

## Thales VesseLINK™

### 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: 42154 <ul style="list-style-type: none"> <li>Update based on Beta user feedback and Testing</li> </ul>	SJacques
Rev C	March 2019	ECN: 42532 <ul style="list-style-type: none"> <li>Update based user feedback</li> </ul>	SJacques
Rev D	Oct 2019	ECN: 42905 <ul style="list-style-type: none"> <li>Update based on s/w updates</li> </ul>	SJacques
Rev E	Jan 2020	ECN 43091 <ul style="list-style-type: none"> <li>Update based on user feedback and added 700 kbps</li> </ul>	SJacques
Rev F	May 2020	ECN: 53373 <ul style="list-style-type: none"> <li>Update based on new software release 2.1</li> </ul>	SJacques
Rev G	Oct 2020	ECN 53662 <ul style="list-style-type: none"> <li>Update based on new software release 2.2</li> </ul>	SJacques
Rev H	Feb 2021	ECN 53827 <ul style="list-style-type: none"> <li>Update to include Certus 200</li> </ul>	SJacques
Rev J	Dec 2021	ECN 54410 <ul style="list-style-type: none"> <li>Clean-up and addition of Certus200 Mounts</li> <li>Added Portuguese Radiation Statement</li> <li>Version 2.2.2 Updates</li> </ul>	SPeters
Rev K	May 2022	ECN 54666 <ul style="list-style-type: none"> <li>Updated certs for Brazil, Japan, and Mexico</li> <li>Updated pictures</li> <li>Updated features – VLAN Tagging, Satellite connection monitoring</li> </ul>	SPeters
Rev L	Sep 2022	ECN 54856 <ul style="list-style-type: none"> <li>Handset updates for PTT &amp; App support</li> <li>GPIO feature addition</li> </ul>	SPeters

### WARNING – INFORMATION SUBJECT TO EXPORT CONTROL RESTRICTIONS

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

**Export Compliance:**

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

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

**Disclaimer:**

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

**Legal Notices**

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

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

**Intellectual Property**

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

**Content Copyright**

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

**Indemnity**

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

**SOFTWARE LICENSE**

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

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

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

**Thales Product Warranty Claim Process**

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

**User Documentation:**

Thales Defense & Security, Inc. continually evaluates its user documentation for accuracy and completeness. Any suggestions you may have for changes or additions should be sent to [THALES\\_ILS@thalesdsi.com](mailto:THALES_ILS@thalesdsi.com) Subject Line: Thales VesseLINK™ User Manual (PN 84469/84469-IETM).

## Table of Contents

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>1-1</b>
INTRODUCTION .....	1-1
ABOUT THIS MANUAL.....	1-1
THE IRIDIUM SATELLITE NETWORK.....	1-1
<b>CHAPTER 2 SYSTEM OVERVIEW.....</b>	<b>2-1</b>
DESCRIPTION .....	2-1
<i>Below Deck Unit (BDU)</i> .....	2-4
<i>Antenna Unit</i> .....	2-7
RF COAXIAL CABLE INSTALLATION CONSIDERATIONS.....	2-7
<b>CHAPTER 3 GETTING STARTED .....</b>	<b>3-1</b>
GETTING STARTED .....	3-1
<b>CHAPTER 4 THALES MANAGEMENT PORTAL.....</b>	<b>4-1</b>
GETTING TO KNOW THE THALES MANAGEMENT PORTAL.....	4-2
<i>Menu Components</i> .....	4-3
<i>Main Dashboard</i> .....	4-7
<i>Status</i> .....	4-9
<i>Alerts</i> .....	4-13
<i>Calls</i> .....	4-14
<i>Emergency</i> .....	4-15
<i>Settings</i> .....	4-16
<i>System</i> .....	4-55
<i>Diagnostics</i> .....	4-60
<i>About</i> .....	4-63
<i>Help</i> .....	4-64
<b>CHAPTER 5 FIRMWARE UPGRADE.....</b>	<b>5-1</b>
INSTALLING THE FIRMWARE ON VESSELINK™ .....	5-1
<b>CHAPTER 6 MAINTENANCE .....</b>	<b>6-1</b>
GENERAL .....	6-1
PREVENTIVE MAINTENANCE.....	6-1
<i>Inspection and Cleaning</i> .....	6-1
TROUBLESHOOTING.....	6-1
SYSTEM RESETS .....	6-5
ALERTS .....	6-8
<b>CHAPTER 7 TECHNICAL SPECIFICATIONS.....</b>	<b>7-1</b>
TECHNICAL SPECIFICATIONS.....	7-1
CONNECTOR DETAILS .....	7-3
<i>General Purpose Inputs / Outputs (GPIO)</i> .....	7-3
<i>BDU 12V Connection Detail</i> .....	7-6
<i>BDU 10-32VDC Connection Detail</i> .....	7-6



