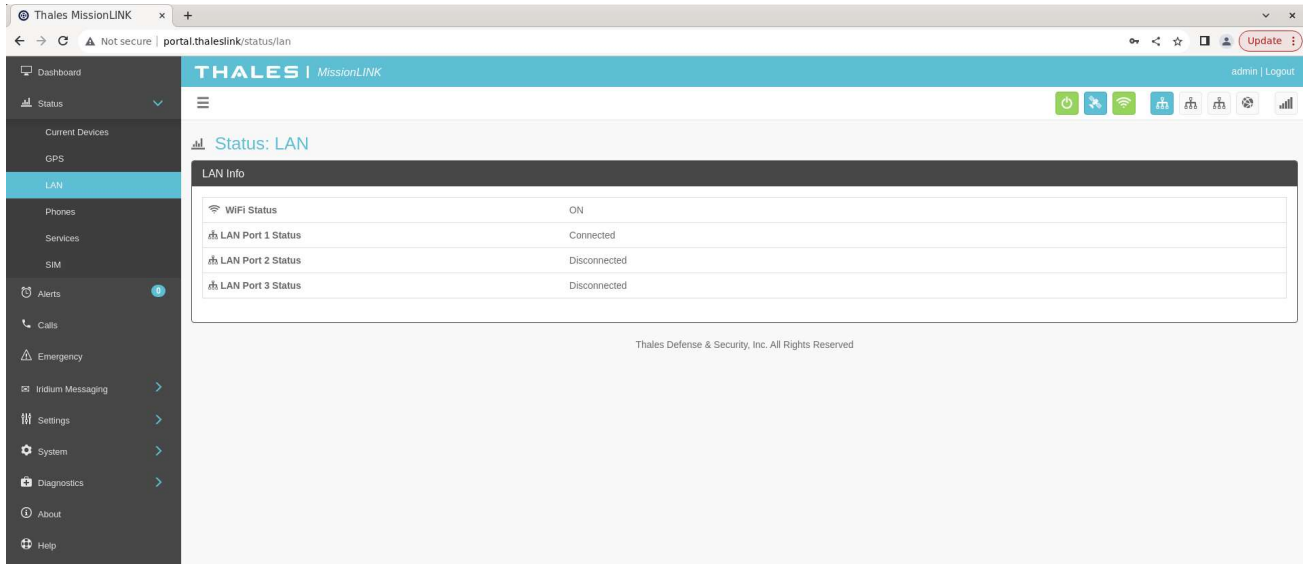
Figure 4-10 Status → LAN Screen

User Manual PN 84468 Rev N

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 4-11.
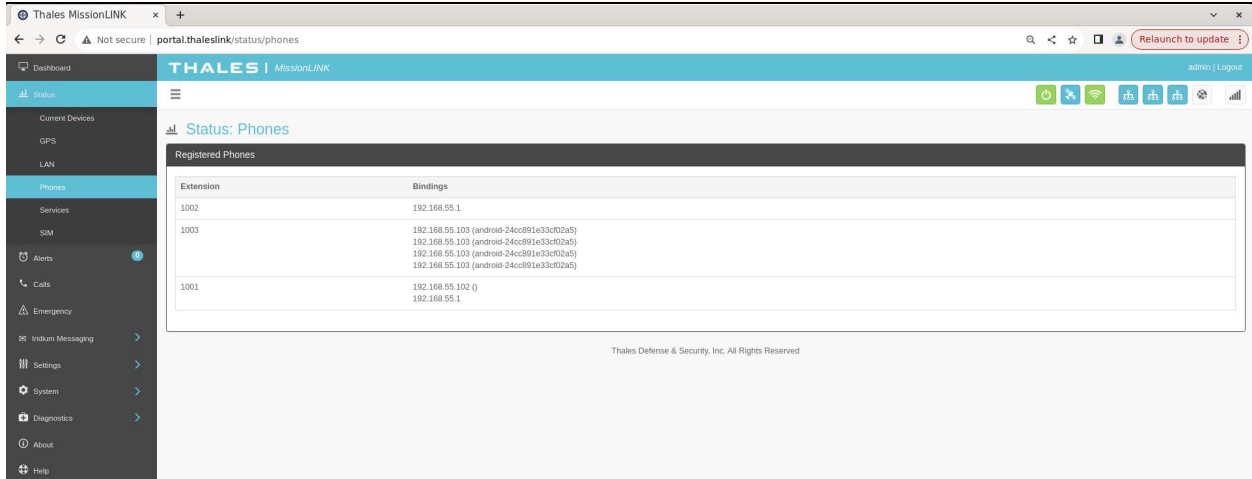
Figure 4-11 Status → PHONES Screen

Services

The Services page provides the status of Satellite and WAN networks, and the current data route as shown in Figure 4-12.
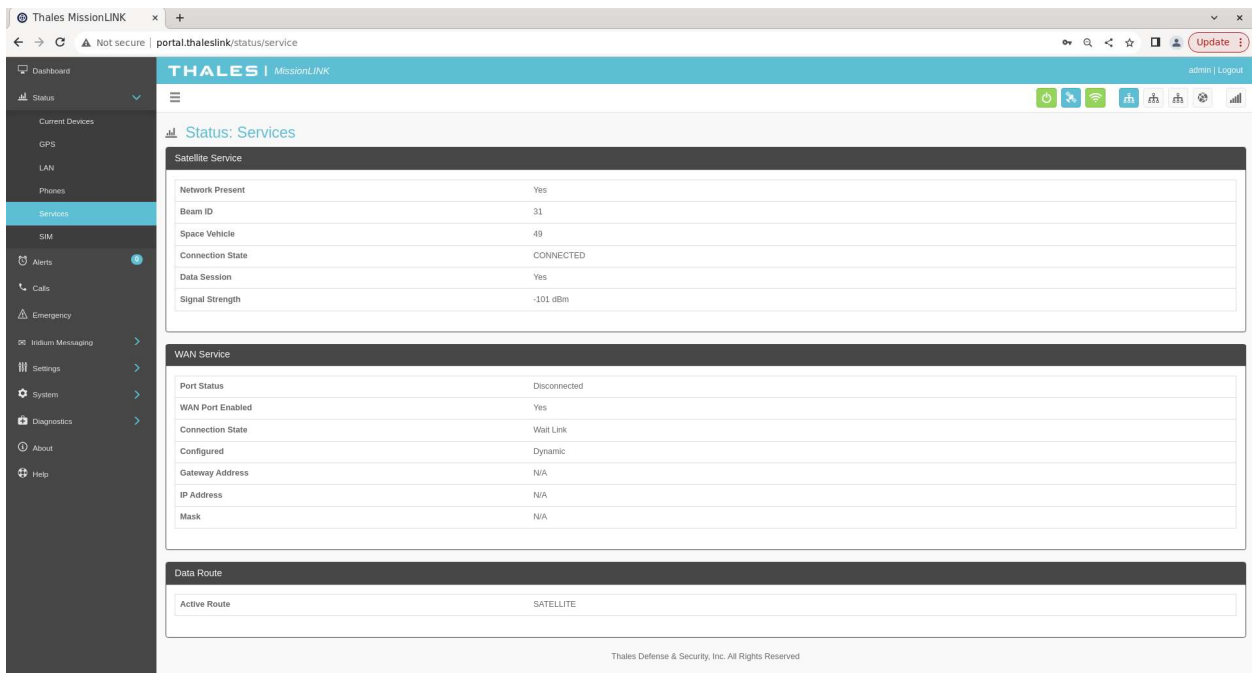
Figure 4-12 Status → *SERVICES Screen*

SIM

The SIM page (Figure 4-13) provides the following information:
- SIM Info – Status of the SIM card, its Unique IMSI ID number and its Private IP Address. The max data rate shows the Certus™ service level that the SIM card is provisioned to.
- Voice Lines – This section lists the dedicated Iridium voice lines (up to three), what type they are and what their MSISDN is.
- Secondary Data Flows (SDF) shows which are provisioned on the SIM and the Subnet they are on.
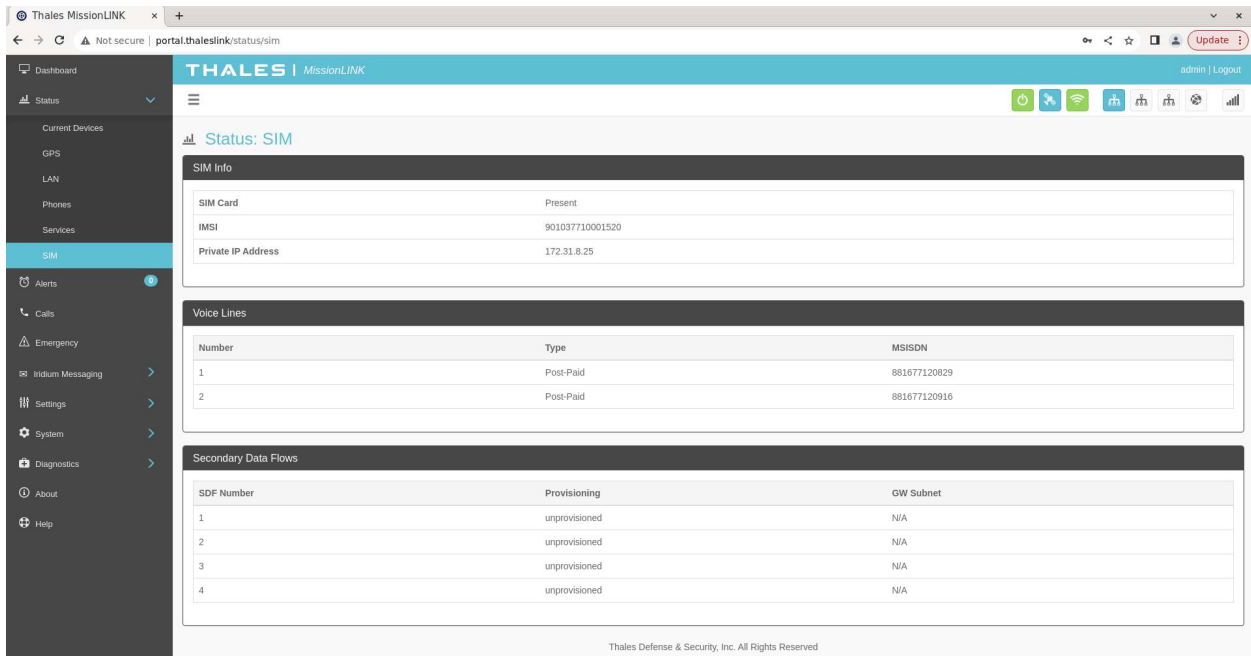
Figure 4-13 Status → *SIM Screen*

Alerts

The ALERTS screen displays a list of active Alerts from the system. If no alerts exist, the alert screen will indicate that there are no active alerts. (Figure 4-14)
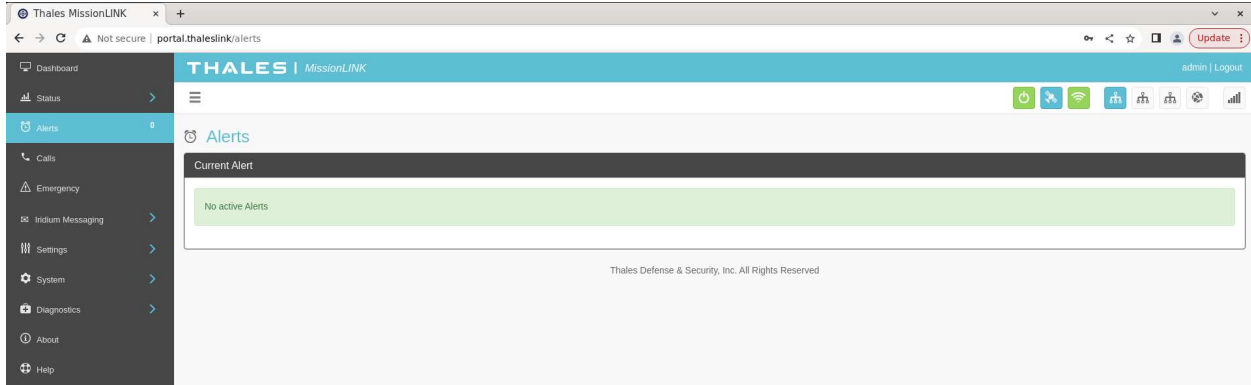
Figure 4-14 ALERTS Screen (Example Shown with No Active Alerts)

Alerts may be generated from a Power-On Self-Test (POST) or during normal operation of the system. (Figure 4-15) 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. (When cleared, the SYSTEM STATUS icon will turn GREEN.)
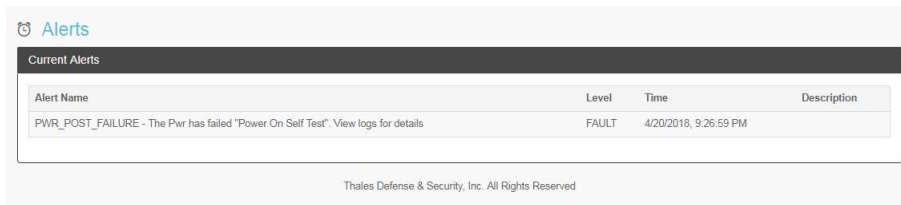
Figure 4-15 ALERTS Screen (Example Shown with Active Alerts)

 For additional information, refer to Chapter 6 Troubleshooting.

NOTE

Calls

Selecting the Calls menu item (Figure 4-16) displays the call logs for active and past calls.
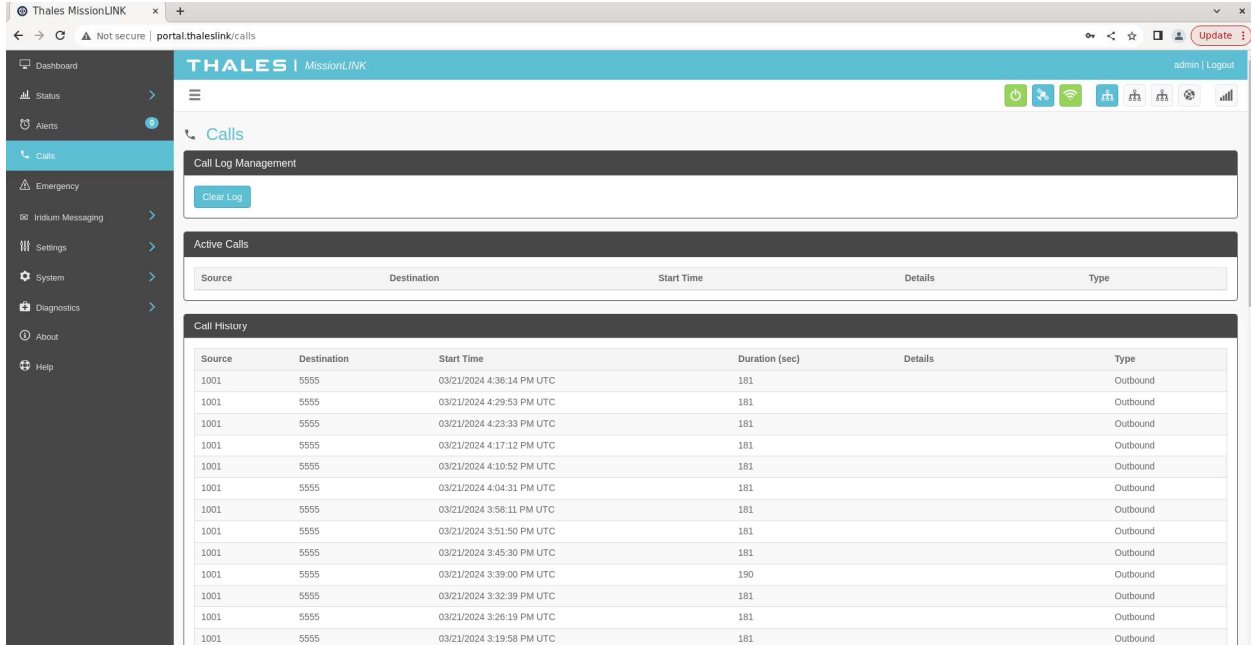
Figure 4-16 Call Log Screen

Under CALL LOG MANAGEMENT (Figure 4-17), the admin can CLEAR the call log by selecting CLEAR LOG and then confirming by selecting YES, CLEAR LOG.

Figure 4-17 Call Log Management - CLEAR Call Log

 CALL HISTORY displays the last 100 calls that were made.

NOTE

Emergency

 NOTE Emergency Messages can only be configured by the administrator. If the user is not logged in as ADMIN and selects MANAGE EMERGENCY, the user will see ⊘ icon, indicating this function is not available.

The Emergency Message (Figure 4-18) menu item allows for enabling and sending an emergency email message.

Selecting MANAGE EMERGENCY will open the SETTINGS → EMERGENCY screen (Figure 4-). From here, set up the Emergency 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 SETTINGS → EMERGENCY.
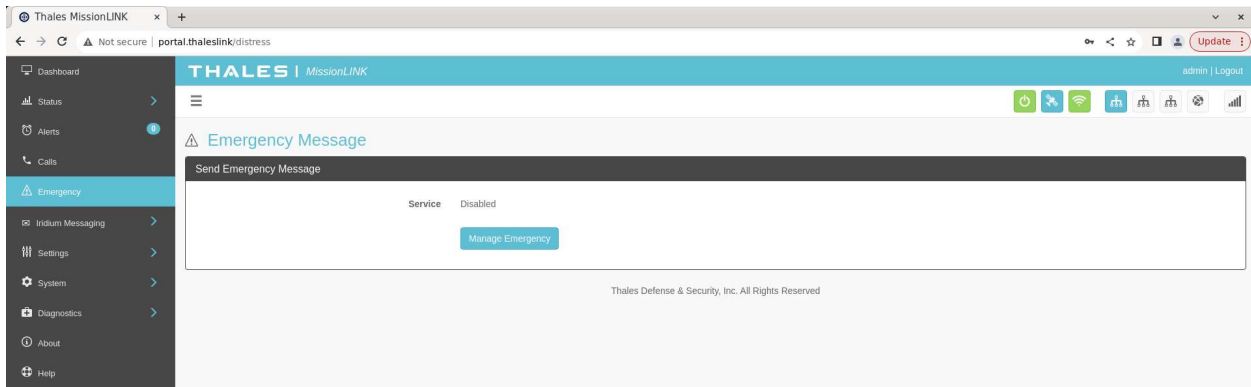
Figure 4-18 EMERGENCY (Disabled View)

Figure 4-19 EMERGENCY (Enabled View)

Sending an EMERGENCY MESSAGE:

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

Confirmation Required

Please confirm sending of emergency message

Yes, Send Emergency   No, Cancel
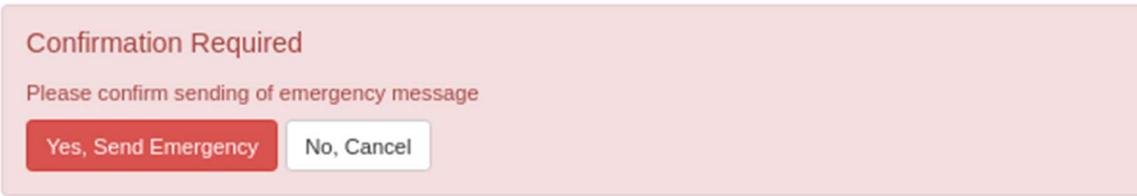
Figure 4-20 Confirmation Required – Send an Emergency Message

NOTE No external indication is given when emergency is activated. This discretion is for user safety in an emergency situation. The only indication of an emergency will be in Management Portal under Emergency menu item.

NOTE An emergency phone call can be made by using the optional Thales SureLINK IP Handset. Configuration of the phone number to be called, as well as, the activation and cancellation of the call takes place on the handset itself. Nothing is set up for the phone call through the Management Portal.

Iridium Messaging

Iridium Messaging Transport® (IMT®) provides customers small to moderate-sized IoT messaging through Iridium CloudConnect and offers industry standard protocols, programming, message topics and Pub/Sub capabilities through a wide range of Iridium Certus™ modules. More information can be obtained at https://www.iridium.com/services/iridium-messaging-transport/.

The Iridium Messaging tab of the portal enables users to send messages over Iridium Messaging Transport® (IMT®) and track outgoing/incoming messages since last reboot. To prevent unauthorized outgoing messages over IMT®, these pages are password protected.

Send Message

On the Send Message page, the admin can send a message using IMT®. Enter the required information shown in Table 4-3 then select SEND MESSAGE. A sending modal will appear and the message will be sent with a prompt indicating so. If any errors occur during this process that cause the message to be rejected and not sent, the page will indicate it.

Sending a message from this tab is one way of sending a message through IMT® with more ways being available by changing settings on the Settings IMT® page.
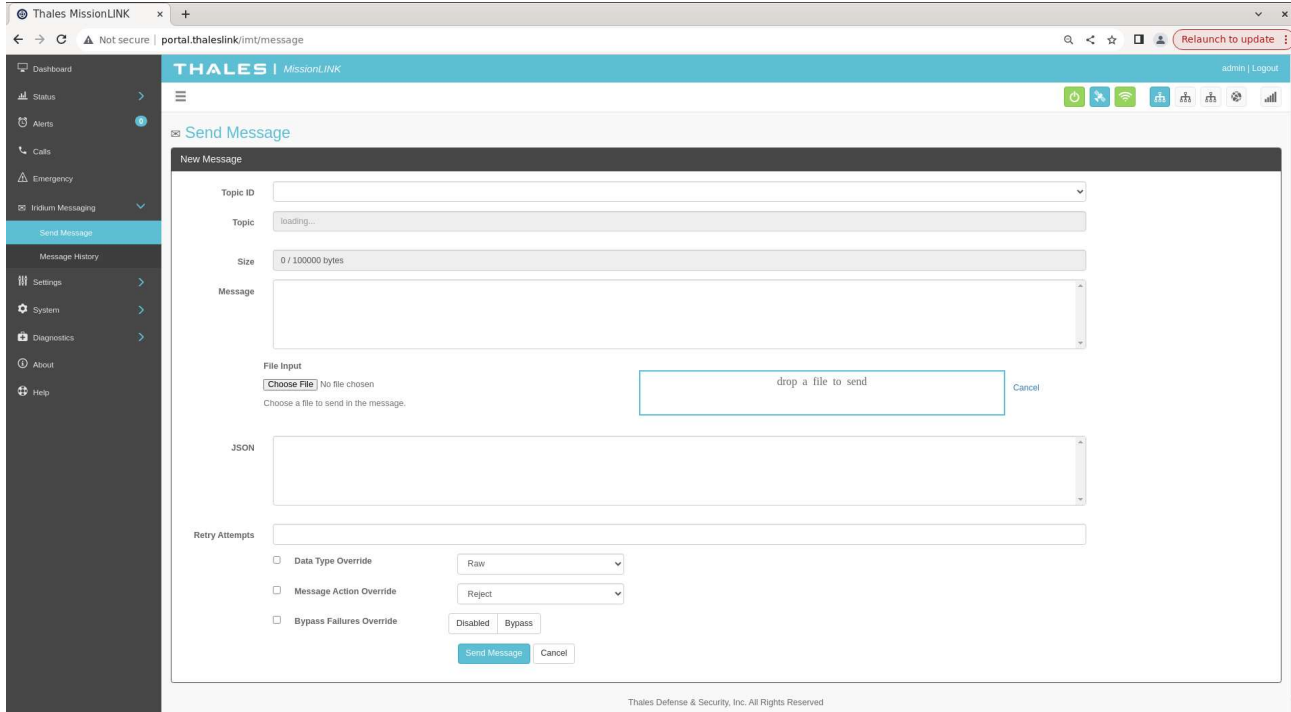
Figure 4-21 Iridium Messaging → Send Message

Table 4-3 Iridium Messaging → Send Message

Section	Required	Value
Topic ID	Yes	The Topic ID to which the message will be sent. A Topic may be subscribed to via your SIM. Contact the user's service provider for making Topic IDs available to the user's SIM.
Retry Attempts	Yes	The number of times to retry sending the message after failed attempts.
Message	Yes if JSON is empty	The text desired to be sent as an IMT$^®$ message. Note: If both the Message and JSON field contain text, the message text will be added to the JSON with the key "message".
JSON	Yes if Message is empty	Text representing a JSON (Java Script Object Notation).
File Input	No	A file can either be selected and loaded through the CHOOSE FILE button or by dropping a file onto the drop zone. These actions will convert the file into a base64 text which will be automatically put in the message field. The CANCEL link on the side may be used to remove a loaded file. **Important**: Sending a file requires the Data Type to be **RAW**. Either configure the topic to use RAW under Settings: IMT or select RAW from Data Type Override and ensure the checkbox is checked for Data Type Override.
Data Type Override	No*	An optional means to override the user configured default data type used for sending messages to this Topic ID. If a

Section	Required	Value
		user desires to override, click the selection box and select the data type desired from the dropdown. The default data type is configured on the Settings: IMT page. • RAW - This data type interprets the message as simply binary data. Submitting RAW data will require the user to convert the data into base64 characters for submission on the Management Portal. • MESSAGE - This data type interprets the message as encodable text. Default encoding used is ASCII. To use another encoding, configure the Topic under Settings: IMT® • JSON_LIST - This data type interprets the message as key value pairs from which it will create a JSON. The keys and values are determined by spaces. The message "key value" would thus be {"key": "value"}. * Data type is required if the Topic's Data Type in settings is not of type RAW, and a user desires to send a file. It is required for Data Type to be selected and the type needed would be RAW.
Message Action Override	No	An optional means to override the user configured default message action used during the sending process. If a user desires to override, click the selection box and select the message action desired from the dropdown. • REJECT- This message action will reject messages above 100 Kilobytes • TRUNCATE - This message action will truncate messages above 100 Kilobytes to 100 Kilobytes (only usable for Data Type MESSAGE). • MULTI_MESSAGE - This message action will break the message up into 100 Kilobyte sub messages. These sub messages will have an internal id recorded in each message along with a number representing count. **See figure <IMT SETTINGS FIGURE>
Bypass Failures Override	No	An optional means to override the user configured default bypass failures option. If a user desires to override, click the selection box and select the bypass failures option desired. When set to true, some failures which would normally cause message rejection during the sending process will be bypassed when possible.

Message History

The Message History page, shown in Figure 4-22, allows users to view active messages in transport and the logs of completed, cancelled, delivered, or rejected messages. The Active Message panel allows cancellation of outgoing messages so long as they have not been delivered. The Message History panel allows admin to redeliver messages to local targets when a topic is configured to support redelivery (see Settings: IMT). The Message Log Management panel allows for adjusting the messing history settings.

ⓘ
NOTE   Message history does not persist over reboots.
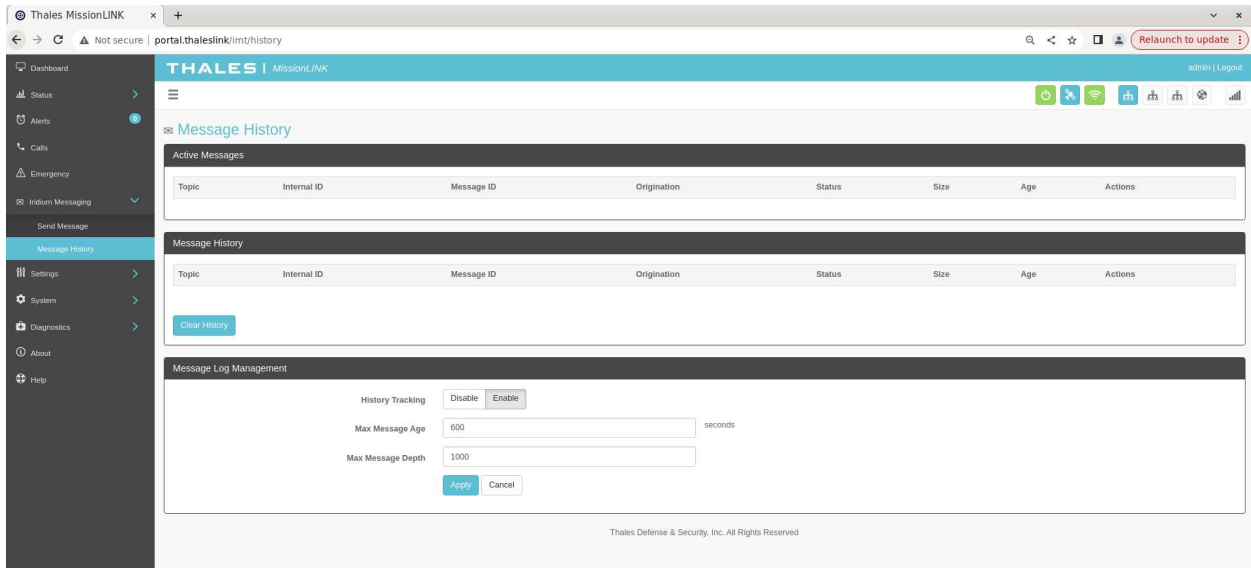
Figure 4-22 Iridium Messaging → Message History

Table 4-224 Iridium Messaging → Message History

Section	Value
Active Messages	
Cancel Message	Cancels the sending of an active message.
Message History	
Clear History	Clears all messages in Message History.
Resend Message	Present when a message is retained, configured on the Settings:IMT page.
Message Log Management	
History Tracking	Disabled / **Enabled** (**Enable** is the default settings)
Max Message Age	Time in seconds to hold a message in history. Messages whose age exceeds this time will be slated to be removed.
Max Message Depth	Maximum number of messages to report in history. Oldest messages will be removed first.

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.

<u>General</u>

From the General page, change passwords, enable (or disable) external API access, and create and edit configurable users as shown in Figure 4-3, Figure 4-24, Figure 4-25, and

Figure 4-24 Adding user screen

User Manual PN 84468 Rev N

Figure 4-25 Editing user screen

Table 4-5.

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

- GUEST: User only account, no password, read only access.
- ADMIN: Password capability, FULL access through the Thales Management Portal via local LAN (or wireless) connection.
- WAN ADMIN: Password capability, FULL access to all data and settings remotely via WAN port or over the Iridium network.
- WAN USER: Password capability, read only access to some API data remotely via WAN port or over the Iridium network.
- < Configurable User >: Created by ADMIN or WAN ADMIN, can change own password, limited access to settings based on permissions given via local LAN (or wireless) connection. Can be configured to also have remote access.

The admin can create up to two configurable users. Strong passwords must be given to the user at time of creation. Admins can deactivate/activate configurable users, as well as edit any parameters or delete the user after creation. Users cannot edit their own parameters other than password. Users can configure any parameters within the access groups that they are given. Please refer to Table 4-6 for details on each access group and what Management Portal page those settings are on. If no panel is specified, it indicates that all panels on that page are in that access group.

NOTE

The following default passwords for ADMIN, WAN_ADMIN, and WAN_USER are as follows:

Default Passwords:
    Username: admin   Password: admin
    Username: WAN_Admin   Password: NextAdmin
    Username: WAN_User   Password: IridiumUser

NOTE

It is recommended that passwords be changed from defaults for added protection and security. When changing the password from the default, a strong password is required that has at least 8 characters with a lowercase letter, an uppercase letter, a number, and a special character.
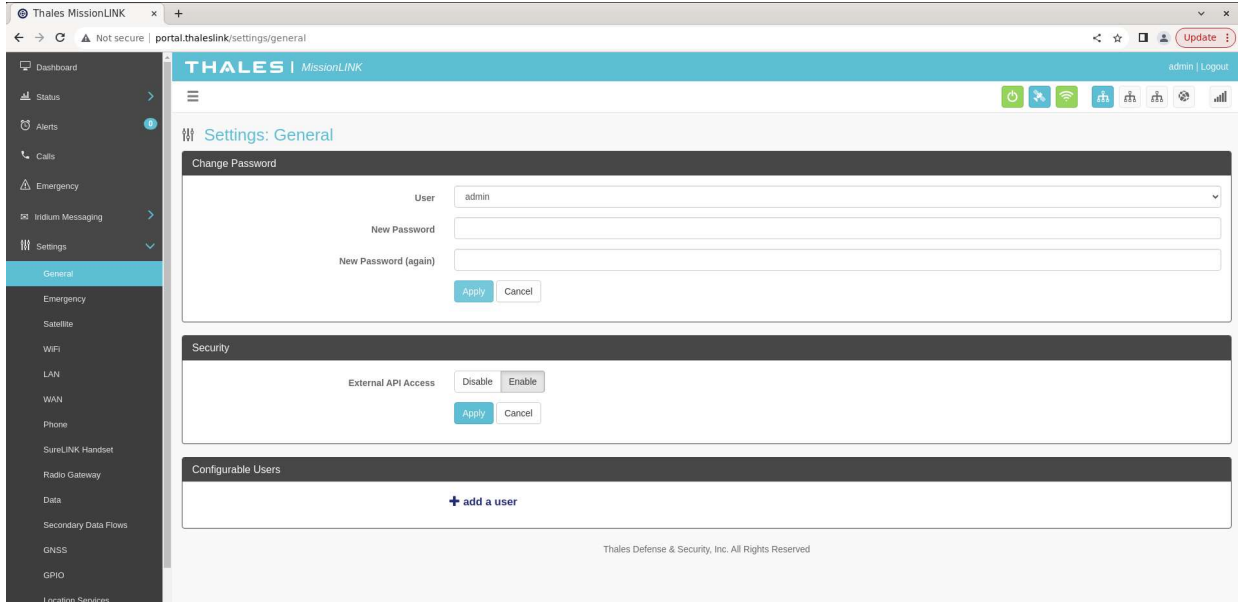
Figure 4-23 Settings → General Screen
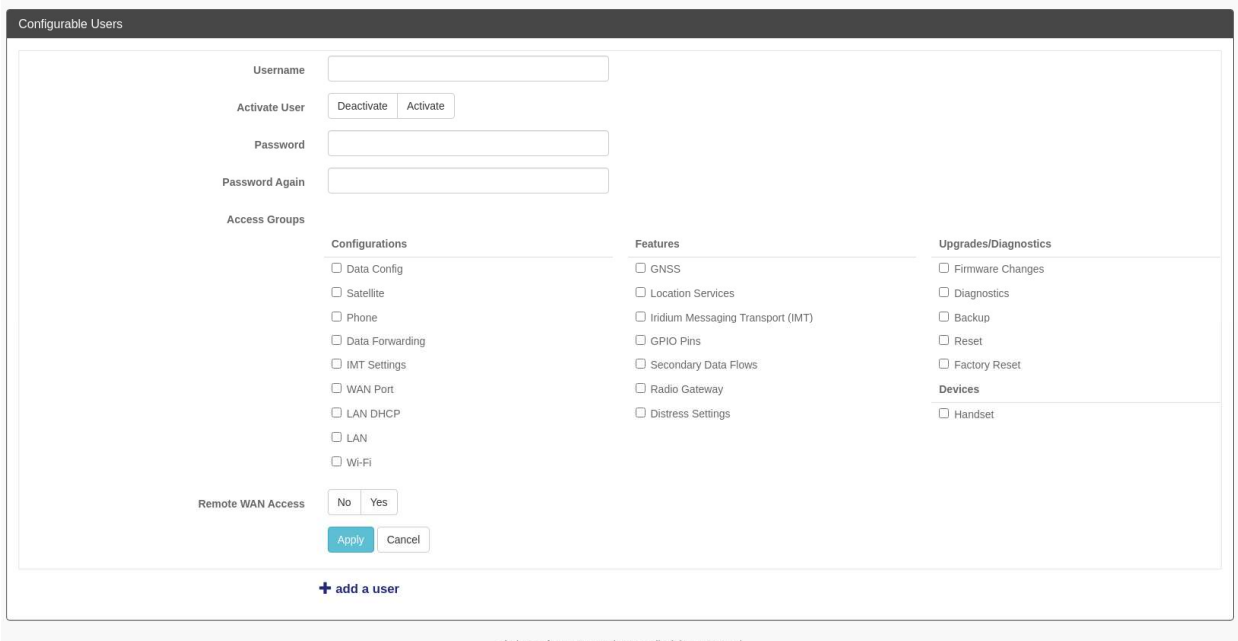
Figure 4-24 Adding user screen
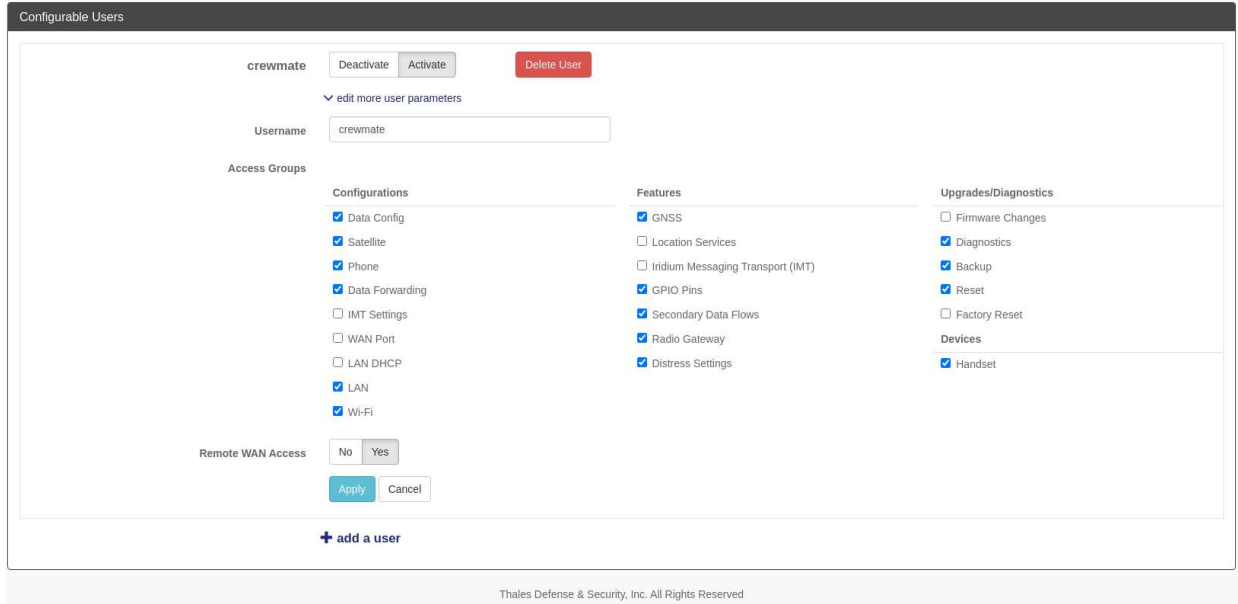
Figure 4-25 Editing user screen

Table 4-5 Settings → General Settings

Section	Parameters
Change Password	• Select User, Currently there are 3 choices (Admin, WAN_Admin, and WAN_User) • Enter NEW Password and confirm the new password (Note: Minimum of 8 characters with a lowercase letter, an uppercase letter, a number, and a special character)
Security	**Enable** / Disable the external API Access. (**Enable** is the default setting)
Configurable Users	
Username	Give new user a username. Must be at least 5 characters with no special characters.
Activate User	Activate/Deactivate new user. Deactivated users cannot log in.
Password	Give new user a strong password and confirm
Access Groups	Determine which settings groups the users had permissions for. Select all that apply.
Remote WAN Access	Select Yes to allow new user to access the terminal and selected groups remotely.

Table 4-6 Access Group Details

Access Group	Description	Page/Panels
Data Config	Configure the data session of the BDU. This includes activating/deactivating data and configuring the data route(s).	Settings: Data Data Configuration, Dashboard: Data Session
Satellite	All satellite data route settings, including port blocking and domain white/blacklisting	Settings: Satellite

Phone	All phone settings including dial plan, extension management, server configuration and phone configuration.	Settings: Phone
Data Forwarding	Configure data inbound routing.	Settings: Data Port Forwarding, Settings: Data Protocol Forwarding
IMT Settings	Configure the settings for Iridium Messaging Transport. This includes topic configuration and local servers and delivery.	Settings: IMT
WAN Port	Configure the WAN port and its traffic.	Settings:WAN
LAN DHCP	Configure the DHCP server and DHCP reservations.	Settings: LAN DHCP, Settings: LAN DHCP Reservations
LAN	LAN Port settings other than DHCP. This includes enabling/disabling POE, static routing, and the MAC address.	Settings: LAN LAN Ports, Settings: LAN Static Routes, Settings: LAN LAN MAC Address, Settings: LAN Dynamic DNS
Wi-Fi	General Wi-Fi settings and device whitelist.	Settings:WiFi
GNSS	Configure the GNSS constellations.	Settings: GNSS
Location Services	Configure the location tracking service.	Settings: Location Services
Iridium Messaging Transport®	Send a message using IMT® and manage the message history.	Iridium Messaging: Send Message, Iridium Messaging: Message History
GPIO Pins	Configure the two available GPIO pins.	Settings: GPIO
Secondary Data Flows	Configure the secondary data flows.	Settings: Secondary Data Flows
Radio Gateway	Configure the radio gateway feature.	Settings: Radio Gateway
Distress Settings	Configure the emergency message service.	Settings: Emergency
Firmware Changes	Upgrade the BDU firmware or revert to backup firmware.	System: Firmware, System: Reset Backup Version
Diagnostics	Perform a self-test or view/manage the BDU logs.	Diagnostics: Self Test, Diagnostics: Logs
Backup	Backup or restore configurations.	System: Backup
Reset	Reboot or shutdown the BDU.	System: Reset Reboot Device, System: Reset Shutdown Device
Factory Reset	Factory reset the BDU.	System: Reset Factory Reset
Handset	Manage SureLINK devices.	Settings: Handset

Emergency

	Emergency messages can only be configured by the administrator. If the user is not logged in as ADMIN and selects MANAGE EMERGENCY, the user will see this ⊘ icon, indicating this function is not available. Login in as the ADMIN to continue.
i **NOTE**	

On the Emergency page, the admin can set up an emergency message. The Management Portal configuration is restricted to an emergency email only. Select EMAIL from the pull down list (Figure 4-26). Enter the required information shown in Table 4-7 (example data shown in Figure 4-27) along with the message to be sent and select APPLY. NOTE: Selecting APPLY does not send an emergency message. It saves the settings and message. Sending the message is done through the EMERGENCY menu item.
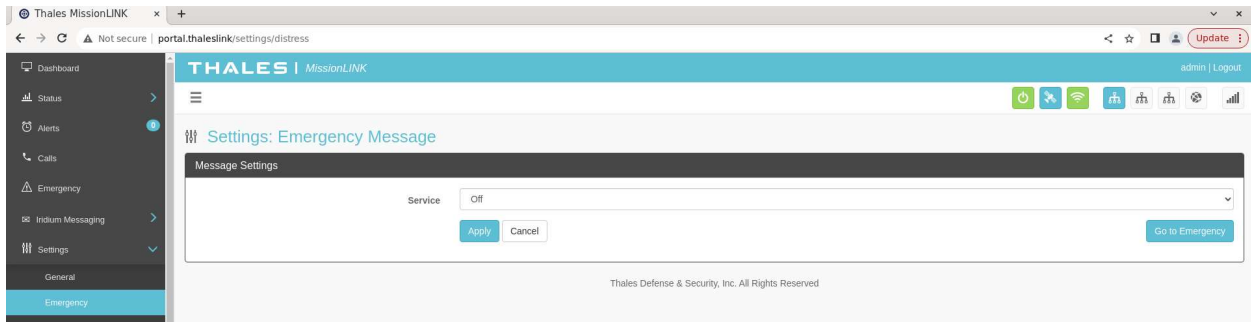
Figure 4-26 Settings → Emergency (Initial Screen)
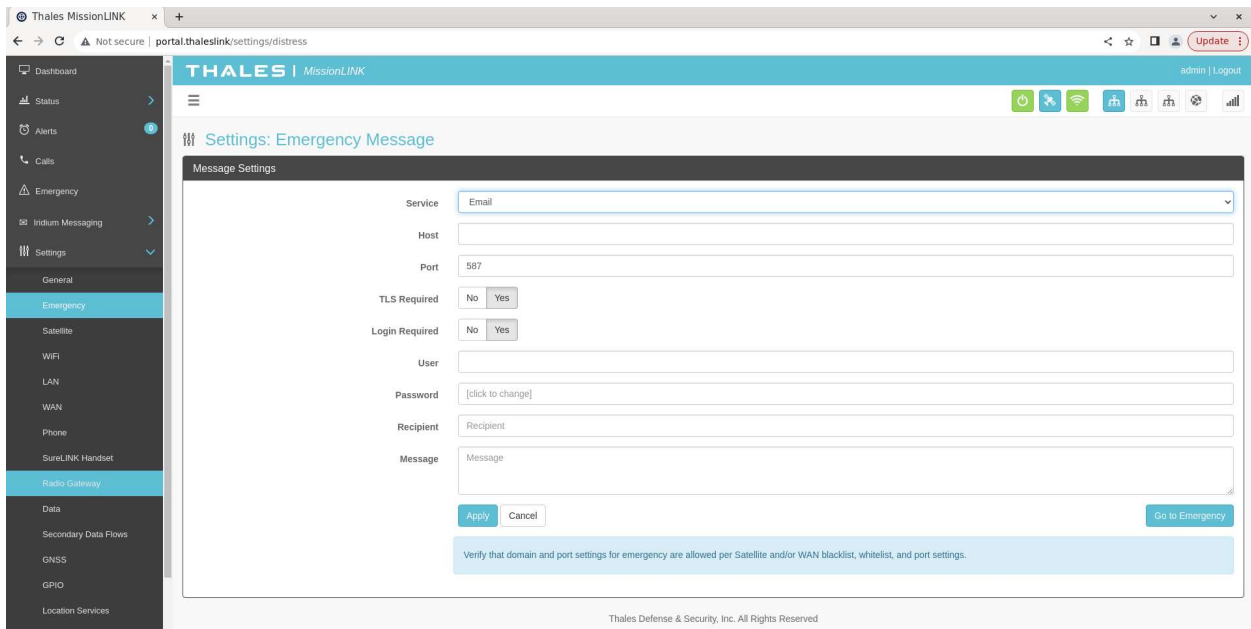
Figure 4-27 Settings → Emergency

Table 4-7 Settings → Emergency

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 **YES** or NO (Default setting is **YES**)
Login Required	Select either **YES** 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 Emergency message to be sent

Satellite

The Satellite page, shown in Figure 4-28, allows configuration of the data service. The configuration includes configuring whitelists and blacklists for domains, configuring port blocking and port whitelists and setting data usage warning thresholds for information purposes.