<b>CHAPTER 8 ACRONYMS / GLOSSARY .....</b>	<b>8-1</b>
ACRONYMS / GLOSSARY .....	8-1
<b>CHAPTER 9 KIT CONTENTS AND ACCESSORIES.....</b>	<b>9-1</b>
VESSELINK™ KIT CONTENTS AND ACCESSORIES.....	9-1
INDEX .....	INDEX-1

## List of Figures

FIGURE 1-1 EARTH SHOWING IRIDIUM SATELLITES IN SIX DEFINED ORBITAL PLANES .....	1-2
FIGURE 1-2 TYPICAL IRIDIUM NETWORK FLOW OF A VOICE OR DATA CALL. ....	1-2
FIGURE 2-1 CALLING OVERVIEW FOR THREE VOICE LINES .....	2-1
FIGURE 2-2 LOCAL COMMUNICATIONS VIA PBX FUNCTIONALITY .....	2-2
FIGURE 2-3 THALES VESSELINK™ SYSTEM WITH ACCESSORIES.....	2-3
FIGURE 2-4 BELOW DECK UNIT (BDU) .....	2-4
FIGURE 2-5 BELOW DECK UNIT (BDU) LEDs.....	2-4
FIGURE 2-6 BELOW DECK UNIT (BDU) FRONT PANEL DETAIL .....	2-6
FIGURE 2-7 BELOW DECK UNIT (BDU) BACK PANEL DETAIL.....	2-6
FIGURE 2-8 ABOVE DECK UNIT (ADU) / ANTENNA FOR CERTUS 350 AND CERTUS 200 SYSTEMS.....	2-7
FIGURE 3-1 BDU FRONT PANEL DETAIL .....	3-1
FIGURE 3-2 VESSELINK™ IMEI AND IMSI FROM MOBILE DEVICE .....	3-3
FIGURE 3-3 SIM CARD WITH COVER OPENED .....	3-3
FIGURE 3-4 INSTALLING SIM CARD AND ENGAGING THE LOCK.....	3-4
FIGURE 3-5 SECURE THE SIM CARD COVER.....	3-4
FIGURE 3-6 SYSTEM, SATELLITE AND WI-FI STATUS LEDs.....	3-5
FIGURE 3-7 VESSELINK™ USER INTERFACE LOGIN.....	3-7
FIGURE 4-1 QUICK LINK ICONS.....	4-4
FIGURE 4-2 QUICK LINK – SYSTEM STATUS .....	4-5
FIGURE 4-3 QUICK LINK – SATELLITE STATUS .....	4-5
FIGURE 4-4 QUICK LINK – WI-FI STATUS .....	4-6
FIGURE 4-5 QUICK LINK – LAN 1 AND LAN 2 STATUS (LAN 3 SIMILAR) .....	4-6
FIGURE 4-6 QUICK LINK – WAN STATUS .....	4-7
FIGURE 4-7 THALES VESSELINK™ DASHBOARD - MAIN SCREEN .....	4-7
FIGURE 4-8 STATUS → CURRENT DEVICES SCREEN .....	4-9
FIGURE 4-9 STATUS → GPS SCREEN.....	4-10
FIGURE 4-10 STATUS → LAN SCREEN .....	4-10
FIGURE 4-11 STATUS → PHONES SCREEN.....	4-11
FIGURE 4-12 STATUS → SERVICES SCREEN .....	4-11
FIGURE 4-13 STATUS → SIM SCREEN .....	4-12
FIGURE 4-14 ALERTS SCREEN (EXAMPLE SHOWN WITH NO ACTIVE ALERTS).....	4-13
FIGURE 4-15 ALERTS SCREEN (EXAMPLE SHOWN WITH ACTIVE ALERTS).....	4-13
FIGURE 4-16 CALL LOG SCREEN.....	4-14
FIGURE 4-17 CLEAR CALL LOG .....	4-14
FIGURE 4-18 EMERGENCY (DISABLED VIEW).....	4-15
FIGURE 4-19 EMERGENCY (ENABLED VIEW).....	4-15
FIGURE 4-20 CONFIRMATION REQUIRED – SEND AN EMERGENCY MESSAGE.....	4-16
FIGURE 4-21 SETTINGS → GENERAL SCREEN.....	4-17