When adding a Domain to a Blacklist / Whitelist it is always necessary to first select the [+] button BEFORE selecting the [Apply] button. After selecting the [+] button, the domain can always be edited or deleted using the [✏] [🗑] buttons BEFORE selecting the [Apply] button to save. If the [Apply] button is not selected before leaving the Satellite menu item, the data will not be saved.
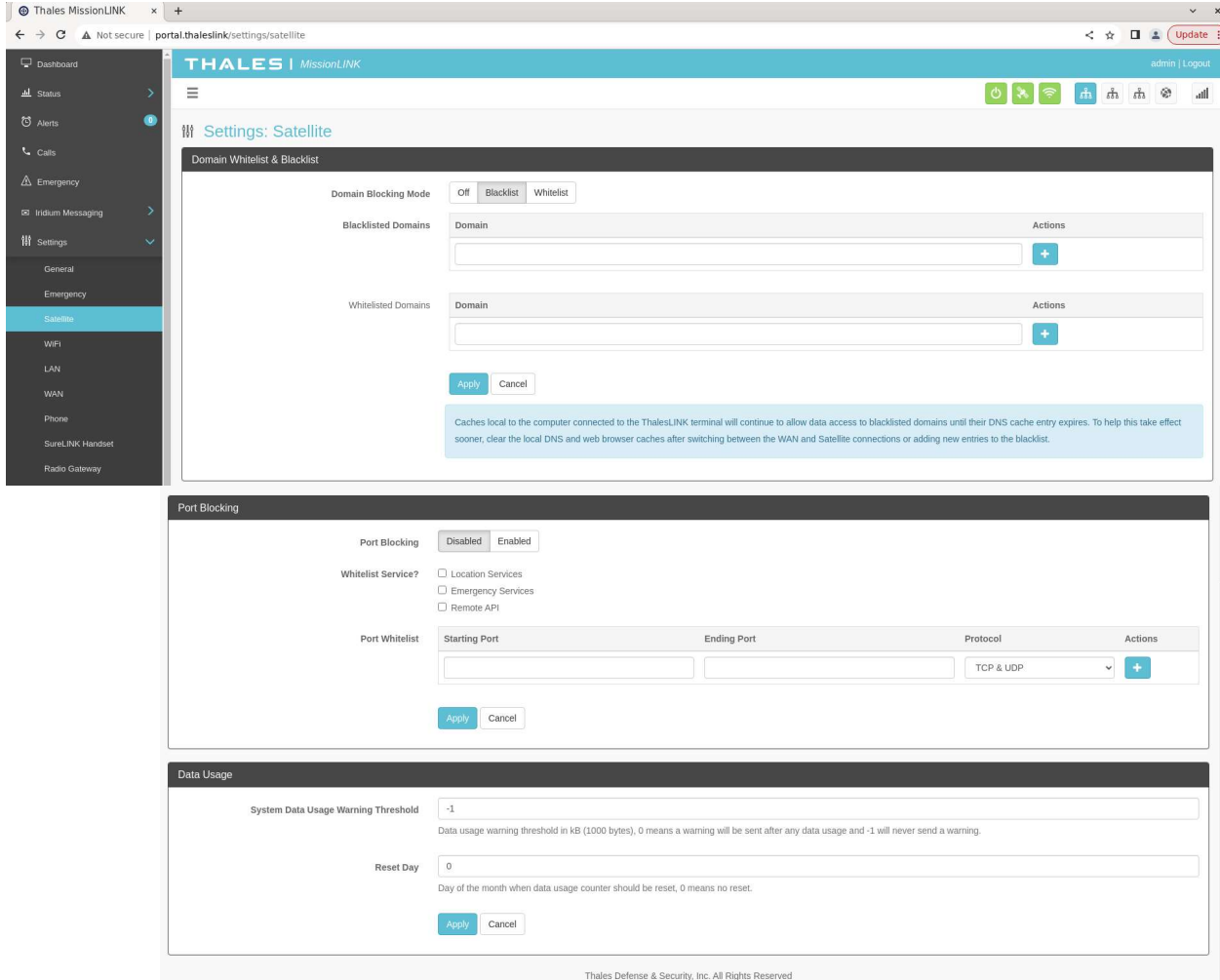
Figure 4-238 Settings→ Satellite Screen

Table 4-8 Settings→ Satellite

Section	Value
Domain Whitelist & Blacklist	
Domain Blocking Mode	**OFF** / Blacklist / Whitelist (**OFF** is the default setting)
Blacklisting	Enabling allows ALL websites EXCEPT those listed (very little restriction)
Whitelisting	Enabling blocks ALL websites EXCEPT those listed (the most restriction)
Port Blocking	
Port Blocking	**Disabled** / Enabled (**Disabled** is the default setting)
Whitelist Service	With Port Blocking Enabled, this allows for certain essential services (Location Services, Emergency Services, and the Remote API) to stay whitelisted/active and not be blocked. Check the services that are to stay active. The whitelisted port is updated if the configured port for that service is changed.
Port Whitelist	Enter the Starting Port and Ending Port number.

	Select the applicable protocol (**TCP & UDP** or TCP only or UDP only) (**TCP & UDP** is the default setting)
Data Usage	
System Data Usage Warning Threshold	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

NOTE Setting data limits is for information purposes only. Data figures are an approximation of data usage. Actual data usage should be obtained by the service provider. 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
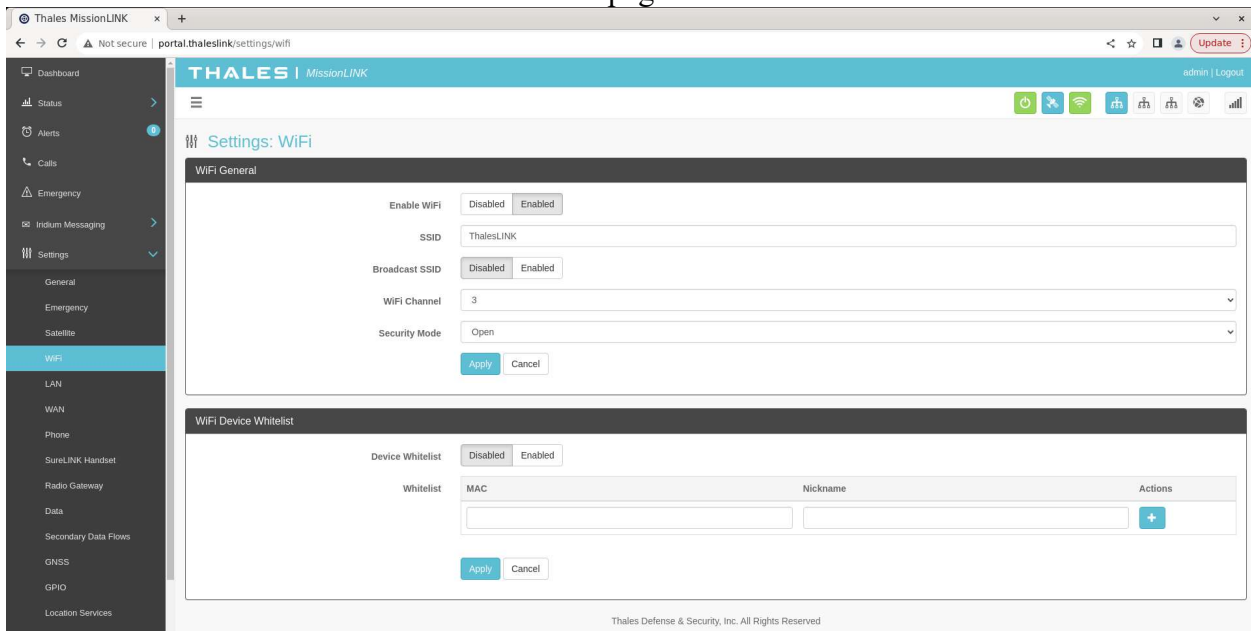
Figure 4-9 allows setup of the Wi-Fi service.
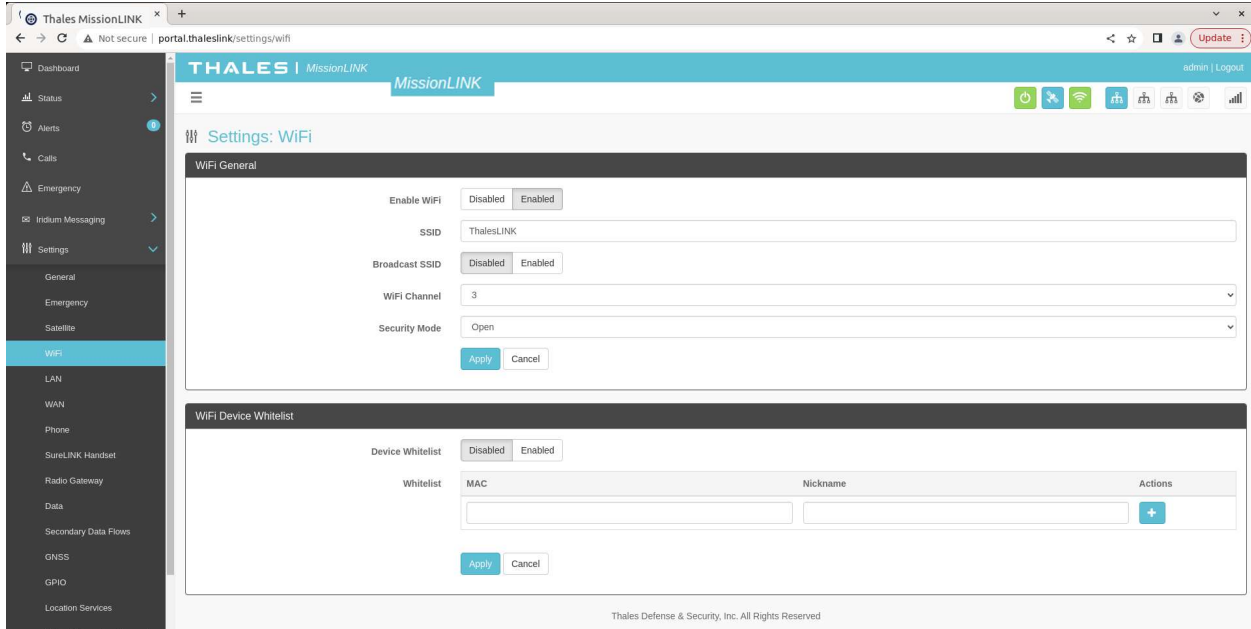
Figure 4-29 Settings→ Wi-Fi Screen

Table 4-9 Settings→ Wi-Fi

Section	Value
Wi-Fi General	
Enable Wi-Fi	Disabled / **Enabled** (**Enabled** is the default setting)
SSID	Enter the name of the SSID. ThalesLINK is default.
Broadcast SSID	Disabled / **Enabled** (**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. The password must be at least 8 characters in length and can be any combination of characters, numbers, etc. Once enabled, any device accessing the ThalesLINK (or new SSID name) Wi-Fi will have to enter the password.
Wi-Fi Device Whitelist	
Device Whitelist	**Disabled** / 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

> **(i) 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.

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 cannot 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.

NOTE

Changing the SSID disrupts the current connections so some Wi-Fi connections are dropped. The behavior is device dependent and will appear to be different for each device. Refer to Table 6-1 for additional information.

NOTE

LAN

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.

NOTE

The LAN page, shown in

Figure 4-, allows PoE to be enabled or disabled on the three LAN ports and DHCP to be enabled and configured or disabled. Each LAN port PoE is Class 2 and capable of providing up to 6.5 watts of power to the connected device. See

Table 4-for more information on the information that is entered.

> ℹ **NOTE** Please use "portal.thaleslink" as the NTP server.

> ℹ **NOTE** Changes to DHCP or LAN MAC address will take up to a minute to process. Data will be unavailable during this time.
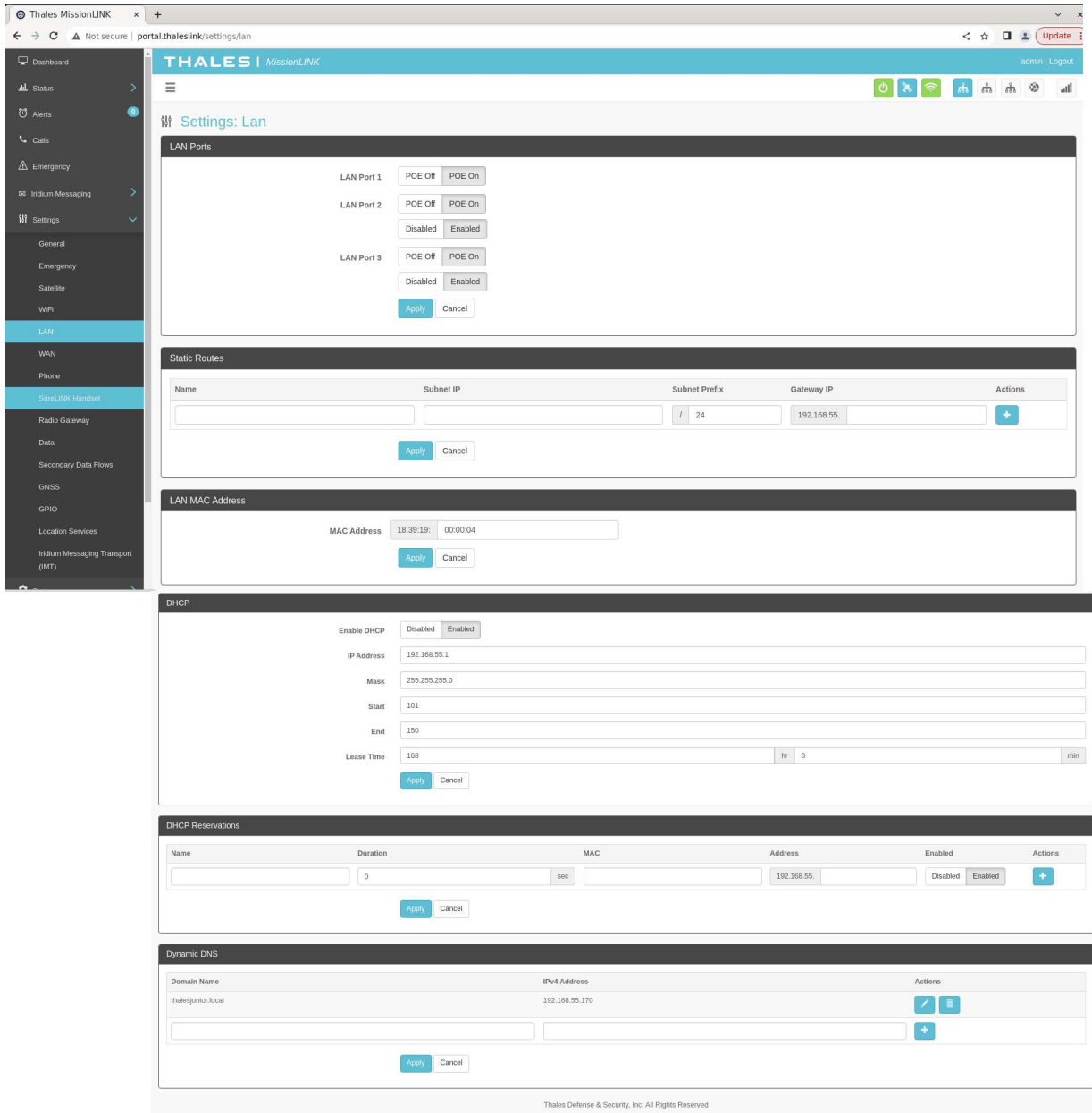
Figure 4-30 Settings→ LAN Screen

Table 4-10 Settings→ LAN

Section	Value
LAN Ports	
LAN Port 1	POE OFF / **POE ON** (**POE ON** is the default setting)
LAN Port 2	Disable POE OFF / **POE ON** (**POE ON** is the default setting) Disabled / **Enabled** (**Enabled** is the default setting)
LAN Port 3	POE OFF / **POE ON** (**POE ON** is the default setting) Disabled / **Enabled** (**Enabled** is the default setting)
Static Routes	
Static Route	Enter the Name, Subnet IP Address, Subnet Prefix, and Gateway IP address for the static route

Section	Value
	(Note: The Gateway address assigned to the router that connects the terminal to the network.)
LAN MAC Address	
MAC Address	Enter the MAC address (same for all LAN switches)
DHCP	
Enable DHCP	Disabled / **Enabled** (**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)
DHCP Reservations	
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 / **Enabled** (Enabled is the default setting)
Dynamic DNS	
Domain Name	A domain name to be added to the ThalesLINK's DNS resolver.
IPv4 Address	An IPv4 address to be associated with the domain name of this entry.

WAN

> **NOTE** This is an ADMIN function 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 4-31, allows configuration of the WAN data service. The settings include configuring whitelists and blacklists for domains, configuring port blocking and port whitelists.

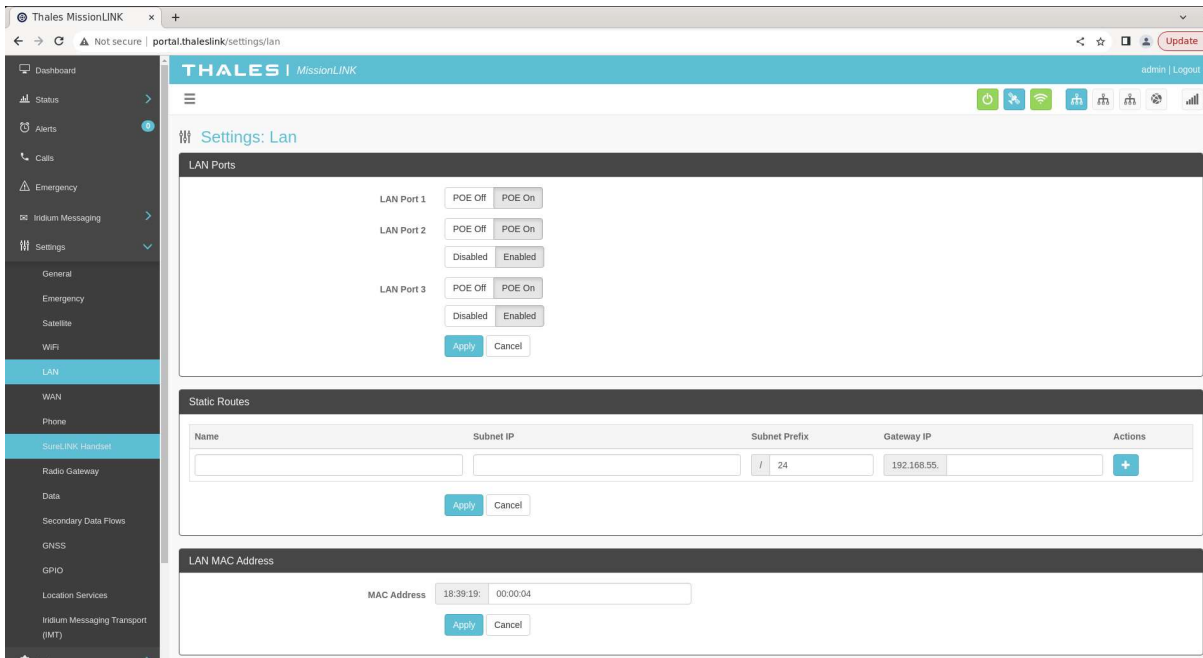When adding a Domain to a Blacklist/Whitelist it is always necessary to first select the [+] button BEFORE selecting the [Apply] button. After selecting the [+] button, the domain can always be edited or deleted using the [✏] [🗑] buttons BEFORE selecting the [Apply] button to save. If the [Apply] button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

> **NOTE** Caches local to the computer connected to the ThalesLINK terminal will continue to allow data access to blacklisted domains until their DNS cache entry expires. To help this take effect sooner, clear the local DNS and web browser caches after

switching between the WAN and Satellite connections or adding new entries to the blacklist.

(i) NOTE   If a WAN Modem connection is changed, it is important to remember that the terminal unit will need to restarted.

(i) NOTE   Changes to WAN configuration will take up to a minute to process. Data will be unavailable during this time.

Additional details about these settings are described in Table 4-11.

Figure 4-31 Settings→ WAN Screen

Table 4-11 Settings→ WAN

Section	Value
Configuration	
Polling Intervals	Sets the length of polling intervals, 30 is the default setting
Hostname	Lists the Hostname. Certus™ is the default setting.
WAN Failover Ping Address	Enter an IP address to change the default network availability ping from gstatic.com to an IPv4 address
Mode	Select **DHCP** or Static. (**DHCP** is the default setting.)
Domain Whitelist & Black List	
Domain Blocking Mode	**OFF** / 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)
Port Blocking	
Port Blocking	**Disabled** / Enabled (**Disabled** is the default setting)
Whitelist Service	With Port Blocking Enabled, this allows for certain essential services (Location Services, Emergency Services, and the Remote API) to stay whitelisted/active and not be blocked. Check the services that are to stay active. The whitelisted port is updated if the configured port for that service is changed.
Port Whitelist	Enter the Starting Port and Ending Port number.
	Select the applicable protocol (**TCP & UDP** 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 4-24, 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. There are up to three (3) high quality Iridium phone lines. 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 [✎] icon, a password can be entered for each extension if desired. An extension can be deleted by selecting the [🗑] icon. Changes are saved only after the settings are applied.

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.

The ThalesLINK sip server is "sip.thaleslink" by default, but can be changed to another domain name or to the IP address of the ThalesLINK. Finally, 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 [Apply] button. Several extensions can be added by selecting the [+] button multiple times, and then selecting the [Apply] button. After selecting the [+] button, the extension can always be edited or deleted selecting the [✏] [🗑] buttons BEFORE selecting the [Apply] button to save. If the [Apply] button is not selected before leaving the Phone menu item, the data will not be saved. Table 4- describes the settings in more detail.
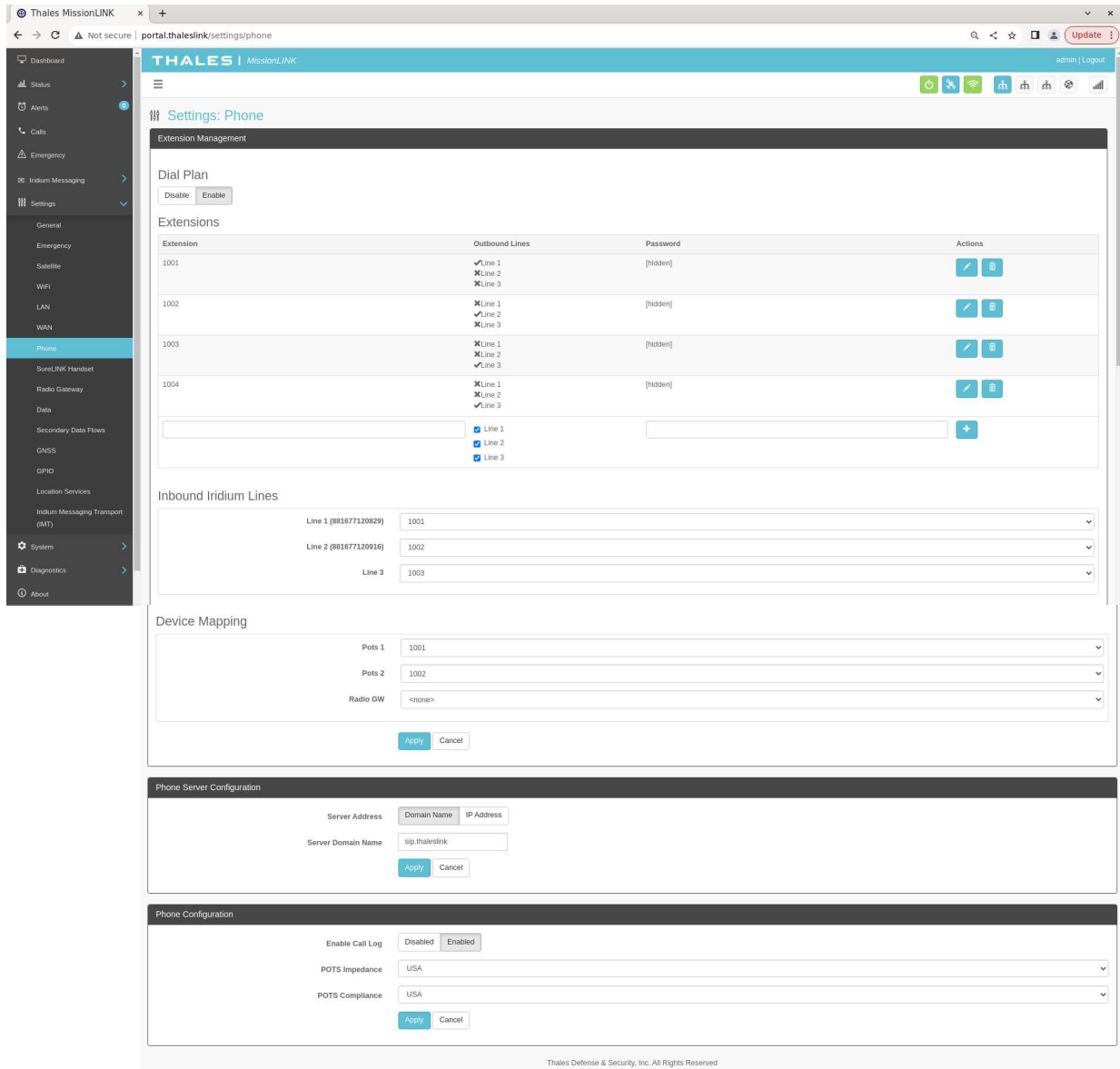
Figure 4-24 Settings → Phone Screen

Table 4-12 Settings → Phone

Section	Value
Dial Plan	
Disabled / Enabled	Disabled – when selected, the requirement to dial a "9" before making a call across Iridium is now disabled. (Note: When disabled, all calls go across the Iridium constellation and local extension to extension calls are disabled.) (**ENABLED** is the default setting)
Extension Mapping	
1-88888	Additional custom extensions of varying lengths can be added.
1001	Default extensions that receives and makes calls on the first Iridium line. Connected to the first POTS line.