FIGURE 4-22 SETTINGS → EMERGENCY (INITIAL SCREEN).....	4-18
FIGURE 4-23 SETTINGS → EMERGENCY .....	4-19
FIGURE 4-24 SETTINGS → SATELLITE SCREEN .....	4-20
FIGURE 4-25 SETTINGS → WI-FI SCREEN.....	4-22
FIGURE 4-26 SETTINGS → LAN SCREEN.....	4-25
FIGURE 4-27 SETTINGS → WAN SCREEN.....	4-28
FIGURE 4-28 SETTINGS → PHONE SCREEN.....	4-31
FIGURE 4-29 VOIP PHONE SETTINGS .....	4-34
FIGURE 4-30 CISCO SPA504G IP ADDRESS .....	4-34
FIGURE 4-31 SPA504G CONFIGURATION UTILITY.....	4-35
FIGURE 4-32 GRAND STREAM GXP2140 CONFIGURATION PAGE .....	4-37
FIGURE 4-33 SETTINGS → SURELINK HANDSET AUTOMATIC APP CONFIGURATION.....	4-38
FIGURE 4-34 SETTINGS → SURELINK HANDSET MANUAL APP CONFIGURATION .....	4-39
FIGURE 4-35 SETTINGS → RADIO GATEWAY .....	4-41
FIGURE 4-36 SETTINGS → DATA SCREEN .....	4-45
FIGURE 4-37 SETTINGS → SECONDARY DATA FLOWS.....	4-47
FIGURE 4-38 SETTINGS → GLOBAL NAVIGATION SATELLITE SYSTEM.....	4-50
FIGURE 4-39 ENABLE GNSS REBOOT NOTIFICATION SCREEN.....	4-51
FIGURE 4-40 SYNCHRONIZE TIME CONFIRMATION SCREEN.....	4-51
FIGURE 4-41 SETTINGS → GPIO.....	4-53
FIGURE 4-42 SETTINGS → LOCATION SERVICES SCREEN.....	4-54
FIGURE 4-43 SYSTEM → BACKUP SCREEN .....	4-55
FIGURE 4-44 SYSTEM → DATA USAGE SCREEN.....	4-57
FIGURE 4-45 RESET DATA USAGE SCREEN.....	4-57
FIGURE 4-46 SYSTEM → RESET .....	4-58
FIGURE 4-47 SYSTEM → FIRMWARE SCREEN.....	4-59
FIGURE 4-48 FIRMWARE SCREEN – SHOW DETAILS.....	4-60
FIGURE 4-49 DIAGNOSTICS → SELF-TEST SCREEN .....	4-61
FIGURE 4-50 PERFORM SELF-TEST CONFIRMATION.....	4-61
FIGURE 4-51 PERFORM SELF-TEST COMPLETED SCREEN.....	4-62
FIGURE 4-52 DIAGNOSTICS → LOGS SCREEN.....	4-62
FIGURE 4-53 ABOUT SCREEN (EXAMPLE).....	4-63
FIGURE 4-54 HELP SCREEN (EXAMPLE).....	4-64
FIGURE 5-1 SYSTEM → FIRMWARE .....	5-1
FIGURE 5-2 FIRMWARE BEING STAGED .....	5-2
FIGURE 5-3 SYSTEM → FIRMWARE UPDATE CONFIRM .....	5-3
FIGURE 5-4 FIRMWARE UPDATE IN PROCESS.....	5-3
FIGURE 5-5 SYSTEM → FIRMWARE UPDATE COMPLETED .....	5-4
FIGURE 6-1 LOCATION OF POWER BUTTON ON BDU .....	6-5
FIGURE 6-2 MANAGEMENT PORTAL - SYSTEM → RESET.....	6-5
FIGURE 6-3 RESET BUTTON .....	6-6
FIGURE 7-1 RADIO GATEWAY FOR ADVANCED LAND MOBILE SERVICES .....	7-4
FIGURE 7-2 GPIO CONNECTOR PIN DETAIL .....	7-5
FIGURE 7-3 12V INPUT AND MATING CONNECTOR DETAIL .....	7-6
FIGURE 7-4 10-32 VDC AND MATING CONNECTOR DETAIL .....	7-6

## List of Tables

TABLE 2-1 BELOW DECK UNIT (BDU) LED STATUS .....	2-5
TABLE 2-2 COAXIAL CABLE LIST .....	2-7
TABLE 3-1 TYPICAL VOIP PHONE CONFIGURATION.....	3-2
TABLE 3-2 BELOW DECK UNIT (BDU) LED STATUS .....	3-5
TABLE 4-1 QUICK LINK ICONS.....	4-4
TABLE 4-2 THALES VESSELINK™ DASHBOARD - MAIN SCREEN.....	4-8
TABLE 4-3 SETTINGS → GENERAL SETTINGS .....	4-17
TABLE 4-4 SETTINGS → EMERGENCY .....	4-19
TABLE 4-5 SETTINGS→ SATELLITE .....	4-21
TABLE 4-6 SETTINGS→ WI-FI.....	4-23
TABLE 4-7 SETTINGS→ LAN.....	4-26
TABLE 4-8 SETTINGS→ WAN.....	4-29
TABLE 4-9 SETTINGS→ PHONE.....	4-32
TABLE 4-10 SETTINGS→ SURELINK HANDSET .....	4-39
TABLE 4-11 SETTINGS→ RADIO GATEWAY .....	4-42
TABLE 4-12 SETTINGS→ DATA .....	4-45
TABLE 4-13 SETTINGS→ SECONDARY DATA FLOWS .....	4-48
TABLE 4-14 SETTINGS→ GLOBAL NAVIGATION SATELLITE SYSTEM.....	4-50
TABLE 4-15 SETTINGS→ GPIO.....	4-53
TABLE 4-16 SETTINGS→ LOCATION SERVICES .....	4-55
TABLE 6-1 TROUBLESHOOTING .....	6-1
TABLE 6-2 ALERTS / ERROR MESSAGES .....	6-8
TABLE 7-1 TECHNICAL SPECIFICATIONS .....	7-1
TABLE 7-2 GPIO CONNECTOR PIN DEFINITION.....	7-5
TABLE 8-1 LIST OF ACRONYMS .....	8-1
TABLE 8-2 LIST OF DEFINITIONS.....	8-2
TABLE 9-1 STANDARD KIT, VESSELINK™ CERTUS 350, LIST OF EQUIPMENT.....	9-1
TABLE 9-2 BASE KIT, VESSELINK™ CERTUS 350, LIST OF EQUIPMENT .....	9-2
TABLE 9-3 BASE KIT, VESSELINK™ CERTUS 200, LIST OF EQUIPMENT .....	9-2
TABLE 9-4 AVAILABLE VESSELINK™ ACCESSORIES .....	9-3

## SAFETY

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



### **SHOCK HAZARD**

The VesseLINK™ 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 Below Deck Unit (BDU) and Above Deck Unit (ADU) 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**

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**

The BDU contains a small Li-ion hold-up 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.