Section	Value
1002	Default extensions that receives and makes calls on the second Iridium line. Connected to the second POTS line.
1003	Default extension that receives and makes calls on the third Iridium line.
Inbound Iridium Lines	
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
Device Mapping	
POTS	Assigns extensions to POTS 1 and POTS 2 phones (Note: 2 POTS phones can be attached with a splitter to the POTS connector.
Radio GW	Assigns extension to the Radio Gateway
Phone Server Configuration	
Server Address	**Domain Name** / IP Address (**Domain Name** is the default setting). Sets the SIP server to either use the below provided Server Domain Name or to use the terminal's IP address as the sip server.
Server Domain Name	The desired domain name to be used when the Server Address option is set to Domain Name. Not used if IP Address is selected above.
Phone Configuration	
Enable Call Log	Disabled / **Enabled** (**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 (**USA**, Australia, Europe, UK, USA-Loaded) (**USA** is the default setting)
POTS Compliance	Sets the POTS Compliance to match regional phone types. (USA or Brazil). (**USA** is the default setting)

NOTE

Extensions must begin with a number from 1 to 8 and must have four (4) or more digits.

NOTE

Changes to Extension management will take up to a minute to process. Data will be unavailable during this time.

VoIP Phone Settings

NOTE

Please use "portal.thaleslink" as the NTP server

The two VoIP phones that Thales recommends include the CISCO SPA504G and the Grand Stream GXP2140. Other phones may work with the MissionLINK terminal, however the functionality cannot be guaranteed.

The two sections below include general recommended settings for the user to get up and running with the VoIP phones.

- **CISCO SPA504G** -- The first section shows how to configure the CISCO SPA504G on the pre-configured extension 1001.
- **GRAND STREAM GX2140** -- The second section shows how to configure the Grand Stream GXP2140 on extension 1002.

CISCO SPA504G

This procedure assumes that the MissionLINK Terminal is starting from its factory reset state and that the CISCO SPA504G phone is also in its factory reset state. Note, most of the initial settings for the CISCO phone stay as they are. Only a few of the settings are required to change as outlined in the steps below.

1.) Connect the CISCO phone to one of the RJ-45 LAN ports on the front of the MissionLINK Terminal.

2.) View the Management Portal (http://portal.thaleslink or https://portal.thaleslink). Note that the SETTINGS →PHONE extensions 1001, 1002, and 1003 are pre-configured as shown in Figure 4-33.
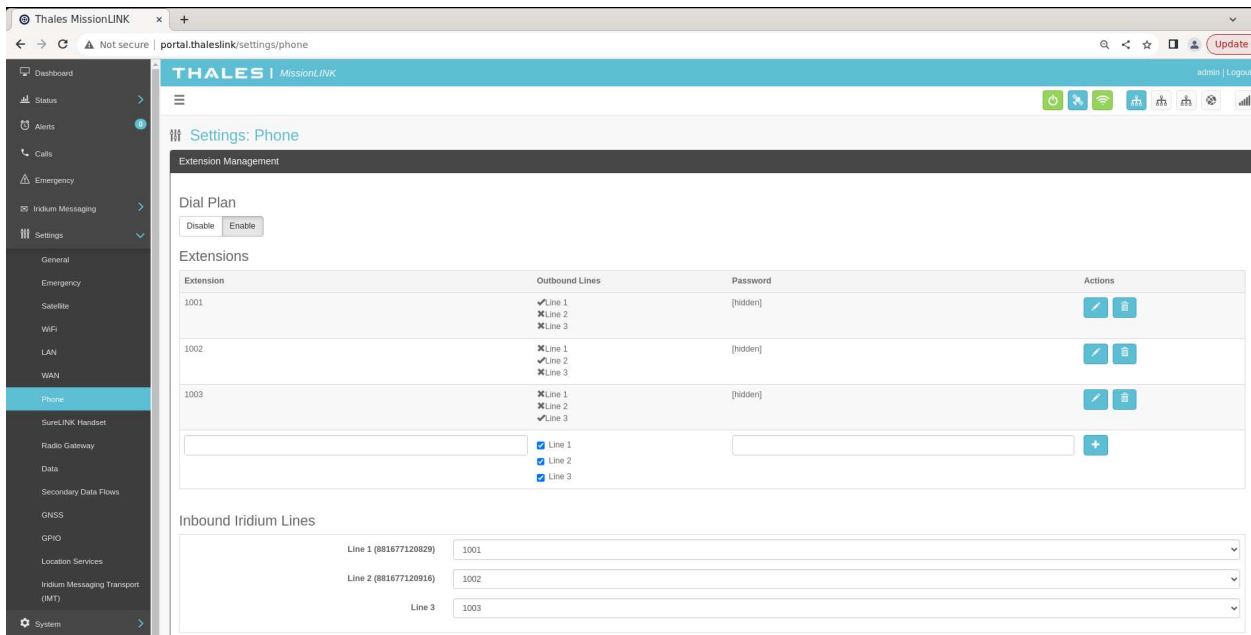
Figure 4-33 VOIP Phone Settings

3.) In order to bring up the phone's configuration page in a browser, one needs to find the IP address of the connected phone. This is accomplished by going to the Management Portal and entering STATUS → CURRENT DEVICES. In this example, the CISCO SPA504G has an IP address of 192.168.55.106 as shown in Figure 4-254 below.
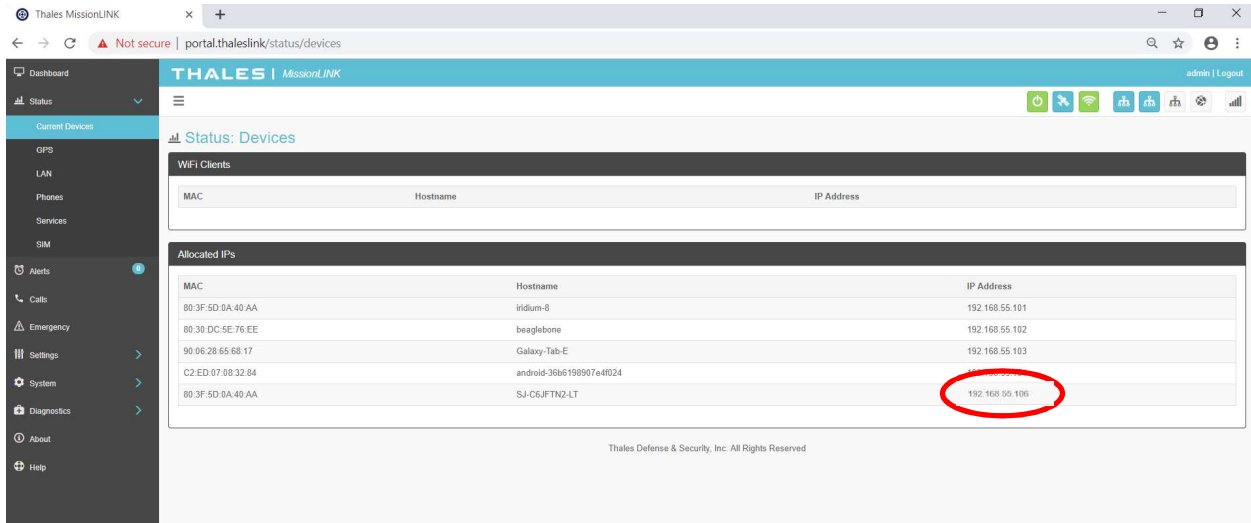
Figure 4-254 CISCO SPA504G IP Address

4.) Using a web browser, use the IP address found in step 3 to go to the CISCO SPA504G phone configuration page and go to Admin Login at the upper right of the menu (after you do this "User Login" will appear). Select Voice→Ext 1.

    a. In the Proxy field, enter "sip.thaleslink". Note: This entry must match the Phone Server Configuration on the Settings:Phone page.

    b. In the Display Name, User ID and Password enter "1001". Although the Display name does not have to be 1001, it is more clear if it set to the same number as the User ID and Password.

    c. When finished, press the "Submit All Changes" button. This will cause the phone to reset. See Figure 4-265 for the entries above.
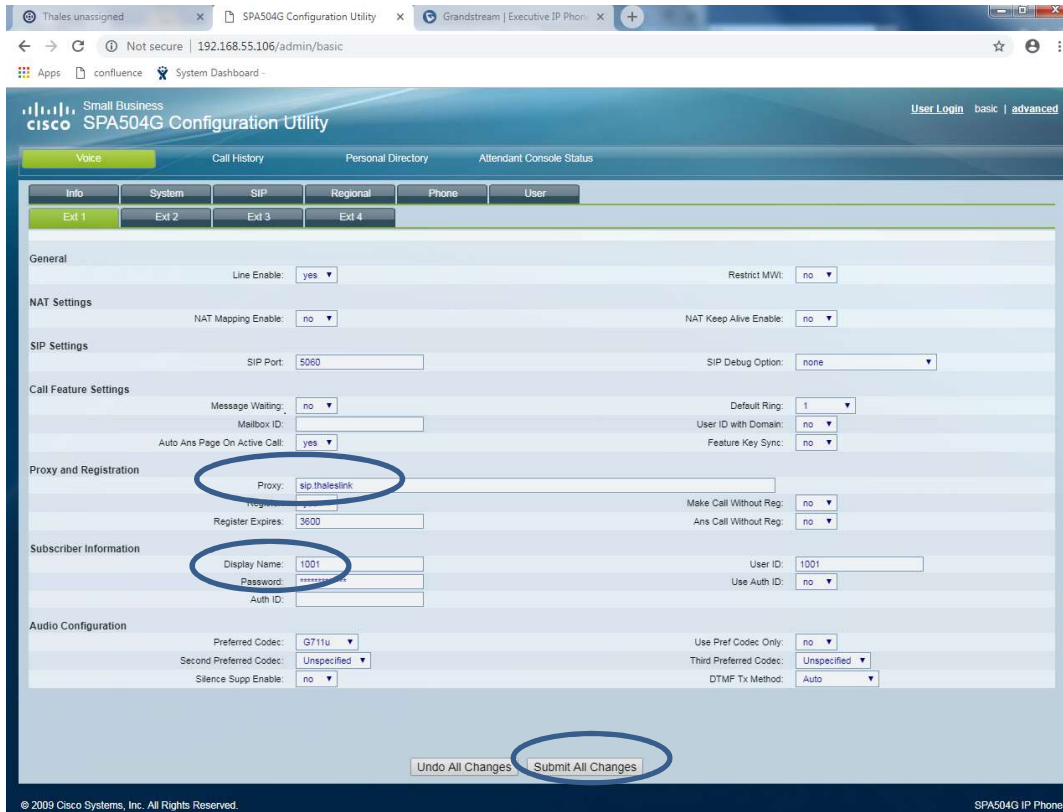
Figure 4-265 SPA504G Configuration Utility

The CISCO SPA504G phone should be ready for calls after these steps.

GRAND STREAM GXP2140

This procedure assumes that the MissionLINK Terminal is starting from its factory reset state and that the GRAND STREAM GXP2140 phone is also in its factory reset state. Note, most of the initial settings for the GRAND STREAM phone stay as they are. Only a few of the settings are required to change as outlined in the steps below.

1.) Connect the GRAND STREAM phone to one of the RJ-45 LAN ports on the front of the MissionLINK Terminal.

2.) View the Management Portal (http://portal.thaleslink or https://portal.thaleslink). Note that the SETTINGS →PHONE extensions 1001, 1002, and 1003 are pre-configured as shown in Figure 4-265 above.

3.) In order to bring up the phone's configuration page in a browser, one needs to find the IP address of the connected phone. This is accomplished by going to the Management Portal and entering STATUS → CURRENT DEVICES. In this example, the GRAND STREAM GXP2140 has an IP address of 192.168.55.102 as shown in Figure 4-254 above. It may take process of elimination to find out what the IP address is.

4.) Using a web browser, use the IP address found in step 3 to go to the GRAND STREAM GXP2140 phone configuration page. Login as an Administrator and go to ACCOUNTS→Account 1→General Settings as shown in Figure 4-276 below.

    a. In the SIP Server field, enter "sip.thaleslink". Note: This entry must match the Phone Server Configuration on the Settings:Phone page.

    b. In the SIP User ID, the Authenticate ID and Authenticate Password, enter "1002".

    c. When finished, press the "Save and Apply" button. See Figure 4-276 below for the entries above.
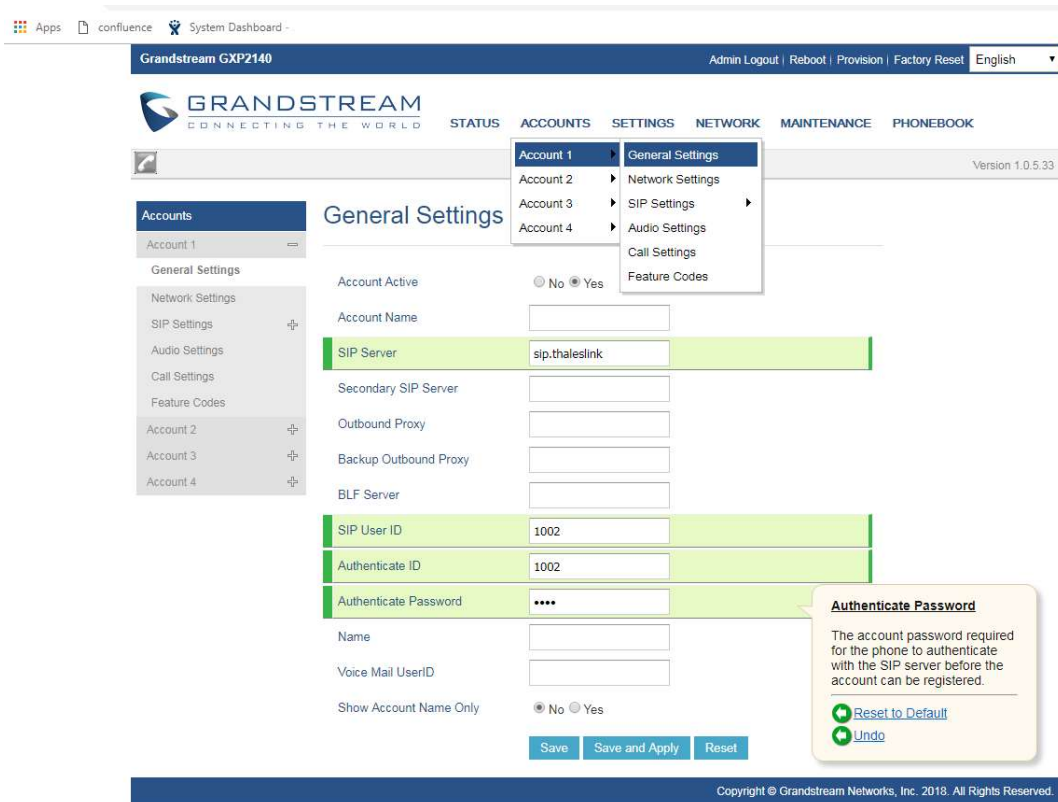
Figure 4-276 Grand Stream GXP2140 Configuration Page

The GRAND STREAM GXP2140 phone should be ready for calls after these steps.

SureLINK Handset

The SureLINK Handset is an accessory that is sold separately and has its own user manual (84481), so reference that for operational guidance. The SureLINK is discontinued, but is still supported.

This section of the manual details how to install, update, or uninstall SureLINK apps that are provided in the MissionLINK system through software updates. Figure 4-37 shows two options for App management on the SureLink, Automatic or Manual. To edit either, its respective button needs to be selected, and then select Apply.

> **(i) NOTE** Detection of a connected SureLINK is done internally and automatically. The SureLINK must be plugged in and turned on for Applications to be installed.
> Neither the LINK app nor Adobe Acrobat can be uninstalled or updated through this feature. Third party applications can be uninstalled.

Automatic mode allows users to modify any SureLINK connected using the designated Settings. The specified settings will apply to all connected SureLINKs if automatic mode is enabled.

Manual mode allows users to affect changes on a specific SureLINK device. Each SureLINK is displayed on the page with its own panel, and the user can choose whether to install, uninstall, or upgrade apps on each SureLINK.

Currently, for this feature, only the ESChat Push-To-Talk (PTT) application is supported on the SureLINK. The Application's name and version supported by the MissionLINK system is listed here along with the option to change its installation status.
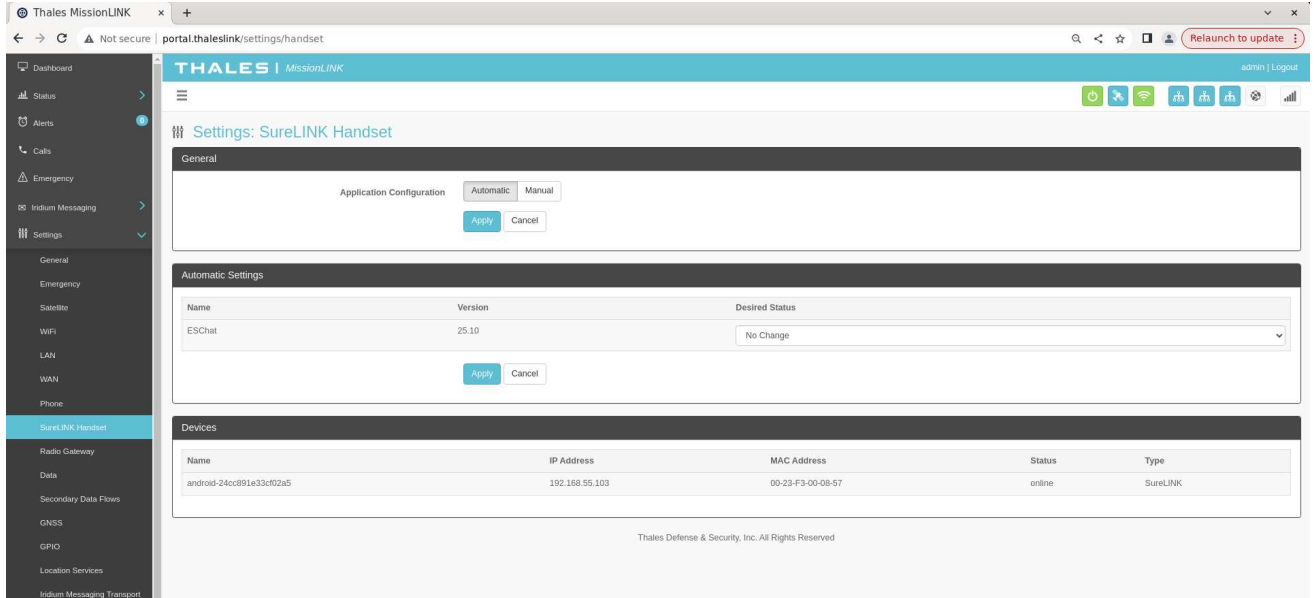
Figure 4-287 Settings → SureLINK Handset Automatic App Configuration
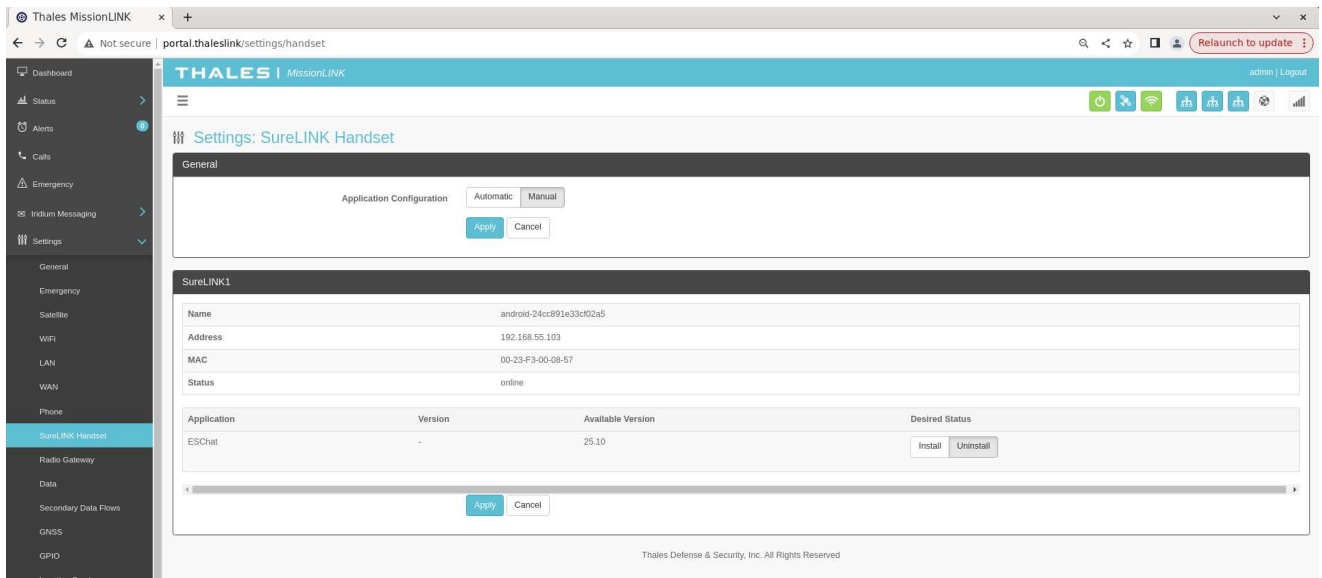
Figure 4-298 Settings → SureLINK Handset Manual App Configuration

NOTE	In Figure 4-37 and Figure 4-38, the screen shot shows that a SureLINK is currently connected. Otherwise, it will display a message that says "No handset devices are currently connected".

Table 4-33 Settings→ SureLINK Handset

Section	Value
General	
Application Configuration	**Automatic** / Manual
Automatic Settings	
Name	The name of the Application as it appears on the MissionLINK
Version	Version of the App as it appears on the MissionLINK.
Desired Status	**No Change**, Install, and Uninstall. This determines how the SureLINK will be modified when connected. If No Change is selected, nothing will occur. Install means the Version of the Application seen will always be put on the SureLINK. This applies to upgrades as well. Uninstall will always uninstall the app if it is seen on the SureLINK, no matter the version.
Devices (Automatic Configuration)	
Name	The name of the SureLINK, typically 'android-' followed by a string of numbers or letters.
IP Address	The IP address of the SureLINK
MAC Address	The MAC address of the SureLINK
Status	Status of the SureLINK (online or offline)
Type	The type of Handset, aka SureLINK
SureLINK 1 (Manual Configuration)	
Name	The name of the SureLINK, typically 'android-' followed by a string of numbers or letters.
Address	The IP address of the SureLINK
MAC	The MAC address of the SureLINK
Status	Status of the SureLINK (online or offline)
Application	The name of the Application as it appears on the MissionLINK
Version	Version of the App as it appears on the MissionLINK.
Available Version	Version of the App as it appears on the MissionLINK
Desired Status	Install/Update, or Uninstall *Install/Update* will put the latest available version of software on the SureLINK. If the Application is not already on the SureLINK, *Install* will be seen instead of *Update* here, and the user can install the latest version of the application on the SureLINK. If no version for the application software exists on the MissionLINK, the *Install/Update* button will be grayed out and not selectable. *Uninstall* removes the specific App from the SureLINK and will always be an available option.

Radio Gateway

![NOTE icon] **NOTE**	This is an ADMIN function only. If the user sees this 🚫 icon, login as the ADMIN to continue. Otherwise this is a view only screen.

Figure 4-309 Settings→ Radio Gateway

User Manual PN 84468 Rev N

Table 4-44 Settings→ Radio Gateway

Section	Value
Configuration	
Transmit VoIP Gateway	
Mode	DTMF or Voice Activated Dialing (**VAD**) (**VAD** is the default setting). This configuration determines how the telephony user of the radio gateway PTTs in order to speak on the radio network. VAD means the telephone user simply needs to speak in order to transmit. DTMF requires the telephone user to press a digit to begin transmitting and a digit to stop transmitting.
DTMF: ON Digit	Valid DTMF digits range from "0" thru "9", "*", "#". (The default digit is "*".) Dialing the selected digit will cause the radio to start transmitting
DTMF: OFF Digit	Valid DTMF digits range from "0" thru "9", "*", "#". (The default digit is "#".) Dialing the selected digit will cause the radio to stop transmitting.
VAD: Voice Hang Time	VAD Voice Hang Time determines how long the telephone user's voice transmission will continue after the voice is no longer present. Acceptable value range is 0 to 5000 msec. (Default setting is **500** msec).
Transmit Audio	
Delay	Sets the delay being applied to the transmit audio (when VoIP is VAD). Acceptable values range from 0 to 500 seconds. (Default setting is **300** msec).
Analog Gain	Sets the gain (in dB) applied to the hardware in the radio to transmit audio. Acceptable values -20 to 20 dB. (Default setting is -**20** dB).
Digital Gain	Sets the gain (in dB) applied to the software in the radio to transmit audio. Acceptable values -40 to 20 dB. (Default setting is -**20** dB).
VAD: Threshold	For VAD mode, controls the sensitivity of voice detection on outgoing telephone user's audio. Acceptable values -40 to 20 dBFS. (Default setting is -**35** dBFS)
Transmit / Radio PTT	
Active Level	**Enabled** / Disabled, (**Enabled** is the default setting). This setting should be adjusted to match the connected radio, depending on if the connected radio has external PTT as ENABLED or DISABLED in order to transmit.
Timeout	The maximum amount of time, in seconds, that PTT to the radio will be continuously asserted. After this timeout expires, the radio will be de-keyed until the telephony user causes it to begin transmitting again.
Receive Activity	
Mode	The mechanism used to detect receive activity from the radio (a.k.a., channel busy or COR)—either via the presence of voice or the assertion of the hardware COR input pin (GPIO). Select **VAD** or **GPIO** (Default setting is **VAD**).