## WARNING

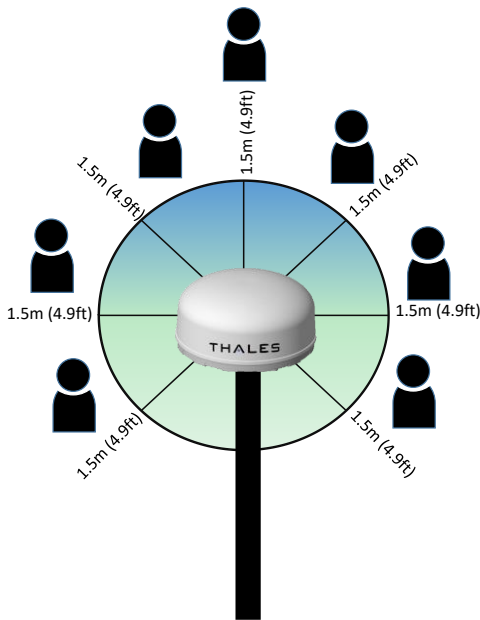
### ANTENNA RADIATION HAZARDS

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

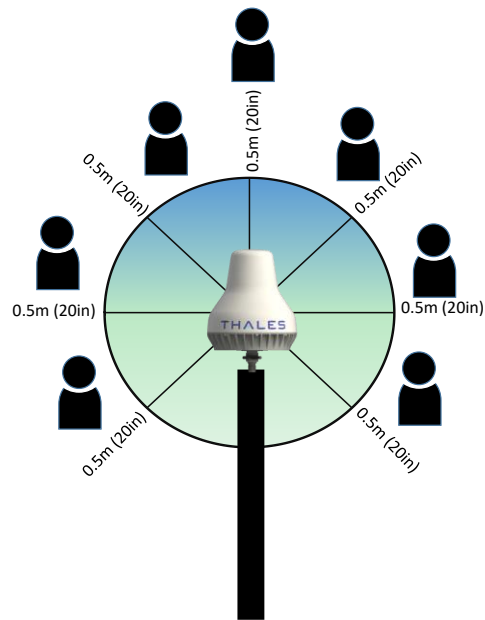
During operation, the antenna radiates high power at microwave frequencies that can be harmful to individuals. While the unit is operating, personnel should maintain a minimum safe distance from the antenna. The antenna should be mounted in an area that prevents the possibility of close exposure to the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

For the Certus 350 antenna, please remain at least 1.5m (4.9 feet) from the antenna while in operation.

For the Certus 200 antenna, please remain at least 0.5m (20 inches) from the antenna while in operation.



**Certus 350**



**Certus 200**



## NOTE

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

## FCC INFORMATION

**NOTE**

Certus 350  
FCC Identifier: OKCVF350BM  
Contains FCC ID: OKCWROOM32U

**NOTE**

Certus 200  
FCC Identifier: OKCVF200BM  
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 into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Industry Canada Information



**NOTE**

Certus 350  
Industry Canada: 473C-VF350BM  
Contains IC: 473C-WROOM32U



**NOTE**

Certus 200  
Industry Canada: 473C-VF200BM  
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-VF350BM or 473C-VF200BM) 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-VF350BM ou 473C-VF200BM) 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.*

## Supplier's declaration of conformity



As required by the following Notices:

- Radiocommunications (Compliance Labelling - Devices) Notice 2014 made under section 182 of the Radiocommunications Act 1992;
- Radiocommunications Labelling (Electromagnetic Compatibility) Notice 2017 made under section 182 of the Radiocommunications Act 1992;
- Radiocommunications (Compliance Labelling - Electromagnetic Radiation) Notice 2014 made under section 182 of the Radiocommunications Act 1992; and
- Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015 made under section 407 of the Telecommunications Act 1997.

### Instructions for completion

Do not return this form to the ACMA. This completed form must be retained by the supplier as part of the documentation required for the compliance records and must be made available for inspection by the ACMA when requested.

### Supplier's details

Company Name (OR INDIVIDUAL)

Braco Compliance Pty Ltd

ERAC Responsible Supplier number

E304

Street Address (Australian)

Unit 308, 469-481 High St

Northcote, VIC 3070

OR

ACN/ARBN

84156023504

### Product details

Product description – brand name, type, current model, lot, batch or serial number (if available), software/firmware version (if applicable)

**THALES**  
Maritime Satellite Communications,  
VesseLINK™, Model VF350BM Terminal with Maritime Antenna.

### Compliance – applicable standards and other supporting documents

Evidence of compliance with applicable standards may be demonstrated by test reports, endorsed/accredited test reports, certification/competent body statements. Having had regard to these documents, I am satisfied the above mentioned product complies with the requirements of the relevant ACMA Standards made under the Radiocommunications Act 1992 and the Telecommunications Act 1997.

List the details of the documents the above statement was made, including the standard title, number and, if applicable, number of the test report/endorsed test report or certification/competent body statement.

Radiocommunications (Electromagnetic Compatibility) Standard 2017, refer MET Laboratories Inc. test report Nos. EMC94508B-ETS489 Rev. 1 dated 15 June 2018 and EMC102479-EN dated 22 April 2019.

Radiocommunications (Short Range Devices) Standard 2014, refer SGS Fimko CFR 47 FCC Pt 15.247 test report No. 268892-2 dated 28 June 2012.

ETSI EN 301 441 v2.1.1, refer MET Laboratories Inc. test report No. EMC94508B-ETS441 Rev. 1 dated 16 March 2018.

Radiocommunications (Electromagnetic Radiation - Human Exposure) Standard 2014, refer MET Laboratories Inc. test report No. EMC94508B-EN62311 dated 25 May 2018.

### Declaration

I hereby declare that:

1. I am authorised to make this declaration on behalf of the Company mentioned above,
2. the contents of this form are true and correct, and
3. the product mentioned above complies with the applicable above mentioned standards and all products supplied under this declaration will be identical to the product identified above.

Note: Under section 137.1 of the Criminal Code Act 1995, it is an offence to knowingly provide false or misleading information to a Commonwealth entity.

Penalty: 12 months imprisonment

Bruce Maule

Director

5 August 2019

The Privacy Act 1988 (Cth) (the Privacy Act) imposes obligations on the ACMA in relation to the collection, security, quality, access, use and disclosure of personal information. These obligations are detailed in the Australian Privacy Principles.  
The ACMA may only collect personal information if it is reasonably necessary for, or directly related to, one or more of the ACMA's functions or activities.  
The purpose of collecting the personal information in this form is to ensure the supplier is identified in the 'Declaration of conformity'. If this Declaration of Conformity is not completed and the requested information is not provided, a compliance label cannot be applied.  
Further information on the Privacy Act and the ACMA's Privacy Policy is available at [www.acma.gov.au/privacy-policy](http://www.acma.gov.au/privacy-policy). The Privacy Policy contains details about how you may access personal information about you that is held by the ACMA, and seek the correction of such information. It also explains how you may complain about a breach of the Privacy Act and how we will deal with such a complaint.  
Should you have any questions in this regard, please contact the ACMA's privacy contact officer on telephone on 1800 226 987 or by email at [privacy@acma.gov.au](mailto:privacy@acma.gov.au).



## RADIO SPECTRUM MANAGEMENT



MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT  
HIKINA WHAKATUTUKI

### Braco Compliance Limited

### Supplier's declaration of conformity

As required by notices under:

- Section 134 (1) (g) of the New Zealand Radiocommunications Act 1989.

#### Supplier's details

Name (name of manufacturer, importer or agent)

Braco Compliance Limited

ERAC Responsible Supplier registration number

E178

Address (address of agent)

9 Braco Place, Ilam  
Christchurch 8041

Contact information

Telephone: +64 21 208 4303  
Email: admin@bracocompliance.com

#### Product details

Product description – brand name, type, model, lot, batch or serial number (if available)

# THALES

Maritime Satellite Communications,  
VesselINK™, Model VF350BM Terminal with Maritime Antenna.

#### Applicable standards

Standard title, number and, if applicable, number of the test report

ETSI EN 301 489-1 v2.1.1 with ETSI EN 301 489-17 v3.1.1, refer MET Laboratories Inc. test report No. EMC94508B-ETS489 Rev. 1 dated 15 June 2018.

EN 60945:2002, refer MET Laboratories Inc. test report No. EMC102479-EN dated 22 April 2019.

ETSI EN 301 441 v2.1.1, refer MET Laboratories Inc. test report No. EMC94508B-ETS441 Rev. 1 dated 16 March 2018.

CFR 47 FCC Pt 15.247, refer SGS Fimko test report No. 266892-2 dated 28 June 2012.

#### Declaration

I hereby declare that the product mentioned above complies with the above mentioned standards, and all products supplied under this declaration will be identical to the sample identified above.

SIGNATURE OF SUPPLIER OR AGENT:

PRINT NAME: Bruce Maule

POSITION IN ORGANISATION: Director

DATE: 5 August 2019

## 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 this declaration

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.