Section	Value
VAD: Hang Time	If Receive Activity Mode is set to "VAD", the Hang Time determines how long the voice transmission will continue to be received after the voice is no longer present. Acceptable value range is 0 to 5000 msec. (Default setting is **500** msec).
GPIO: Active Low	If Receive Activity Mode is set to "GPIO", set the GPIO Active Level to either High or Low (Default setting is **Low**).
Receive Audio	
DTMF: Threshold	For DTMF mode, controls the sensitivity of tone detection on incoming DTMF. Acceptable values -35 to 0 dBFS. (Default setting is **-20** dBFS)
VAD: Threshold	For VAD mode, controls the sensitivity of voice detection on incoming audio. Acceptable values -40 to 20 dBFS. (Default setting is **-35** dBFS)
Analog Gain	Sets the gain (in dB) applied to the hardware in the radio to receive audio. Acceptable values -20 to 20 dB. (Default setting is **0** dB).
Digital Gain	Sets the gain (in dB) applied to the software in the radio to receive audio. Acceptable values -40 to 20 dB. (Default setting is **0** dB).
Calling	
DTMF Dialing Phrase	Phrase of DTMF digits which, when received from the radio, will cause the RGW to enter dialing mode. Subsequent digits will be accumulated into a phone number buffer, and a call will be placed to that number once the user stops dialing. Acceptable values are any string of valid DTMF digits (0-9, *, #) (Default setting is "******")
DTMF Disconnect Phrase	Phrase of DTMF digits which, when received from the radio, will cause any ongoing call or operation to terminate. Acceptable values are any string of valid DTMF digits (0-9, *, #) (Default setting is "**##**")
Digit Timeout	When the radio user is entering a number in dialing mode, how long to wait, in seconds, after receiving a DTMF digit before concluding that the user is done entering the target number. After this timeout elapses, a call is attempted to the target number. Acceptable values ≥ 0 sec. (Default setting is **3 sec**)
Max Digits	The maximum length of a phone number that may be entered by a radio user in dialing mode, including any prefixes such as country code and external calling access digit. The phrase used to initiate dialing (e.g., "**") does **not** count towards the maximum number of digits. Acceptable values ≥ 0. (Default setting is **20**)
Dialing Duration	When a radio-initiated outbound call is being placed, a burst of ringback tone is transmitted to the radio user for this amount of time as confirmation. Acceptable values ≥ 0 msec. (Default value is **1000** msec).
Disconnect Duration	When an active call is hung up, a burst of busy tone is transmitted to the radio user for this amount of time. Acceptable values ≥ 0 msec. (Default value is **2000** msec)

Section	Value
Error Duration	When an outbound call fails or an active call ends prematurely due to an error, a burst of fast-busy tone (a.k.a. congestion tone) is transmitted to the radio user for this amount of time. Acceptable values are ≥ 0 msec. (Default value is **2000** msec).
Answer Timeout	After an outbound call has been placed, how long to wait for the peer to answer before giving up and terminating the call. Note that the call attempt may terminate before this timeout is reached if an error is encountered. Acceptable values are ≥ 0 sec. (Default value is **60** sec).

Data

NOTE This is an ADMIN function 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 4-40, 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.

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

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.
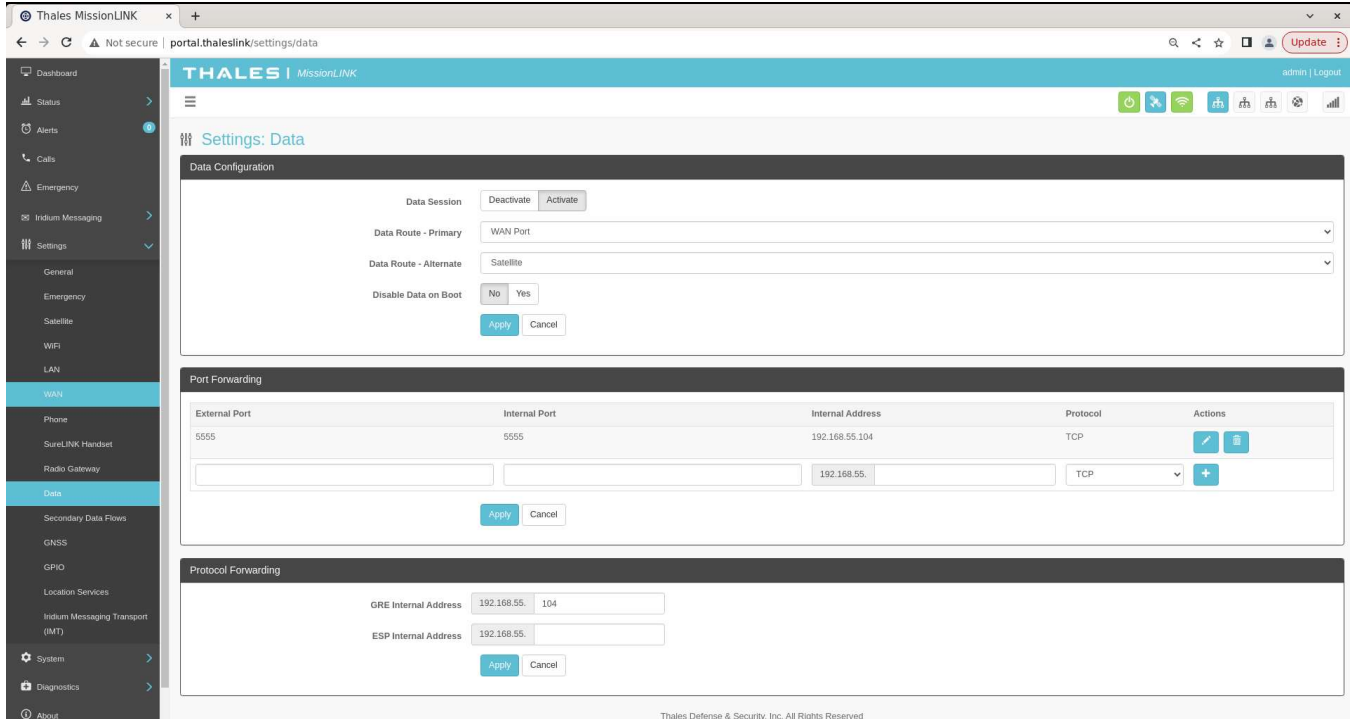
Figure 4-40 Settings→ Data Screen

Table 4-55 Settings→ Data

Section	Value
Data Configuration	
Data Session	Deactivate / **Activate** (**Activate** is the default setting)
Data Route - Primary	Select the desired data route (**WAN** or Satellite Port) (WAN is the default setting).
Data Route - Alternate	Select the desired alternate data route. (**Satellite** is the default setting) Note: If Satellite is selected, the available options are WAN Port or Disabled. If WAN Port is selected, the available options are Satellite or Disabled.
Disable Data on Boot	**NO** / YES (**NO** is the default setting). Determines the default data operations state when the system is restarted.
Port Forwarding	
Port Forwarding	Enter the External Port, Internal Port, Internal IP Address, and Protocol. Up to seven ports can be forwarded in the range of 1 - 53247. Ports greater than 53247 cannot be forwarded
Protocol Forwarding	
Protocol Forwarding	Enter the GRE Internal IP Address and/or the ESP Internal IP Address.

> ℹ️ **NOTE**
> "Disable Data on Boot" allows the operator to manually set the data session to ON whenever the unit is powered on.

Secondary Data Flow (SDF)

> **i** This is an ADMIN function only. If the user sees this 🚫 icon, login as the ADMIN to continue. Otherwise this is a view only screen.
> **NOTE**

A Secondary Data Flow (SDF) connects a port on the terminal to a service on the network. The device connects directly to the service without interference from the terminal.

The ports and/or Wi-Fi can be configured in Map mode to route all untagged packets on a physical or virtual port directly to the SDF provisioned service.

Ports and Wi-Fi can be configured in VLAN Tag mode, which provides access to all provisioned SDFs. If the incoming packets are tagged with a valid, provisioned VLAN tag, the packets are routed directly to the associated SDF. See below for tagging information. Untagged data will be routed to the default data flow.

Internal Services (virtual ports) can only be mapped to SDFs. The virtual ports cannot be tagged.

> **i** SDFs: An SDF cannot be assigned to a Port and a Service simultaneously. However, the same SDF may be assigned to multiple ports or multiple services.
> **NOTE**

> **i** Virtual and physical ports must remain separate. Multiple ports can be mapped to the same SDF or packets tagged for the same SDF from different devices. An SDF assigned to a virtual port cannot be used by a physical port and a physical port cannot be used by a virtual port. This also means data on a VLAN Tag port will not be routed down an SDF in use by a virtual port.
> **NOTE**

> **i** At least one physical LAN Port must be configured in either Default or Bridge mode.
> **NOTE**

Figure 4-41 Settings → Secondary Data Flows

User Manual PN 84468 Rev N

Table 4-66 Settings→ Secondary Data Flows

Section	Value
Port and Service Mapping	
LAN Port 1	Default / VLAN Tag / Map
LAN Port 2	
LAN Port 3	Select the mode for each port.
Wi-Fi	
	If Map mode is selected, select an SDF to be routed through each external LAN connection. VLAN tag data is automatically routed down matching SDF tagging without associating the SDF to a tag. **Note:** The SDF must be activated by your Service Provider to be valid.
Location Services	Select an SDF to be routed to each terminal provided service. Default is used for no SDF. VLAN tagging isn't available for services.
Emergency Services	
Remote Control (API)	**Note:** The SDF must be activated by your Service Provider to be valid.
External Port Configuration (Example SDF1 in Figure 4-41 above)	
State	Deactivate/**Activate**, Turns on or off SDF X
Gateway	Enter the Gateway IP and Prefix for the SDF network.
Port Forwarding	Enter the External Port, Internal Port, Internal IP Address, and Protocol. Up to seven ports (combined total of Data and Secondary Data Flows) can be forwarded throughout the system, and SDFs allow the full range of ports to be used (1 – 65535)
GRE Internal Address	Enter the GRE Internal IP Address
ESP Internal Address	Enter the ESP Internal Address
DHCP	Enter the DHCP Start, End and Lease times in seconds. **Enable** or Disable DHCP.
Internal Port Configuration (Example SDF3 in Figure 4-41 above)	
State	Deactivate/**Activate**, Turns on or off SDF Y
Service Networks	Each service can be deactivated individually. When active, an arbitrary name and the destination subnet are required.

NOTE

SDFs: Each SDF can be deactivated individually. GRE, ESP, and DHCP can be routed through an SDF as done previously in the data tab. Port forwarding is also supported through an SDF as done previously in the data tab.

SDF requires the Service Provider (SP) to associate a SIM with a service provided by the SP through an SDF.

NOTE

For example, LAN Port 2 on the terminal can be associated with a corporate Virtual Private Network and LAN Port 3 can be associated with the internet for crew welfare.

A SP can use an SDF to route Location Services messages directly to a Location Services server and count the data for that service separately.

The user cannot select an unprovisioned SDF. These are grayed out and may only be assigned through the API.
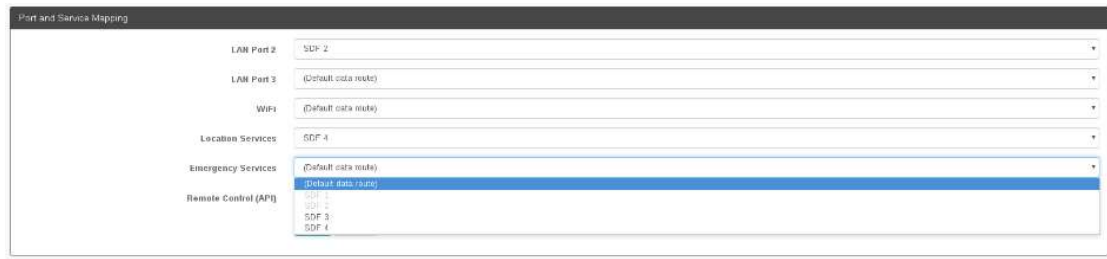
NOTE

Global Navigation Satellite System (GNSS)

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

NOTE

Certus antennas with GNSS chipsets are capable of using all four GNSS constellations; GPS, Galileo, GLONASS, and BeiDou. Those without a GNSS chipset will not display the constellation choices and default to GPS.

NOTE
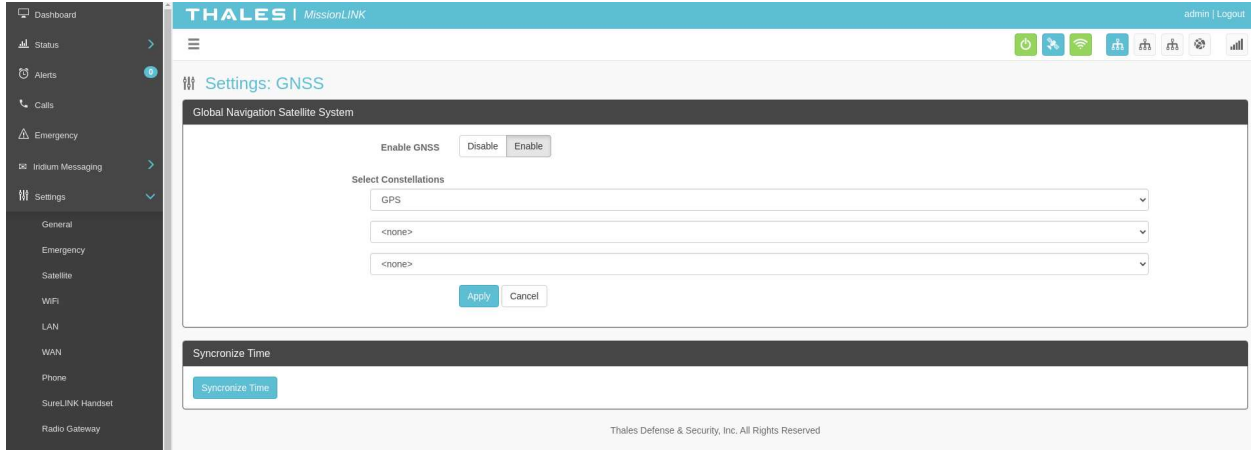
Figure 4-42 Settings → Global Navigation Satellite System

Table 4-77 Settings → Global Navigation Satellite System

Section	Value
Global Navigation Satellite System	
Enable GNSS	Select Disable or **Enable**. **(Enable** is the default setting) When the setting is changed, the system requires a reboot (refer to Figure 4-).
Select Constellations	Select up to three GNSS satellite constellations to receive positioning and timing data from. **GPS** is the default. When multiple constellations are chosen, the terminal uses the system with the best signal for position data. Note: When BeiDou and GLONASS are both selected, no other constellations can be selected.
Synchronize Time	
Synchronize Time	Synchronize time is only used when the terminal's system time is incorrect, GNSS is disabled, and the GNSS cannot be enabled for security purposes or operational reasons. (Note: When performing a software upgrade and a failure occurs, synchronizing the terminal's time will often solve the problem.)

Figure 4-43 Enable GNSS Reboot Notification Screen

Figure 4-44 Synchronize Time Confirmation Screen

GPIO

(i) **NOTE** This is an ADMIN function only. If the user sees this ⊘ icon, login as the ADMIN to continue. Otherwise this is a view only screen.

(i) **NOTE** For more information about the pinout of the DB-15 GPIO connector, see Figure 7-4. Refer to the tech note, produced by Thales, for information on applications and physical connections of the DB-15 connector.

This section describes how to configure two general purpose GPIO pins, pins 6 and 13, located on the DB-15 connector on the rear of the BDU (see Figure 7-2). This configuration includes activating the pins with output voltage of about 3.3V, setting the pins as an input and reading the applied voltage value, and a satellite connectivity status feature. A "high" reading indicates that the input pin is reading about 3.3V, and "low" indicates a reading of about 0V. The two pins can be configured in any combination.

⚠ If a pin is set to *Input*, the maximum voltage applied should be 3.3VDC. Higher voltages could damage the BDU.
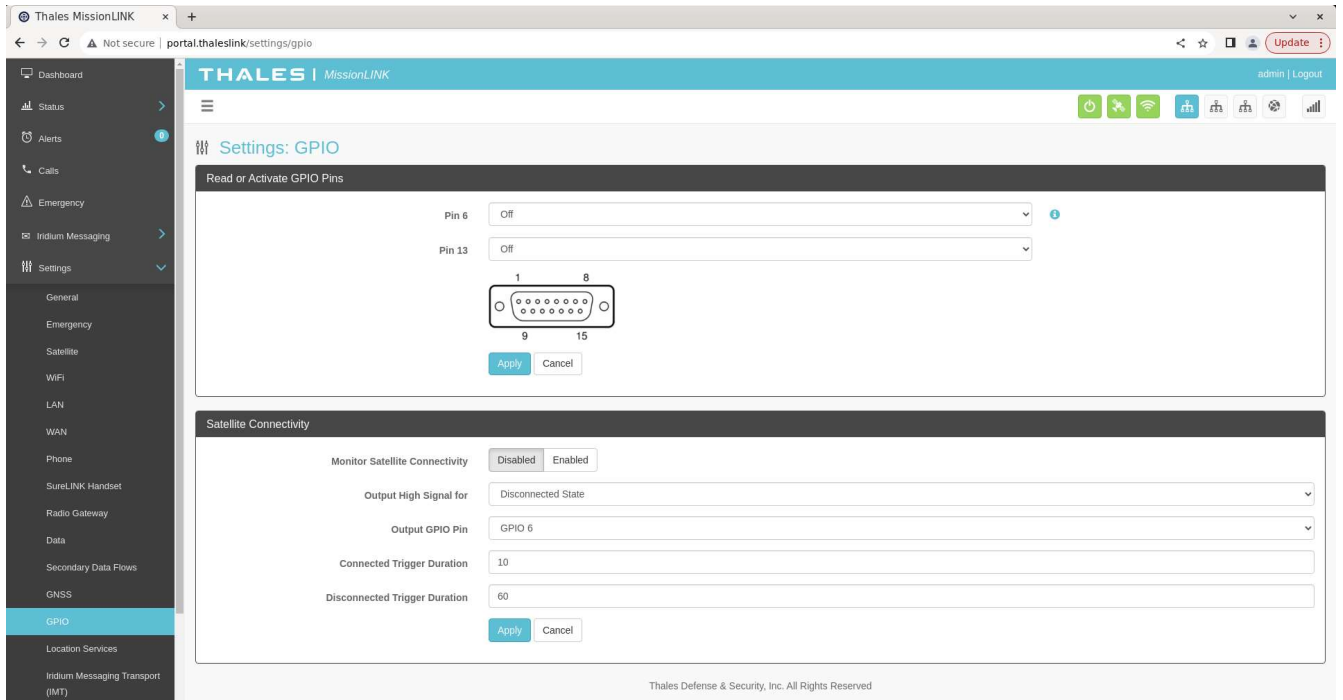
Figure 4-315 Settings → GPIO

(i) **NOTE** The same pin, either Pin 6 or Pin 13, cannot be used for both the *Read or Activate GPIO Pins* feature and the *Satellite Connectivity* feature. Separate pins must be used for each.

4-56

Table 4-88 Settings → GPIO

Section	Value
Read or Activate GPIO Pins	
Pin 6	**Off**/ Input / Active. If *Input* is selected, the pin will be configured to read voltage applied to it, and if *Active* is selected, the pin will be powered with about 3.3.V.
Pin 13	**Off**/ Input / Active. If *Input* is selected, the pin will be configured to read voltage applied to it, and if *Active* is selected, the pin will be powered with about 3.3.V.
Satellite Connectivity	
Monitor Satellite Connectivity	**Disabled** / Enabled
Output High Signal for	Connected State / **Disconnected State** (choose whether a high output signal represents a connected or disconnected state regarding the satellite)
Output GPIO Pin	**GPIO 6** / GPIO 13
Connected Trigger Duration	Integer in seconds. Multiples of 5 are valid with a minimum of 5. Default is **10**.
Disconnected Trigger Duration	Integer in seconds. Multiples of 5 are valid with a minimum of 5. Default is **60**.

Location Services

From the Location Services page, shown in Figure 4-46, Location Services are enabled and disabled and the settings are configured (when enabled). A Location Services server is required to interact with Thales's open protocol. Contact Thales Customer Support for details.
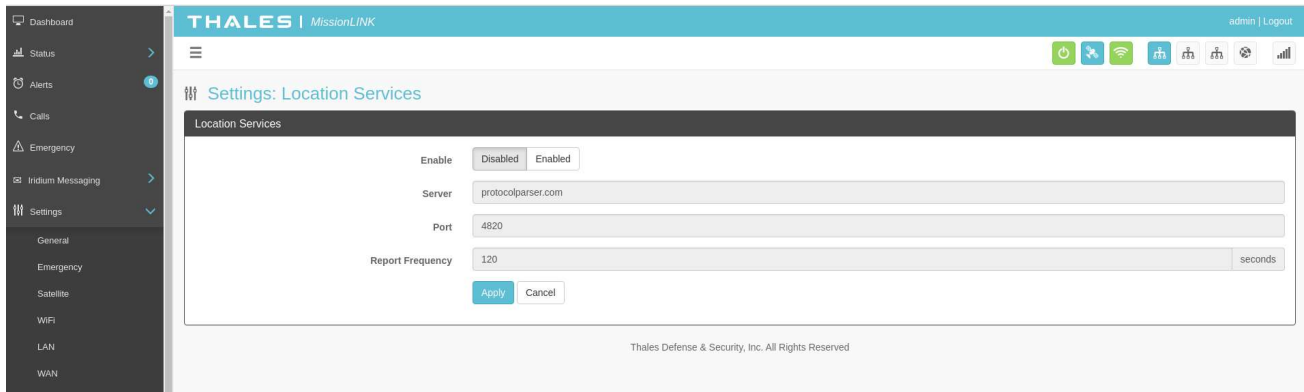
Figure 4-326 Settings → Location Services Screen

Table 4-99 Settings → Location Services

Section	Value
Location Services	
Enable	**Disabled** / Enabled (**Disabled** is the default setting)
Server	Enter the name of server.
Port	Enter the port number of the service from server.
Report Frequency	Default setting is 120 seconds. When EMERGENCY is activated, frequency will be every 5 seconds.

Iridium Messaging Transport (IMT®)

From the Iridium Messaging Transport® page, shown in Figure 4-47, the admin may configure IMT® topics. Available IMT® topics in the dropdown menu are determined by the SIM, so please contact your service provider to set up topics.

The admin can also configure local socket servers, which listen for and send packets as outgoing IMT messages, or configure the local delivery of incoming IMT Messages.

For details on individual parameter, refer to Table 4-19.
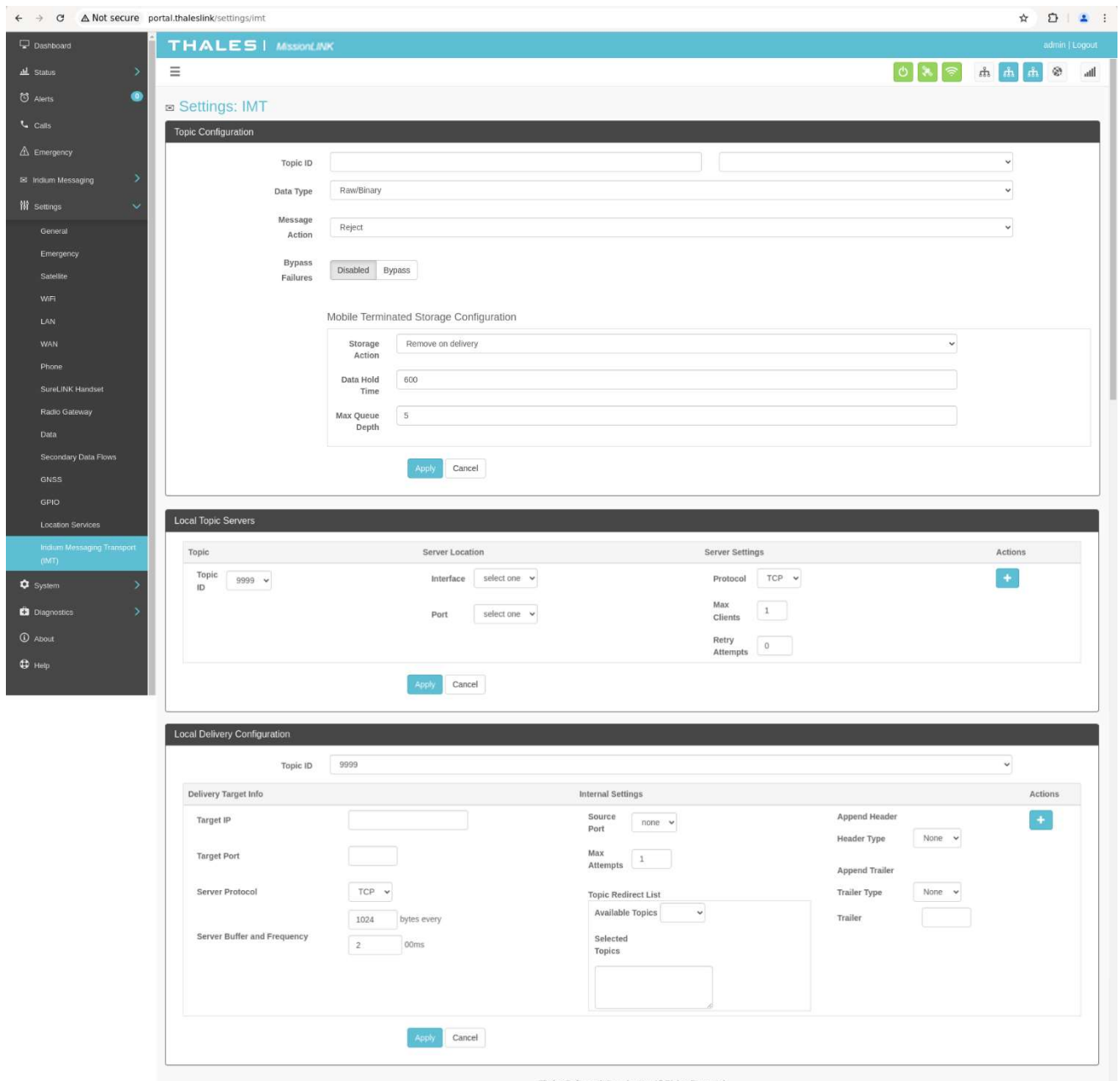
Figure 4-337 Settings → IMT® Screen

| Data Type | Message | ⌄ |
| Encoding | ascii | |

Figure 4-348 Settings → IMT® Encoding

Table 4-20 Settings → IMT®

Section	Value
Topic Configuration	
Topic ID	If the Topic ID exists on the terminal, use the drop down to select the ID to configure. Topic IDs the SIM is subscribed to are automatically loaded with default settings by the terminal.
Data Type	Select the data type to apply to messages of this topic. Default setting is **RAW/BINARY**. • RAW/BINARY - This data type interprets the message as simple binary data. *Note: Submitting binary data to the API will require users to convert the binary to base64 for submission. • MESSAGE - This data type interprets the message as encodable/decodable text. To use another encoding, configure the encoding input box. The character "\r" is not allowed and will cause the message to be invalid.
Encoding	When Data Type is set to Message, enter the encoding used to convert the message into binary, see Figure 4-48. Default is **ASCII**. Examples include ascii, utf-8, utf-16, or utf-32. If the entered encoding is not supported, an error alert will appear when settings are applied.

Message Action	Select the message action to be applied when a message is over the maximum size (100 Kilobytes).
	• REJECT- This message action will reject messages above the maximum size
	• TRUNCATE - This message action will truncate messages above maximum size to maximum size (only usable for Data Type MESSAGE).
	• MULTI_MESSAGE - This message action will break the message up into maximum size sub messages. These sub messages will have an internal id recorded in each message along with a number (0-2046) representing count. The count and internal id can be used to determine message order to recombine messages. Count 2047 is reserved for messages at the maximum size for MULTI_MESSAGES, roughly 204.5 megabytes.
	*Note: Requires Bypass Failures to be set to True.
	   • RAW/BINARY Multi-Message
	
	{{TABLE_A}}
	
	   • MESSAGE Multi-Message

Table A (embedded in Message Action cell):

Internal id (base 36 [0-9][A-Z]	Count	User data
37 bits (0-ZZZZZZZ, eg A5KL4TR)	11 bits (0-2047 eg 1273)	99,994 bytes

Section	Value
	JSON Object, removed spacing (outside of data) {"id": "0-ZZZZZZZ", "cnt": 0-2047, "data": "...99,964 characters..."} eg: {"id":"A5KL4TR","cnt": 2022,"data":"Hello World!"}
Bypass Failures	**DISABLED** / BYPASS (**DISABLED** default) When BYPASS, the following are notable reasons (normally resulting in Message rejection) will be bypassed: - Data Type Message - Encoding failures will be replaced with backslash then hex code "\r" in the message will be replaced with "\n" character - Data Type Raw - If data_json is supplied when sending a message, bypass simply drops the data_json value rather than reporting error.
Mobile Terminated Storage Configuration	
Storage Action	Select the storage action to be applied to incoming messages (aka mobile terminated messages). If stored, the messages do not persist over terminal reboots. **REMOVE ON DELIVERY**- The default, this option removes message data after delivery(s) has been made or delivery attempts have been exhausted. - STORE BASED ON SUBSCRIPTION - Holds the message data after delivery(s) has been made or delivery attempts have been exhausted. Uses the SIM configured hold time and queue depth to determine when to discard the data. - STORE BASED ON USER SETTINGS - Holds the message data after delivery(s) has been made or delivery attempts have been exhausted. Uses the user configured hold time and queue depth to determine when to discard the data.
Data Hold Time	If STORE BASED ON SUBSCRIPTION is selected, displays the subscription hold time. If STORE BASED ON USER SETTINGS is selected, enter the length of time in seconds desired to hold a message after delivery attempts.
Max Queue Depth	If STORE BASED ON SUBSCRIPTION is selected, displays the subscription max queue depth. If STORE BASED ON USER SETTINGS is selected, enter the number of messages to be held after delivery attempts.
Local Topic Servers	
Topic ID	Select the Topic ID this socket server on the ThalesLINK will send locally received data to. The SIM must have a subscription to the Topic ID.
Interface	The logical interface on which this socket server on the ThalesLINK will receive data. Options are default or any SDF interface. The IP address on default will be the IP Address configured for DHCP on the Settings: LAN page. The IP address on SDFs will be the same as the DHCP Host for that SDF. DHCP must be enabled on the chosen SDF.

Section	Value
Port	Select from the list of ports that the ThalesLINK will listen on for incoming data. Available ports are 9950-9975. *Note: If a port is specified as a source port for delivering using the same protocol used for this server, it will not be an option here until the delivery source port setting is changed.
Protocol	TCP or UDP, the protocol used in this socket server.
UDP Timeout	The amount of time this server will wait for the next packet to arrive before creating and sending a message. Only used for UDP.
Max Clients	The maximum allowed simultaneous connections to this socket server on the ThalesLINK
Retry Attempts	The number of times to retry sending a message delivered to this socket server if it fails to deliver.
Local Delivery Configuration	
Topic ID	Configure local delivery of incoming IMT messages for this selected Topic ID. The Topic ID must already be configured by the user or automatically added by subscribing on the SIM.
Target IP	IPv4 Address of a local computer. Incoming IMT messages will be delivered to this address via a socket.
Target Port	Enter a port on the local computer that will receive socket connections.
Server Protocol	TCP/UDP – The protocol used by the local computer for this socket connection.
Server Buffer*	The buffer size in bytes of the UDP socket. This determines the amount per packet the ThalesLINK will deliver to this socket. Default of **1024** *Only used for UDP sockets
Server Frequency*	The expected frequency in 100s of ms of the socket server. Default is **200 ms.** Note: Slower receiving sockets that may be found on embedded devices may need more time in between packets. *Only used for UDP sockets
Source Port	The source port desired for delivery packets: 9950-9975 or random source port at delivery. Required if using a Topic Redirect List with UDP. NOTE: This value can conflict with Local Topic Server's ports, so if an option is unavailable, check your Local Topic Servers list for a potential conflict.
Max Attempts	The max number of attempts to make delivering a message to this target. NOTE: A TCP socket times out after 20 seconds per attempt and the time between each attempt is a static 5 seconds. If the ThalesLINK fails to connect to the server's socket or some other failure occurs, an additional attempt will be performed 5 seconds later. Due to the nature of UDP, a UDP packet will be assumed delivered after one attempt.
Header Type	Type of header to be attached to the beginning of each socket's data. - NONE - No header 64 BIT- An 8 byte header will be sent to this target. The header consists of 16 bits or 2 byte Topic ID, 37 bit internal id, and 11 bits reserved. - STRING - A string representation of the header will be sent to this target, using the encoding specified by the Topic. This string contains the internal id of the message, a hyphen, the Topic ID of the message, and finally two colons. - Example: "5AYN081-245::"

Section	Value
	• JSON – JSON header will contain two keys and their values. The keys are "topic_id" and "internal_id". o Example: {'topic_id': 4156, 'internal_id': 'AB12ZXY'}
Trailer Type	Type of trailer to be attached to the end of each socket's data. • NONE - No trailer • STRING - Uses the Trailer field as the text to be appended. Encoding used is configured under Topic Configuration panel. • HEX - Uses the Trailer field as the hexadecimal value to be appended as binary data.
Trailer	The string to be appended as interpreted by the Trailer Type.
Topic Redirect List	
Available Topics	Drop down of available topics to send response data to. This will be added to the Selected Topics text area.
Selected Topics	A comma separated list of topics to send messages to in the event that the server responds to a socket connection. Any data received will be sent to each topic in this topic list. NOTE: The ThalesLINK TCP delivery socket will wait for up to 20 seconds for a response on the connection and the ThalesLINK UDP delivery socket will wait up to 5 seconds for a response at the same port as the packet's source port. The UDP socket's buffer size is max UDP packet size and only waits for one packet.

System

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

Backup

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

NOTE

Refer to Figure 4-9. When performing a firmware update, replacing 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 4-359 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 settings to a replacement unit or cloning setup for multi-units.

- 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

NOTE   Config files dating back to software version 2.1.0 are supported. This will apply for future software releases unless otherwise noted.

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 4-50. Data usage is shown for information purposes only. If there is a data limit set, this information will be provided on this screen. Satellite Data Session is the data used since the last power-up. Satellite Data Total is the data used since the last reset (manual or automatic). The system data usage can be reset to restart the data count. Select RESET and then YES, RESET to confirm. Otherwise, select NO, CANCEL (Figure 4-51). For Satellite Data Limits – pressing the VIEW SATELLITE LIMITS button, will bring up the SETTINGS → SATELLITE Screen (Figure 4-238).

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.
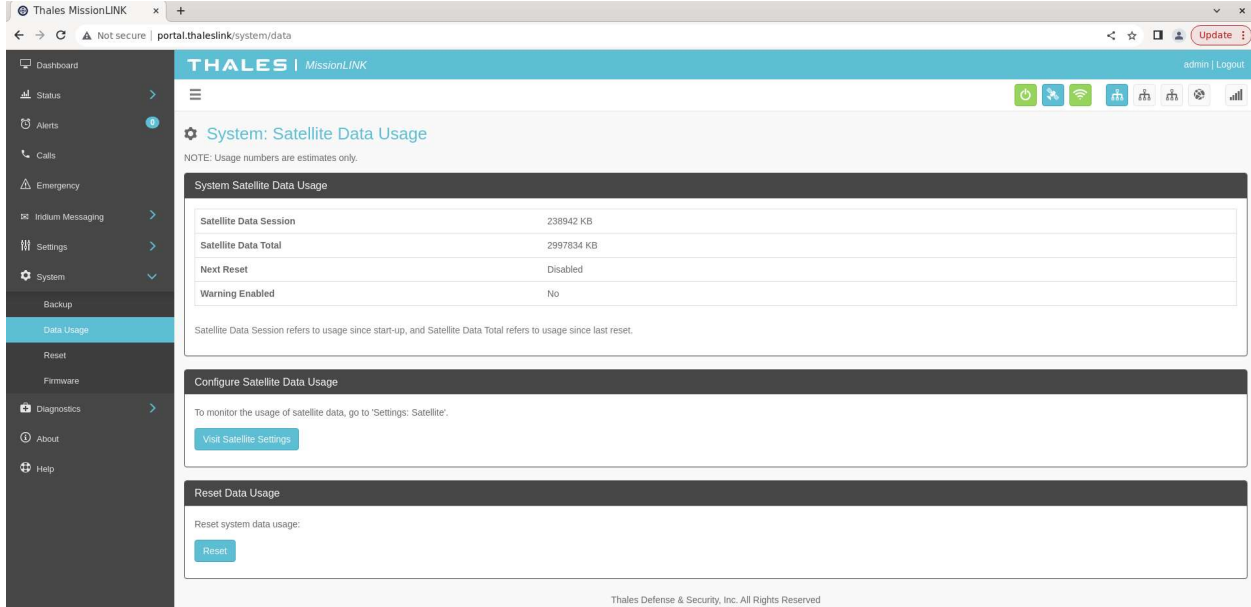
Figure 4-50 System → Data Usage Screen

Figure 4-51 Reset Data Usage Screen

Reset

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

Refer to Figure 4-52. In the event the system is not responding correctly, a system reboot can be performed. Select REBOOT to restart the system.

The SHUTDOWN button allows and administrator to shut down the BDU but this will require manual action to turn the BDU back on.

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.

Backup Version will revert the system to the previous software version.
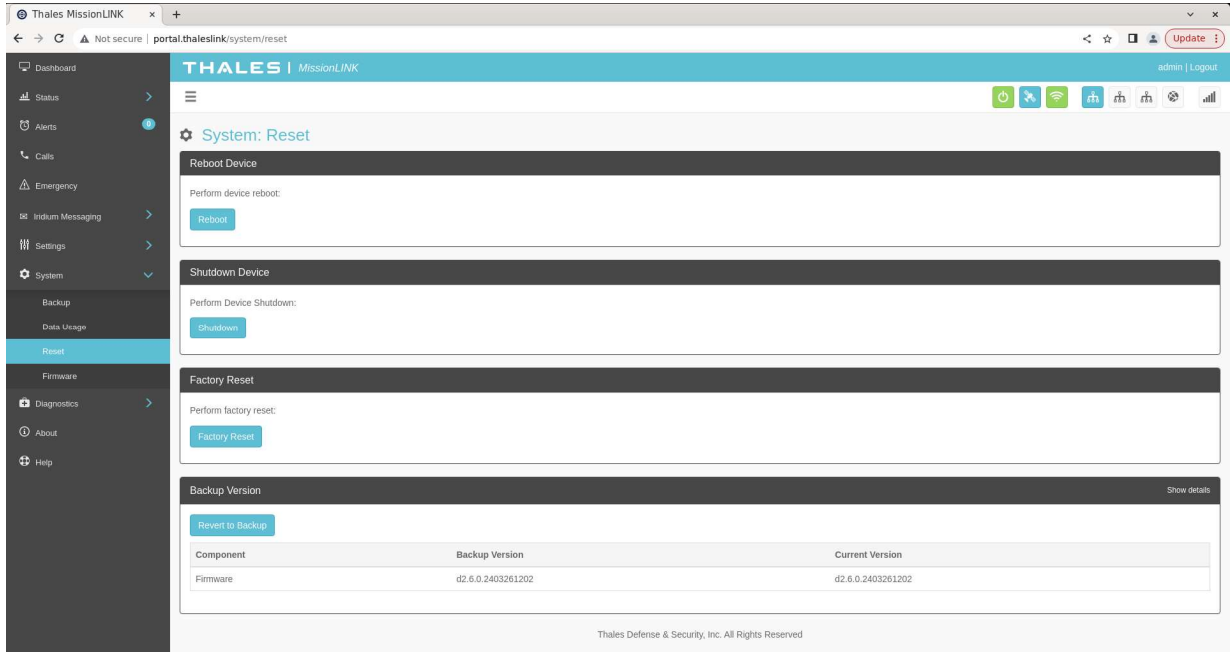
Figure 4-3652 System→ RESET

Factory Reset will restore factory defaults and all users' customized settings will be lost. It is advised to back up your configuration before performing a Factory Reset. See **Error! Reference source not found.**9 for configuration backup and restore.

NOTE

Firmware

Refer to Figure 4-53. The Firmware page displays the current firmware version numbers. These may be helpful if customer service is contacted to resolve an issue.
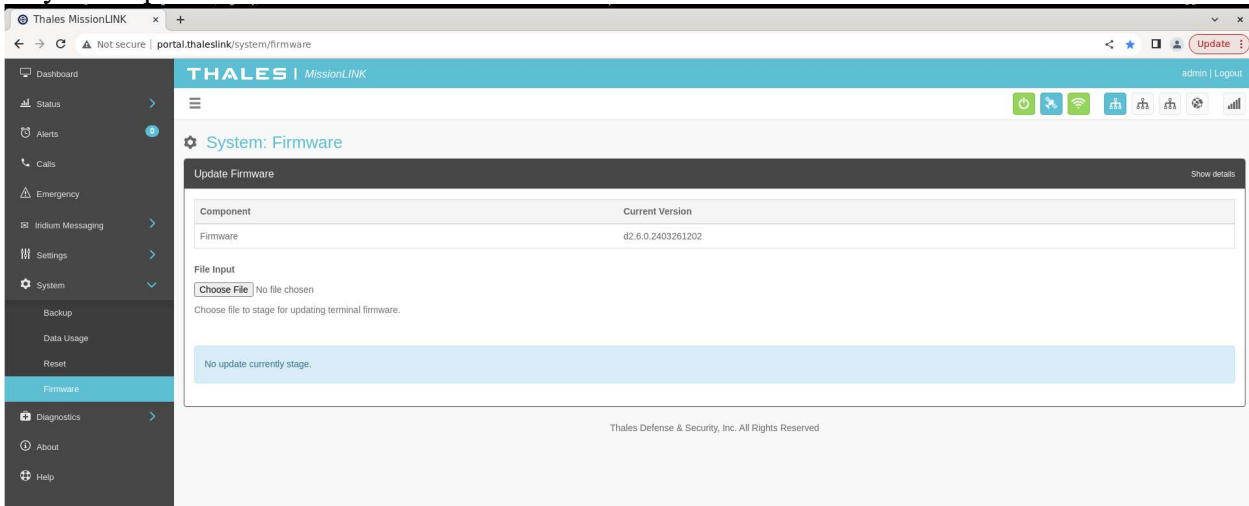
Figure 4-53 System→ Firmware Screen

Selecting the SHOW DETAILS will display system level information (Figure 4-54).
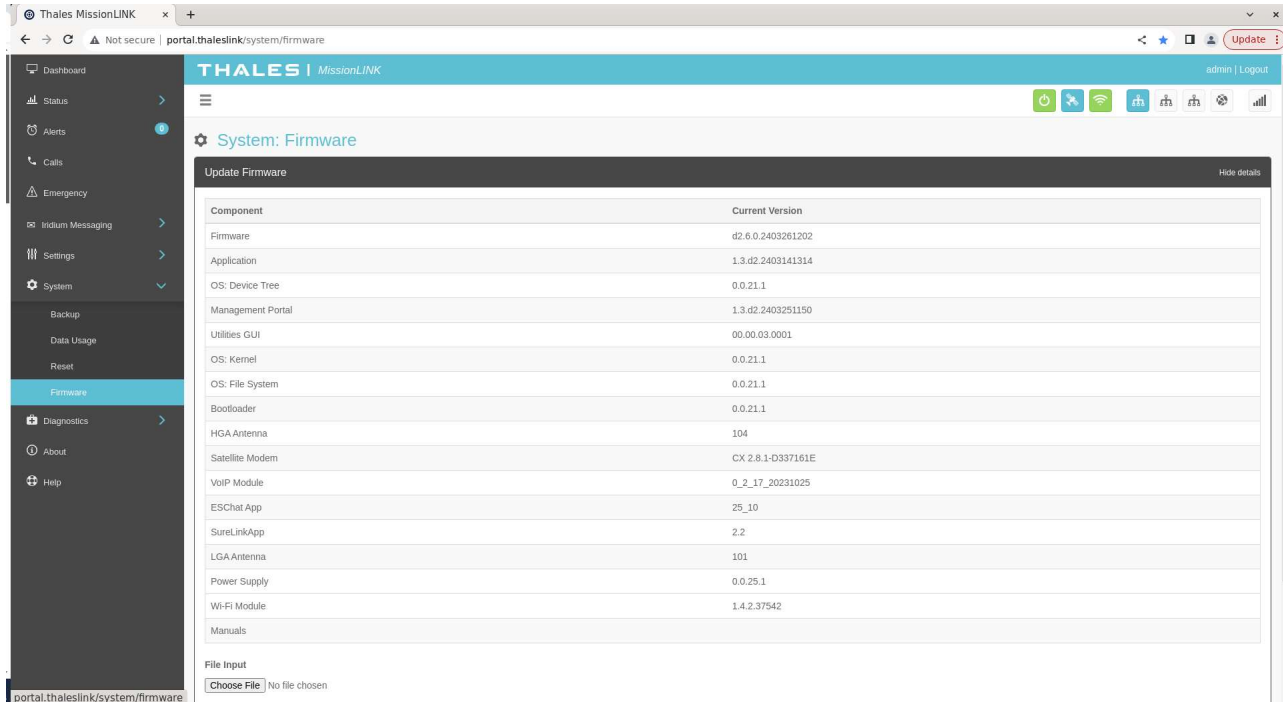
Figure 4-54 Firmware Screen – Show Detail

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

Diagnostics

Self-Test

> **ℹ️ NOTE**
>
> This is an ADMIN function 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 (Figure 4-55), users will be able to run a diagnostic test of the system and results will be available in the diagnostic logs page for debug.
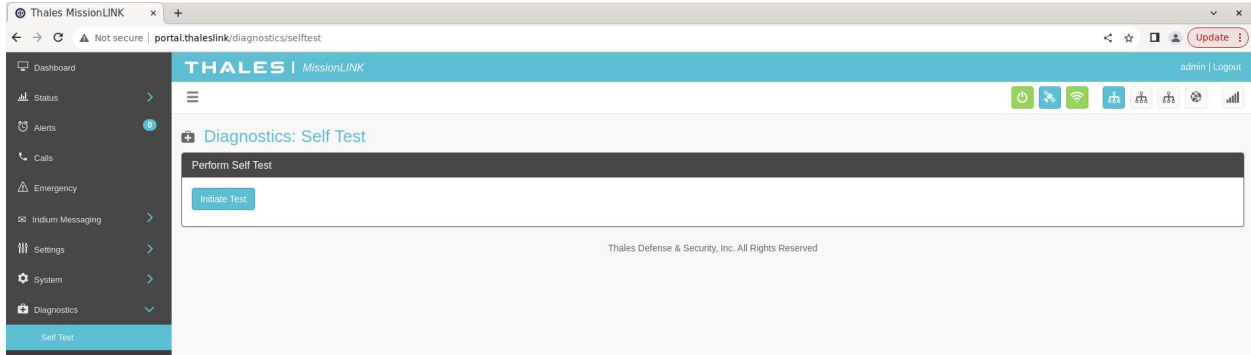
Figure 4-55 Diagnostics➔ *Self-Test Screen*

Refer to Figure 4-56. Select INITIATE TEST and then confirm by selecting YES, TEST to perform the self-diagnostics test.