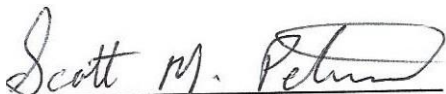
#### Manufacturer

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

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	VesseLINK VF200BM
License Holder	Thales Defense & Security, Inc.
Manufacturer	Thales Defense & Security, Inc.
Certificate number	005-102887
Certification date	2021-10-29

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





(Translation)

## Type Approval Certificate

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) 0.55W 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) 0.51W 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) 2.26W 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) 5W
Model Name	VesseLINK VF350BM
License Holder	Thales Defense & Security, Inc.
Manufacturer	Thales Defense & Security, Inc.
Certificate number	005-102914
Certification date	2021-12-22


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

JRF-005-102914-001

2021-12-22

TÜV Rheinland Japan Ltd.





Federative Republic of Brazil  
Telecommunications National Agency

## Certificate of Equipment Authorization

(Not Transferable)

Nº **18495-21-12044**

Expires: Indeterminada  
Date of Certificate: 06/05/2022

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

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 22.0314, 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 Anatel's Rules and Regulations.

Type - Category: **Transceptor do SMM por Satélite - III**

Model - Commercial Name (s): **VF350BM (VesselLink) / VF200BM (VesselLink)**

Basic technical characteristics:

Designação de Emissões	Potência Máxima de Saída (W)	Faixa de Frequências Tx (MHz)
590KG1D	314,992	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](http://www.anatel.gov.br)).

Davison Gonzaga da Silva  
Gerente de Certificação e Numeração

UNIDAD DE CONCESIONES Y SERVICIOS  
DIRECCIÓN GENERAL DE AUTORIZACIONES  
Y SERVICIOS



INSTITUTO FEDERAL DE  
TELECOMUNICACIONES

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

## CERTIFICADO DE HOMOLOGACIÓN

Clase: PROVISIONAL

Número: RCSTHVF20-0843

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: <b>4 de mayo de 2020</b>	Oficio respuesta a solicitud: <b>IFT/223/UCS/DG-AUSE/ 2247 / 2020</b>
Equipo: <b>Terminal satelital (Thales VesseLINK)</b>	
Marca: <b>THALES</b>	Modelo: <b>VF350BM</b>
Perito(s) en Telecomunicaciones: <b>Ing. José Luis Pérez Baez (IFT-P-0065-2017)</b>	
<b>CARACTERÍSTICAS TÉCNICAS</b>	
Bandas de frecuencias	1616 – 1626.5 MHz (Banda "L")
Potencia isotrópica radiada efectiva (PIRE)	9 dBW (voz), 18.2 dBW (datos)
Tipo de modulación	DQPSK, QPSK, 16 APSK
<b>Antena:</b>	
Tipo	IP67 matriz escalonada
Diámetro	36.8 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. 05720  
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

Verificable: [www.ift.org.mx/industria/concesiones-y-servicios/homologacion/lista-de-equipos](http://www.ift.org.mx/industria/concesiones-y-servicios/homologacion/lista-de-equipos)

## CHAPTER 1 INTRODUCTION

### INTRODUCTION

Thank you for your recent purchase of the Thales VesseLINK™ 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 of the Thales VesseLINK™ systems including the Certus 350 VesseLINK™ and the Certus 200 VesseLINK™.

Additional information can be found in the following documents:

- The Thales VesseLINK™ installation process is covered in the Installation Guide for VesseLINK (Document # 84464)
- The Thales VesseLINK™ Quick Start Guide (QSG) (Document # 3402131-1)



#### NOTE

Some figures throughout 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 Thales VesseLINK™ 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 airtime provider or Thales at [www.Thalesdsi.com](http://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.

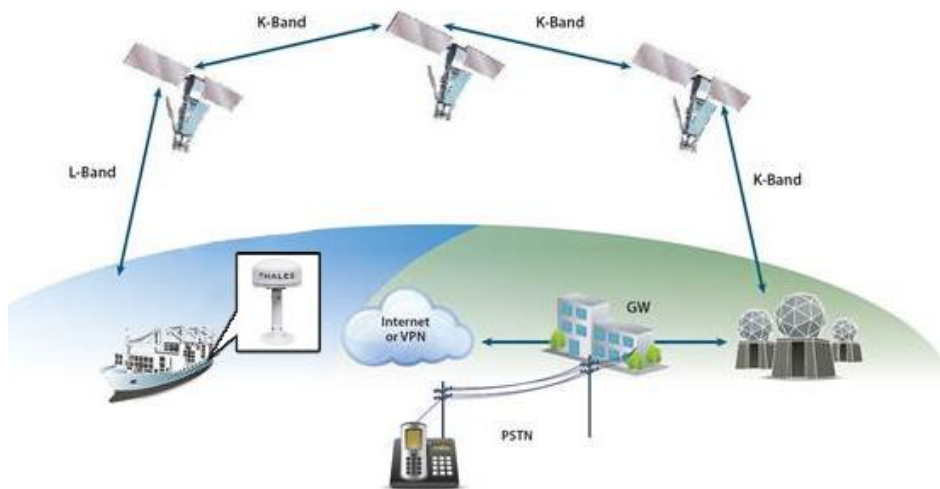
The Iridium NEXT satellite constellation replaced the legacy Iridium satellite constellation with faster data rates, more capacity and better voice quality.