 NOTE Running the Built-in-Test will render the unit unusable for several minutes. Any on-going calls or data sessions will be dropped.
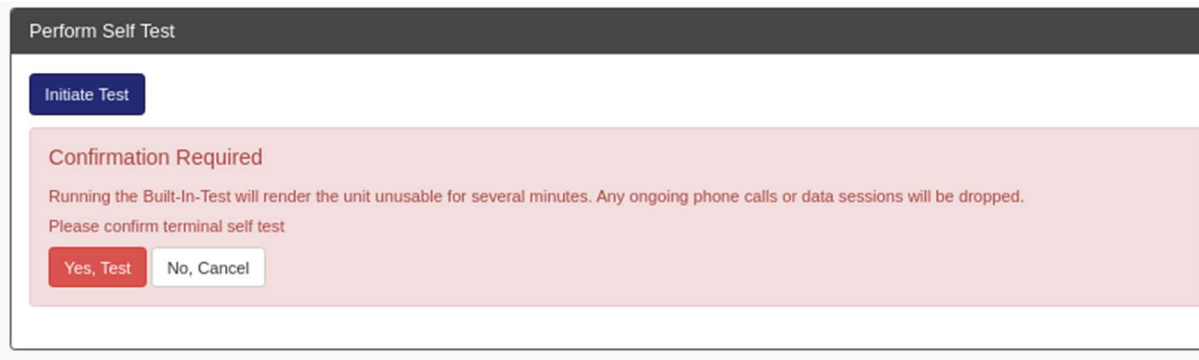
Figure 4-56 Perform Self-Test Confirmation

Once the Self-Test is complete, you will be directed to refer to the system logs for results of the test (Figure 4-377).
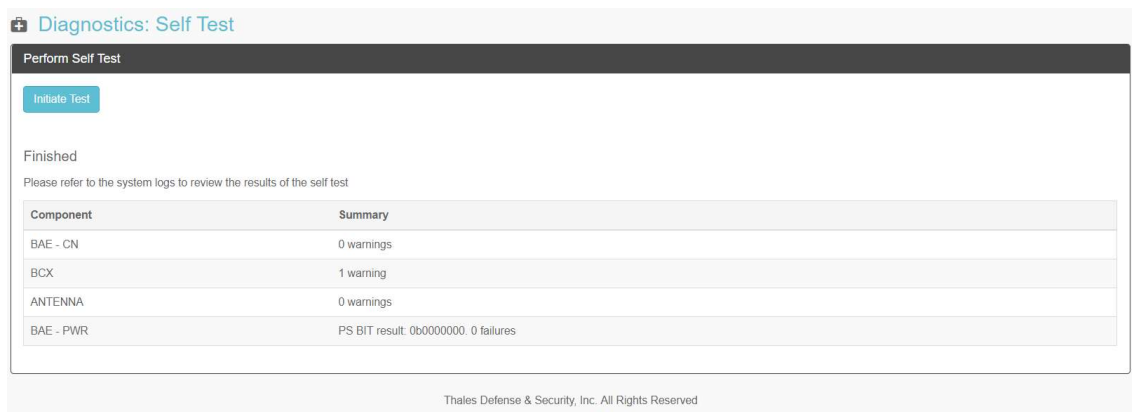
Figure 4-377 Perform Self-Test Completed Screen

User Manual PN 84468 Rev N

Diagnostics Logs

Refer to Figure 4-8. The Diagnostics Logs provide the operator with the results of all recent diagnostic tests. This information can be used in debugging / troubleshooting the system. A limited number of logs can be viewed on the screen or detailed logs can be downloaded by selecting DOWNLOAD LOGS. Logs can be erased by selecting DELETE LOGS.
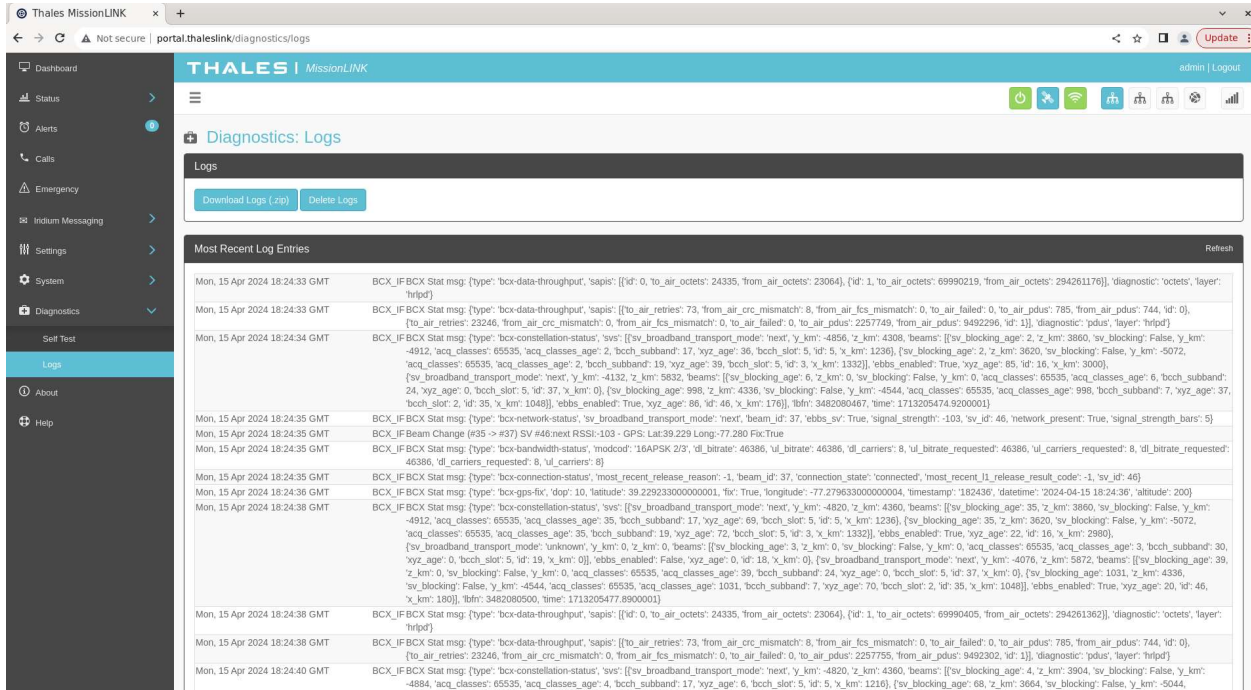
Figure 4-388 Diagnostics→ Logs Screen

The "Most Recent Log Entries" only shows the last 50 log entries. For additional information, select DOWNLOAD LOGS (.zip) for additional information.

NOTE

About

Refer to Figure 4-9. This page provides detailed information relating to the equipment, including unique HW information and its current software version.

This includes,

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

Figure 4-399 About Screen (Example)

Help

This Help page, shown in Figure 4-60, provides access to all manuals and links to customer support.

This section includes:
- User Manual
- Quick Start Guide
- Installation Guide
- SureLINK Handset
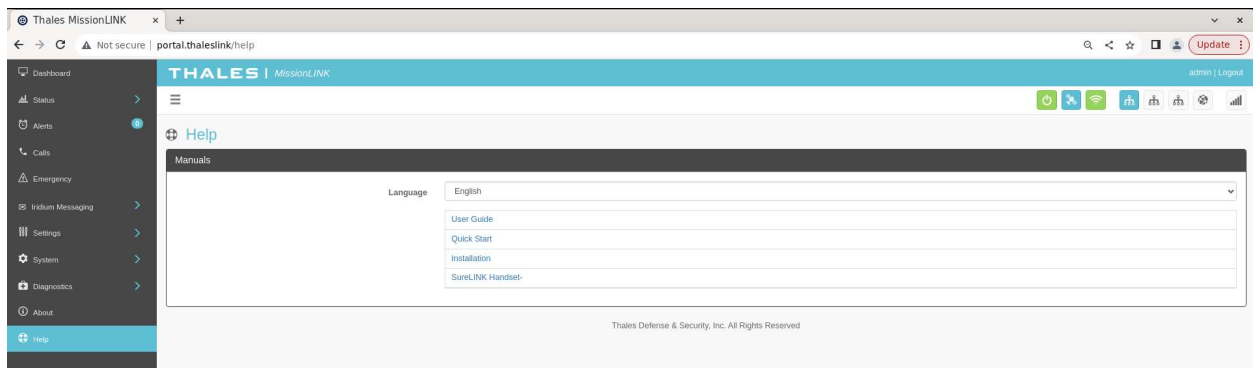
Figure 4-60 Help Screen (Example)

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. 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 reverting to the previous software version.

(i)
NOTE
For SW reset or returning to factory defaults please refer to Chapter 6 → RESETS.

INSTALLING THE FIRMWARE ON MISSIONLINK

Via Computer or Mobile device.

1. With PC or Mobile Device connect to "ThalesLINK" on Wi-Fi or via Ethernet (RJ-45) port.

2. Open a web browser and type: http://portal.thaleslink (or https://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)
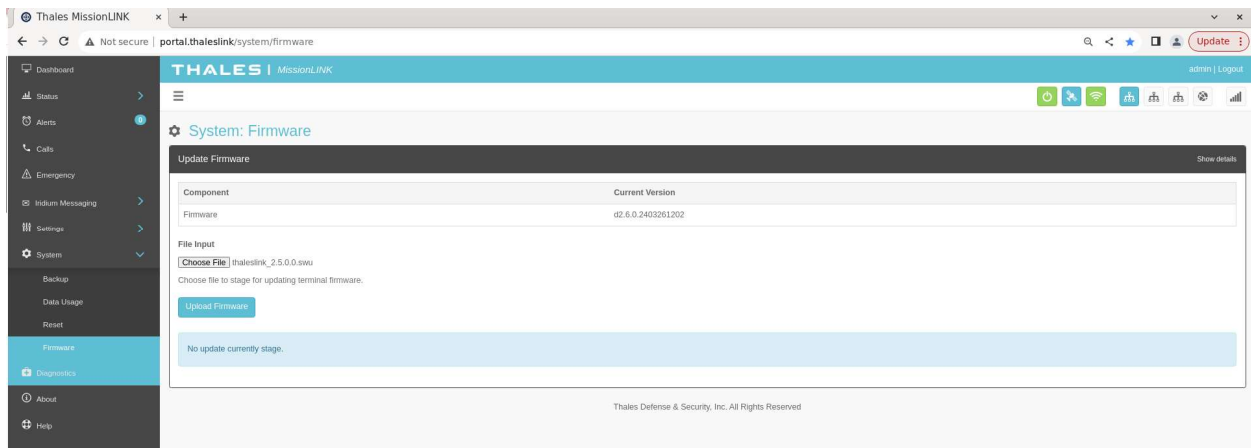
Figure 5-1 System→ Firmware

5. Select CHOOSE FILE.

6. Go to File Input and select the Browse button.

7. Navigate to location of downloaded file. This file should have the firmware version and ".swu" as the file extension

   o   Example: thaleslink_1.1.0.1.swu

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).
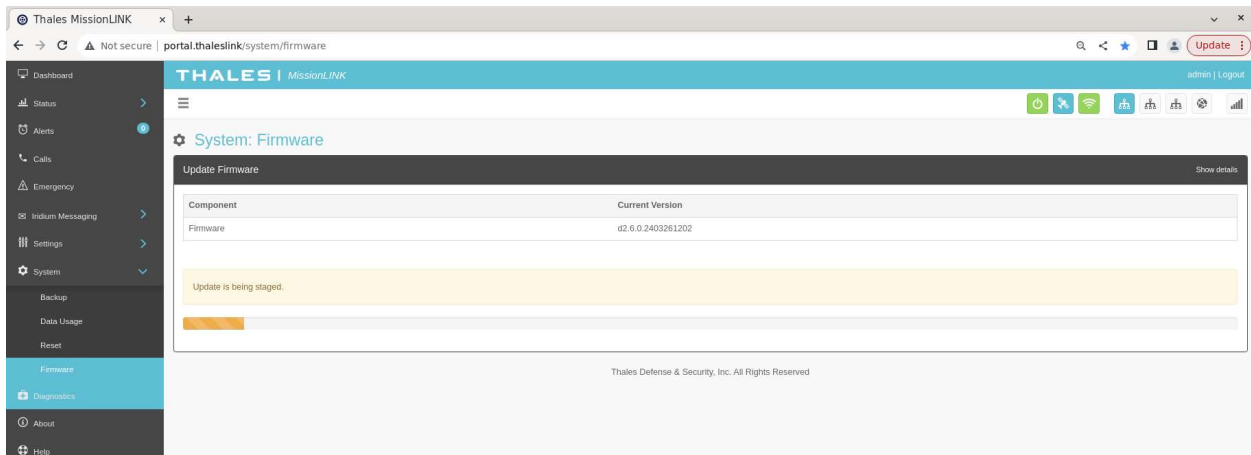
Figure 5-2 Firmware Being Staged

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 "Yes, Update".
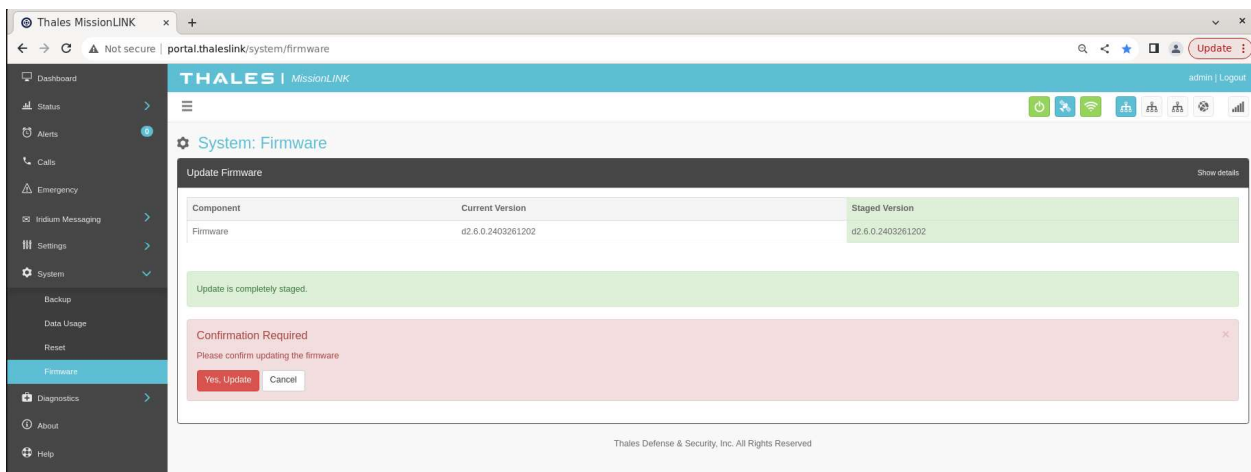
Figure 5-3 System→ Firmware Update Confirm

13. Once YES, UPDATE is selected, the process to Update Firmware has begun and will take approximately 10 to 15 minutes to complete. ***DO NOT REMOVE POWER DURING THIS PHASE***
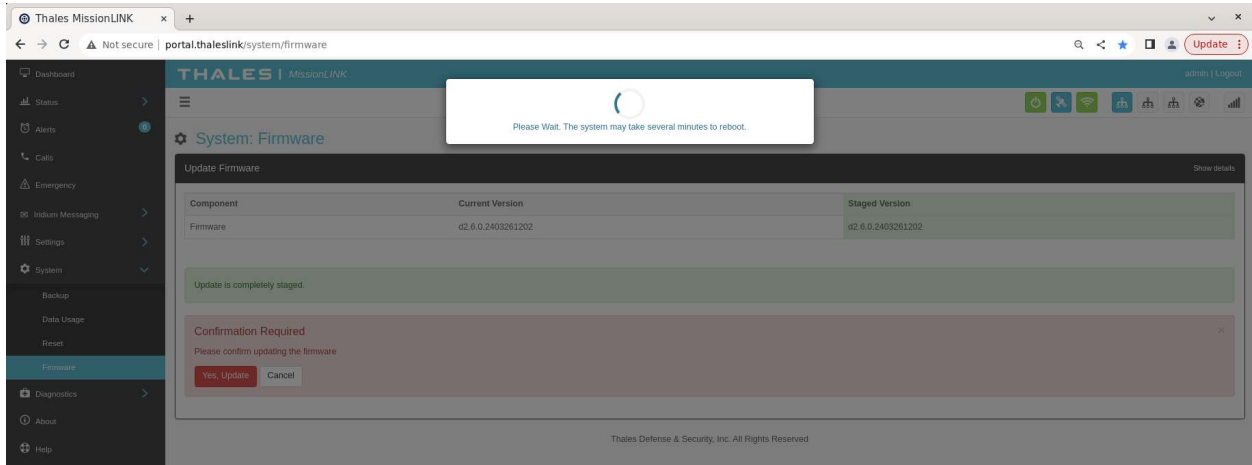
Figure 5-4 Firmware Update in Process

14. Once completed and the system reboots, wait for <u>all the Status LEDs</u> to go Solid Green and/or Blue. This may take a few more minutes.

15. Verify Firmware Update by connecting to "ThalesLINK" (or SSID set in MissionLINK) on Wi-Fi or Ethernet port.

16. Open a web browser and type: http://portal.thaleslink (or https://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.)

Figure 5-5 System➔ Firmware Update Completed (Example)

i

NOTE

Once the firmware upgrade for MissionLINK is completed, the web browser cache will need to be cleared.

CHAPTER 6   MAINTENANCE

GENERAL

This chapter provides operator maintenance instructions for the TU and BAA. This includes, preventive maintenance and troubleshooting procedures.

PREVENTIVE MAINTENANCE

Inspection and Cleaning
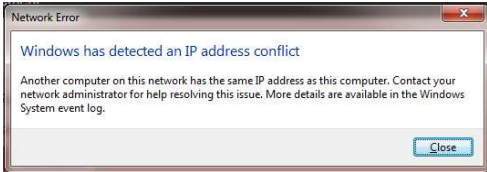
The equipment should be occasionally inspected for external damage, such as bent connectors and wear items, such as loose attaching hardware. The equipment should be cleaned periodically, particularly after exposure to salt water, sand, or mud. With the TU turned off, use a slightly damp rag (water only) to clean the TU and/or BAA. If water ingress is detected, air dry (or dry with low pressure air (if available)) to allow the unit to dry prior to applying power.

TROUBLESHOOTING

Table 6-1 Troubleshooting

PROBLEM	SOLUTION
🛰 Satellite LED Flashing GREEN	• 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. • Reboot TU.
🛰 Satellite LED Flashing RED	• Critical Fault Detected. Open Management Portal http://portal.thaleslink (or https://portal.thaleslink) and check Alerts. Make any adjustments. (For example: check antenna connection, or GPS not acquired.) • Turn unit off and on again. If same result, contact your service provider.
⏻ System LED Flashing Green	• 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 • Switch power off and back on if the light doesn't turn solid green after 5 minutes.
⏻ System LED Solid YELLOW	• The unit has a warning indicating a minor issue that should not affect performance. Open the management portal, check alerts, and make any adjustments needed.

PROBLEM	SOLUTION
⏻ System LED Flashing RED	• Fault Detected. Open Management Portal http://portal.thaleslink (or https://portal.thaleslink) 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.) • Turn unit off and on again. If same result, contact your service provider.
⏻ System LED Flashing MAGENTA	• A defective fault is detected. This is associated with a processor not booting correctly. If system reboots, factory resets, or software reverts don't clear the issue, contact your service provider.
📶 Wi-Fi LED	• OFF – Turn Wi-Fi ON using the Management Portal through a hardwired, PoE connection. ThalesLINK > Settings > Wi-Fi • Solid RED – Wi-Fi may need to turned off and back on again from the Management Portal. If the LED does not turn to GREEN within a minute, reboot the TU. • Flashing GREEN – If this continues for more than a minute or two, check for NO OR WEAK Wi-Fi
Call Logs are not appearing	• Call logs must be enabled. Verify call logs are enabled (SETTING → PHONE → PHONE CONFIGURATION)
Calls unexpectedly drop when using Gateway	• Verify that the Gateway number is not assigned to any other phone. If it is, your Gateway call may drop unexpectedly. To correct this, remove the duplicate number.
Cannot connect to the internet	• Data sessions default is OFF. Check to make Satellite Data Sessions is ACTIVATED on Dashboard. If not, select ACTIVATE and then APPLY next to SATELLITE DATA SESSION.

PROBLEM	SOLUTION
Cannot connect to the Management Portal	• You may need to clear your browser cache. • Ensure Terminal Unit is powered ON • Ensure Wi-Fi is enabled and connected to ThalesLINK (or renamed SSID). If using a Wi-Fi enabled device, the Wi-Fi LED on the TU should be solid GREEN. If not using Wi-Fi, 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 • Open web browser and type http://portal.thaleslink (or https://portal.thaleslink). Ensure network settings are correct on the connected device. • Device's browser may be incompatible. Update or try different browser. • You may need to reconnect via Ethernet or Wi-Fi to the TU. • Check to make sure the correct address is typed in http://portal.thaleslink (or https://portal.thaleslink) • If system LED is flashing GREEN, wait until it turns solid GREEN, then try reconnecting to the portal.
Cannot connect to Wi-Fi service	• Check that the Wi-Fi antenna is attached and tightly screwed in. • Check that the TU's Wi-Fi LED is solid GREEN. • Check to see if there's an available connection by checking the devices that are connected in Status → Current Devices page. • Only 3 simultaneous devices can connect to the Wi-Fi. Any additional connection attempts are blocked. • Remove one or more devices from the Wi-Fi and try again to connect. • Use the Wi-Fi Device Whitelist to limit access to specific wireless devices. • Verify that the SSID has NOT been disabled. If disabled, enable the SSID. If the device does not "automatically" reconnect, then manually reconnect by adding the network on the device. Refer to device user manual for instructions on how to do this.
Network Error	• If you receive a message similar to this, another user is attempting to use the same IP Address as your computer.

PROBLEM	SOLUTION
No or Weak Wi-Fi Signal	• Connect Wi-Fi antenna and ensure it is secured tightly • 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 • Check to make sure Wi-Fi device is connected to the TU's Wi-Fi and verify that you are connected to the ThalesLINK. • Check the Management Portal to make sure the Wi-Fi device is registered as a user.
MissionLINK is not obtaining a satellite signal (Satellite LED is red)	• 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. • 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. • Check antenna for a clear view of the sky with no obstructions. Relocate antenna if needed. • 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. • Move vehicle to a new location and retest if other interfering vehicles are in the area • Reboot TU and check the Alerts. • Call Service Provider if the satellite connection is still not working.
Terminal Unit does not Power-ON	• Check TU for Green lights, If green light is on Unit has Power • Push power button on front of TU. • Check that the power source is providing 10-32V and is not current limited. • Check connection of the 10-32V DC cable has correct polarity. • Check to ensure Ignition line is connected to switched line or connected to Red (Positive line) for continuous operation. • Check that ignition or remote switch is turned on if ignition line is connected. • If using AC/DC converter, make sure the AC outlet has power and that the plug is securely in the AC outlet and the other end is securely connected to the TU.

PROBLEM	SOLUTION
Terminal Unit has power but accessories not working	• 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. (Note: This applies to all accessories, EXCEPT the antenna. Do not disconnect the antenna while booting up the system.) • If PoE accessory not receiving power, make sure PoE is enabled for that port. • PoE is not available on WAN port. Any device on WAN port needs its own power source. • Check VoIP phone manuals for proper configuration. Each phone may have a different configuration method.
Terminal Unit is not responding	• 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. • Reboot the system and recheck for any Alerts that may have been generated. • Call Service Provider if the TU is still not responding. • 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. NOTE: This is not recommended as a routine troubleshooting measure. All user data and debug information will be lost and factory defaults returned.

System Resets

In a rare situation where the MissionLINK system is not responding or operating properly, it may be necessary to reset the system. There are varying levels of system resets that are explained below:

Power Cycle

There are four (4) ways to power cycle the system:
- If power is already on (LEDs are illuminated), press and hold the Power Button on the unit until the unit turns off. Again, press and release the Power Button to power the unit on. It will take a few minutes before the boot-up cycle completes.
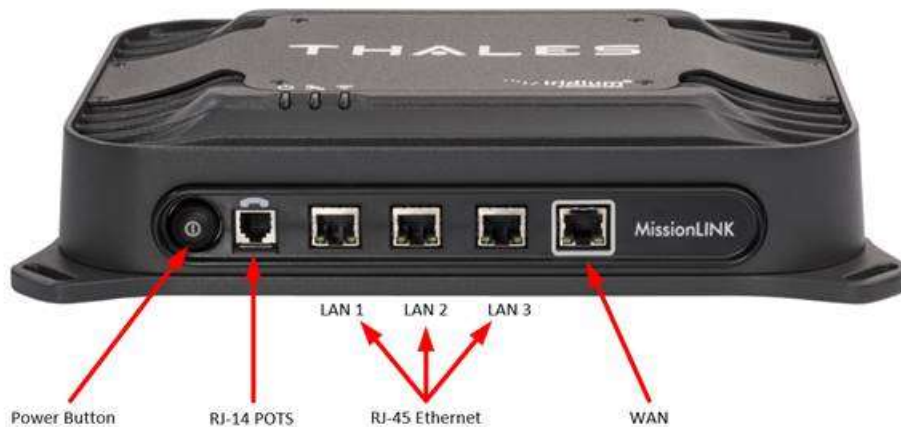
Figure 6-1 Location of Power Button on Terminal Unit (TU)

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

- From the Management Portal, select SYSTEM → RESET→ SHUTDOWN. Press SHUTDOWN. The system will turn off but not boot back up. Pressing the Power Button will turn the system back on.

- If neither of these work, then unplugging the system from the power source may be necessary. Note: Always wait at least 20 seconds for power inside the unit to dissipate before reconnecting the input power.
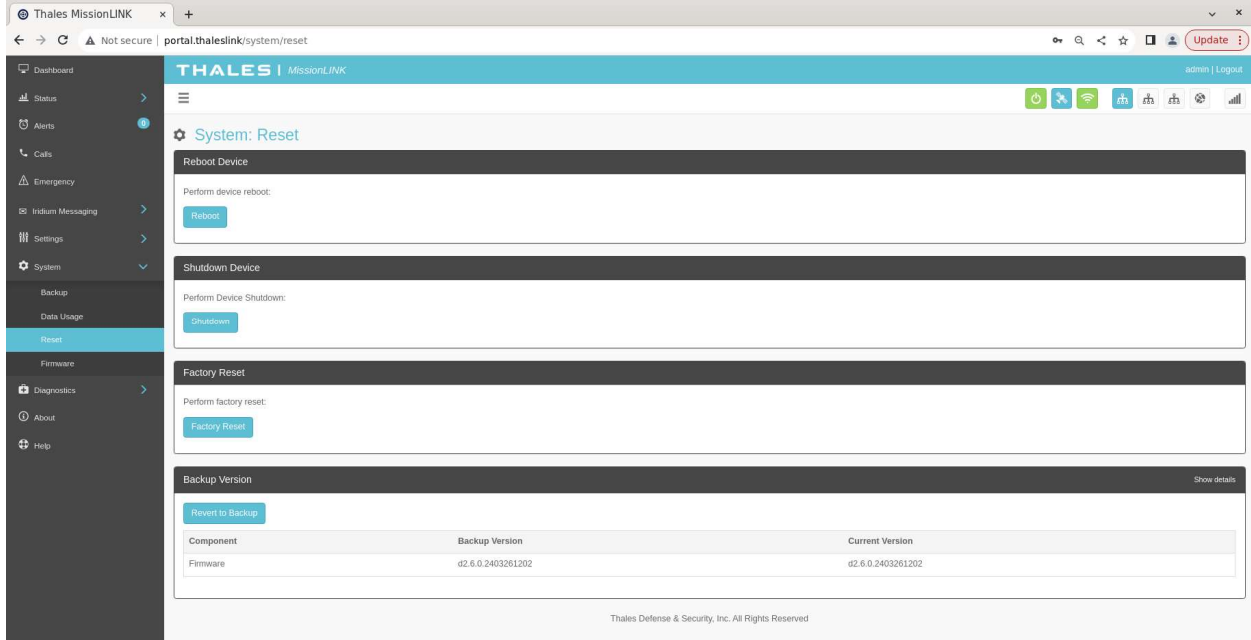
Figure 6-2 Management Portal - SYSTEM → RESET

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. After clearing all the user configuration, it will reboot the terminal a couple of times to reset the internal components correctly. This may take several minutes. Once it is complete, the System Status LED will be solid green. You can then log into the Management Portal using the default password and change settings as desired.

Factory Reset can be accomplished by either of these two actions:
- Remove the SIM card cover exposing the reset hole. Power up the TU and wait until the System LED stops blinking green. Using a straightened paperclip, insert it into the round hole just to left of the SIM card as shown in Figure 6-3. Push straight in **gently** until the paperclip causes the switch to click and hold until LEDs flash. A factory reset will occur which takes up to 5 minutes until the system is reconfigured and boots up completely.
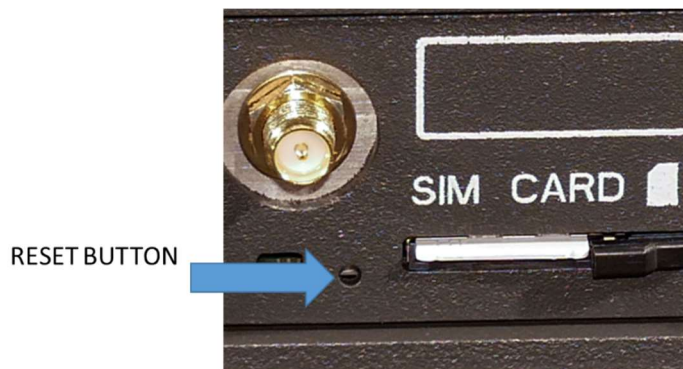
Figure 6-3 Reset Button

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

Firmware Revert

> **i**
> **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.
- From the Management Portal select SYSTEM → RESET→ FIRMWARE REVERT. Confirm by selecting YES, FIRMWARE REVERT. The TU will reboot into the previous firmware version.

If the unit will not boot to access the Management Portal, a Firmware Revert can be accomplished by following these steps:

- Power down the system.

- 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 straight in **gently** until the paperclip causes the switch to click. At the same time turn the unit ON by pressing the power button. Hold the paperclip 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; performance maybe degraded.	Critical	Cable loss may exceed the system spec of 10 dB	Check Antenna cable for damage or loose connections. Replace if necessary.
ANT_MISSING	Unable to detect antenna	Fault		Check Antenna for damage. Check for loose connections. Remove and reinstall the antenna. If problem continues, the antenna may need to be replaced.
ANTENNA_POST_FAIL URE	The antenna has failed POWER ON SELF TEST	Fault		Check Antenna for damage. Check for loose connections. Remove and reinstall the antenna. If problem continues, the antenna may need to be replaced.
ANT_WRONG_VER	The antenna is running incorrect version	Warning		Restart TU. Contact representative if problem persists.
APPROACHING_MAX_T EMP	System approaching maximum internal temperature - the terminal may reboot.	Critical	A system component may exceed the maximum internal temperature of 85 C. The terminal may automatically shut off.	Move TU to a cooler area or allow to cool down prior to further operations.
BCX-denial	Failed to connect to pass data, reason – location	Fault		Restart TU. Contact representative if problem

Alert Name	Description	Level	Additional Information	Corrective Action
				persists for more than 4 hours.
BCX_IBIT_FAILURE	The BCX has failed "Initiated Built In Self-Test" View Logs for details.	Fault		Open http://portal.thaleslink (or https://portal.thaleslink) and review Self-Test logs. Restart the TU. If problem persists, contact representative.
BCX_SIM	Modem failed to read SIM card	Fault		Remove, clean and re-insert SIM. Contact service provider if problem persists.
BCX_WRONG_VER	The modem is running an incorrect version.	Warning	The modem is running an outdated software version. The system will still function.	Restart TU and contact representative if problem persists.
DATA_WARN	The data cap has been reached.	Warning	The user specified data cap has been reached. Data will continue to pass.	Reset data cap, or wait until Reset Day.
IMT_CONN	Failed to connect to IMT server, check BCX Status or BCX version	Fault		Restart TU. Contact representative if problem persists.
MODEM_ACT	Modem returned an unknown error – cannot activate	Fault		Restart TU. Contact representative if problem persists.
MUX_PLL_UNLOCKED	Antenna mux out-of-lock with the modem.	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 http://portal.thaleslink (or https://portal.thaleslink)

Alert Name	Description	Level	Additional Information	Corrective Action
				and review Self-Test logs. Contact representative.

Alert Name	Description	Level	Additional Information	Corrective Action
PWR_POST_FAILURE	The power has failed "Power On Self-Test". View logs for details.	Fault		Open http://portal.thaleslink (or https://portal.thaleslink)and review Self-Test Logs. Contact representative.
SIM_MISSING	SIM card not detected	Fault	SIM Card is physically missing	Insert or replace SIM card
TIME_INVALID	The system time is not properly set.	Warning		Open http://portal.thaleslink (or https://portal.thaleslink) and Synchronize Time on the Settings: GNSS page. Restart the TU.
VOIP_FAULT	The core node reports a fault.	Fault	The system may still operation.	Restart TU. Contact representative if problem persists.
VOIP_OFF	Core node is powered off, restart required	Defective	Core Node is noticed to be unexpectedly off.	Restart TU. Contact representative if problem persists.
VOIP_REBOOT	Core Node Reboot has occurred, full system restart is required.	Warning	Core Node Module restarts while the system is up and running.	Restart TU. Contact representative if problem persists.

CHAPTER 7   TECHNICAL SPECIFICATIONS

TECHNICAL SPECIFICATIONS

Table 7-1 Technical Specifications

Description		Parameters	
Technical			
Frequency of Operation	Uplink (TX)	1616 to 1626.5 MHz	
	Downlink (RX)	1616 to 1626.5 MHz	
Channelization	FDMA spacing	41.667 KHz	
	TDMA Timing	8.3ms Slot in a 90ms window	
	Channels Available	240 channels	
		Certus 200	**Certus 350**
EIRP (Weighted Average)	Voice	9 dBW	9 dBW
	Data Certus™ 2xC8 QPSK	12 dBW	-
	Data Certus™ 1xC8 16 APSK	-	15.2 dBW
	Data Certus™ 2xC8 16 APSK	-	18.2 dBW
	Certus™ C1, C8 Voice/Data	QPSK	QPSK
	Certus™ C8 APSK Data	-	16 APSK
Antenna	Type	Single passive element	Electronically steered phased array
	Polarization	RHCP	RHCP
	Gain	1 dBi	9.5 dBi
	Beam Width	Omnidirectional	31° typical per beam
	MissionLINK coverage	8° to 90° elevation	8° to 90° elevation
Power			
Main Power (AC/DC Power Adapter)	AC Input Voltage	100-240 VAC	
	Frequency	50/60 Hz	
	DC Output Voltage	12 VDC	
	Max Power	120 Watts	
DC Input 10-32VDC	Voltage	10-32 VDC	
	Max Current	12 Amps (10V) – 3.75 Amps (32V)	
	Max Power	120 Watts	
DC Input 12 VDC	Voltage	12 VDC (+10%/-5%)	
	Max Current	10 Amps	
	Max Power	120 Watts	
Ethernet	3x PoE	PSE Class 2 (6.5 Watts each)	
Environmental		**Certus 200**	**Certus 350**
Antenna	IP Rating	IP67	IP66
Terminal Unit	IP Rating	IP31	

TEMPERATURE

Table 7-2 Operating and Storage Temperatures

Description		Temperature Range
Broadband Active Antenna	Operating Temp	-40°C to +55°C
	Storage Temperature	-60°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	
		Certus 200	**Certus 350**
Broadband Active Antenna	Dimensions	5" D x 5.5" H (12.5 cm x 14 cm)	14" D x 4" H (35.6 cm x 10.2 cm)
	Weight	1.1 lbs. (0.5 kg)	6.2 lbs. (2.8 kg)
Terminal Unit	Dimensions	12" L x 9" W x 3" H (30.5 cm x 23 cm x 7.6 cm)	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)	7.5 lbs. (3.4 kg)

CONNECTOR DETAILS

General Purpose Inputs / Outputs (GPIO)

Refer to Figure 7-2 for the connector and its pinout. The connector is located on the back of the TU and is labeled I/O. The GPIO has 4 main functions. Some of the functions are reserved for this connector are not yet implemented (they are reserved for future use.) Refer to Table 7-2 for the pin descriptions of the GPIO connector.

1. **1-Wire Emergency→** 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 Emergency 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, it will increase frequency of transmission to every 10 seconds.

   NOTE: THERE IS NO LOCAL INDICATION OF AN EMERGENCY MESSAGE BEING SENT

This security feature is for user protection. **The ONLY way to remove an active emergency message is to enter Management Portal under EMERGENCY TAB**

2. **Radio Gateway** → Advanced users can connect Land Mobile Radio I/O to send and receive voice and Push-To-Talk (PTT) calls over the MissionLINK. This feature is for advanced users familiar with Land Mobile Radio systems and requires a custom cable connection between the GPIO connector (DB-15) and the target Radio (cables not offered by TDSI).   Because each radio system will require a unique setup, it is highly recommended that you contact your TDSI representative for help in setup of this advanced user feature. See pinout (Figure 7-2) for creating the custom Radio Gateway cable. Refer to Table 4- for settings related to the Radio Gateway.
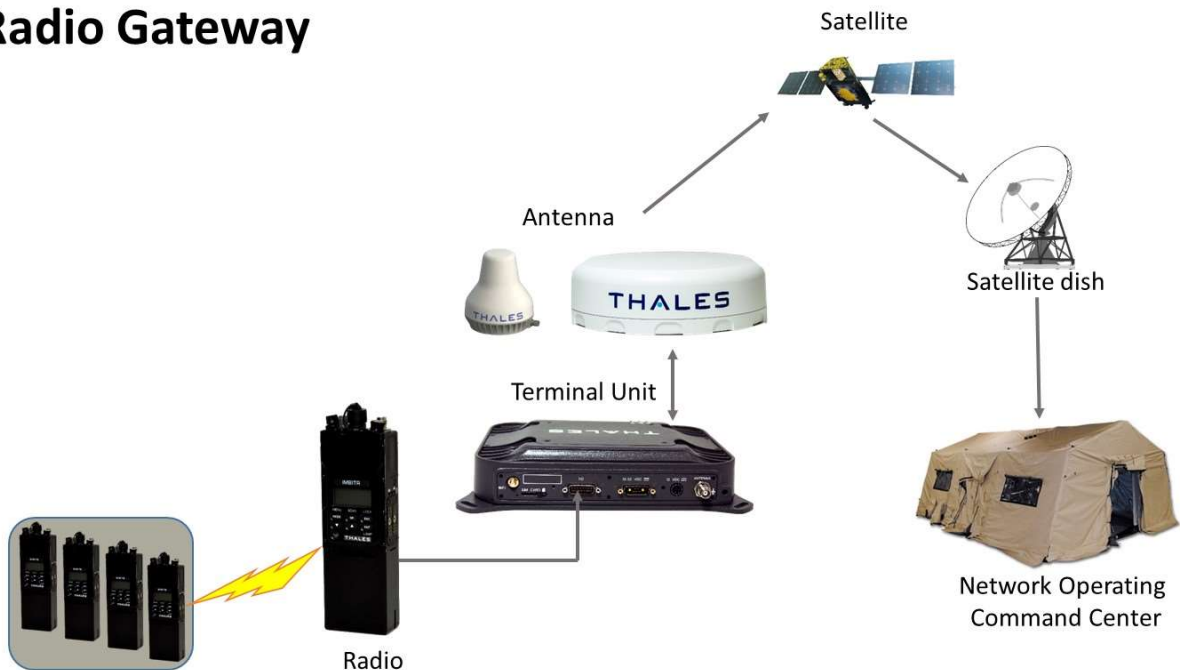
Figure 7-1 Radio Gateway for Advanced Land Mobile Services

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

The DB-15 connector with Pin out shown in Figure 7-2.
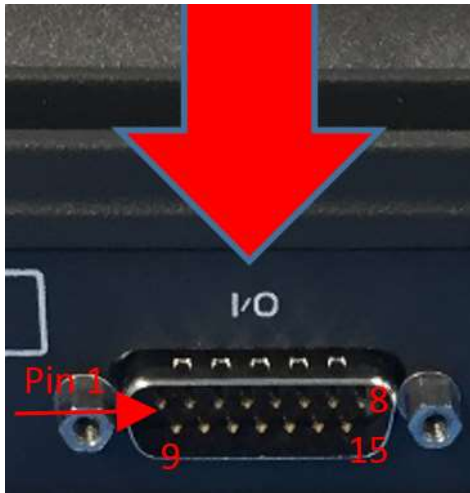
Figure 7-2 GPIO Connector Pin Detail

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	EMER_IN	Emergency remote functionality, Ground pin to activate internal Emergency
6	GPI01	Software configurable GPIO pin #1
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)
11	RadioPTT	Radio Gateway functionality, Output 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
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.

PIN NO	OUTPUT
2, 4	+V
1, 3	-V

VIEW INTO END OF MATING CONNECTOR

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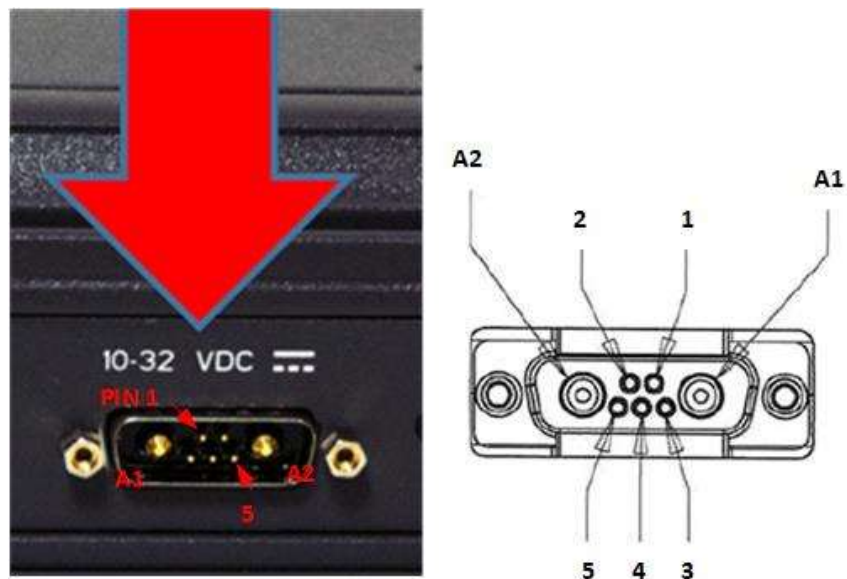
Figure 7-4 10-32 VDC and Mating Connector Detail

THIS PAGE INTENTIONALLY LEFT BLANK

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
ESP	Encapsulated Security Packet
ETSI	European Telecommunications Standards Institute
FR	Fire Rated
GNSS	Global Navigation Satellite System
GPIO	General Purpose Inputs/Outputs
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
HGA	High Gain Antenna
HRLP	High Speed Radio Link Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
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
msec	Milliseconds
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

Acronym	Description
PSTN	Public Switched Telephone Network
PTT	Push To Talk
QSG	Quick Start Guide
R/W	Read/Write
RF	Radio Frequency
RGW	Radio Gate Way
SBC	Smart Battery Charger
SDF	Secondary Data Flow
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
VAD	Voice Activity Detection
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)

Acronym	Description	
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
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 704 kbps 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
HTTPS	Hypertext Transfer Protocol Secure	HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.
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 LGA supports the Certus™ 100 and Certus™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.
PTT	Push To Talk	Two way radio term indicating the pressing of a button to initiate transmit before speaking
R/W	Read / Write	Read / Write Capability
RGW	Radio Gateway	Radio Gateway feature enables communication between telephone users and users of ground radios.
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

Acronym		Description
		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
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   KIT CONTENTS AND ACCESSORIES

MISSIONLINK KIT CONTENTS AND ACCESSORIES

The following tables list the kits available for purchase and their contents as well as accessories and spare parts that can be purchased separately.

Table 9-1 Standard Kit, MissionLINK Certus 350, List of Equipment

Part Number			Description
MF350BV			Standard Kit, MissionLINK® Certus 350**
	Qty	Part Number	Description
✔	1	1100789-501	Kit, Terminal Unit, Mounting Hardware
✔	1	1100790-501	Kit, Antenna Magnetic Mounts
✔	1	1100792-501	Kit, Antenna Mounting Hardware
✔	1	1600899-1	Broadband Active Antenna (BAA), Certus 350
✔	1	3402174-1	Quick Start Guide (QSG) MissionLINK®
✔	1	3900011-1	Mounting Template, Terminal Unit
✔	1	3900013-1	Mounting Template, BAA
✔	1	4102947-512	Terminal Unit, MissionLINK ®
✔	1	855021-010	RF Cable, 10 ft LMR240
✔	1	855024-003	Cable, Vehicle DC Power Harness, 3 ft.
✔	1	855026-010	Cable, RJ-45 Ethernet, 10 ft.
✔	1	85728-001	Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi

** The MF350BV is capable of up to 352 kbps uplink and 704 kbps downlink speeds.

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

Table 9-2 Base Kit, MissionLINK Certus 350, List of Equipment

	Part Number		Description
	MF350BV-1		Base Kit, MissionLINK® Certus 350
	Qty	**Part Number**	**Description**
✔	1	1600899-1	Broadband Active Antenna (BAA), Certus 350
✔	1	3402174-1	Quick Start Guide (QSG) MissionLINK®
✔	1	3900011-1	Mounting Template, Terminal Unit
✔	1	3900013-1	Mounting Template, BAA
✔	1	4102947-512	Terminal Unit, MissionLINK ®
✔	1	85728-001	Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi

Table 9-3 Certus 200 Base Kit, List of Equipment

	Part Number		Description
	MF200BV-1		Kit, MissionLINK® Vehicular Low Gain 200 Base
	Qty	**Part Number**	**Description**
✔	1	1600951-1	Broadband Active Antenna (BAA), Certus 200
✔	1	3402174-1	Quick Start Guide (QSG) MissionLINK®
✔	1	3900011-1	Mounting Template, Terminal Unit
✔	1	4102947-522	Terminal Unit, MissionLINK ®
✔	1	85728-001	Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi

Table 9-4 Available MissionLINK® Accessories

Description	Part Number	Qty
19" Rack Mount Shelf Kit	1100796-501	1
Kit, Antenna Magnetic Mounts (Certus 350 only)	1100790-501	1
Kit, Antenna Magnetic Mounts (Certus 200 only)	1100856-501	1
Antenna Premium L-Bracket Pole Mount Kit (Certus 200 only)	1100855-503	1
Kit, Antenna Mounting Hardware (Certus 350 only)	1100792-501	1
Kit, Terminal Unit, Mounting Hardware	1100789-501	1
Mounting Template, Terminal Unit	3900011-1	1
Mounting Template, BAA (Certus 350 only)	3900013-1	1
Thales SureLINK IP Handset Kit	1100818-501	1
Power Supply, AC/DC 12V – 160W	84670-001	1
Cable AC Power with USA Plug Type B IEC 60320-C13 Connect Blk 6 ft.	854024-001	1
Cable AC Power with Euro Plug Type E IEC 320-C14 Connect Blk 6 ft.	854025-001	1
Cable AC Power with AUS Plug Type 1 IEC 320-C14 Connect Blk 6 ft.	854026-001	1
Cable AC Power with UK Plug Type G IEC 320-C13 Connect Blk 6 ft	854027-001	1
RF Cable: 10 ft., LMR240	855021-010	1
RF Cable: 20 ft., LMR240	855021-020	1
RF Cable: 30 ft., LMR240	855021-030	1
RF Cable: 50 ft., LMR240	855021-050	1
RF Cable 100 ft., LMR400	855022-100	1
RF Cable, Coaxial 25m LMR300 Fire Rated	855023-082	1
RF Cable, Coaxial 50m LMR400 Fire Rated	855033-164	1
Cable, 10-32Volt DC Power Harness	855024-003	1
Cable, RJ-45 Ethernet, 10 ft.	855026-010	1
Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi	85728-001	1

Note: The above accessories are compatible with both Certus 200 and Certus 350 systems unless otherwise noted in the description.

INDEX

THALES

T