*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 VesseLINK™ system.

A VesseLINK™ 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

### DESCRIPTION

The Thales VesseLINK™ 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

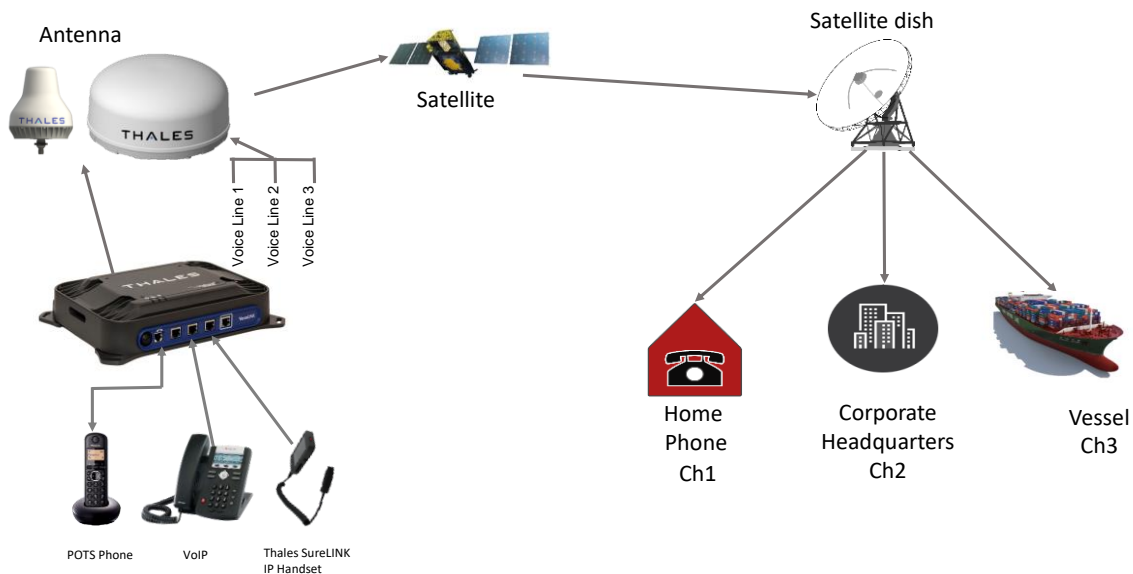


Figure 2-1 Calling Overview for Three Voice Lines

## 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.
- Private Branch Exchange (PBX) functionality provides extensions for 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.).
- 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 Below Deck Unit (BDU).
- 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

## Private Branch Exchange (PBX)

Local call extensions for on vessel calling

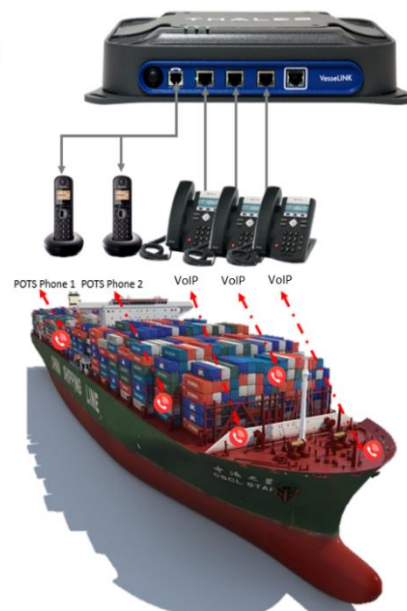


Figure 2-2 Local Communications via PBX Functionality

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 system and not the WAN port.



*Figure 2-3 Thales VesseLINK™ System with Accessories*

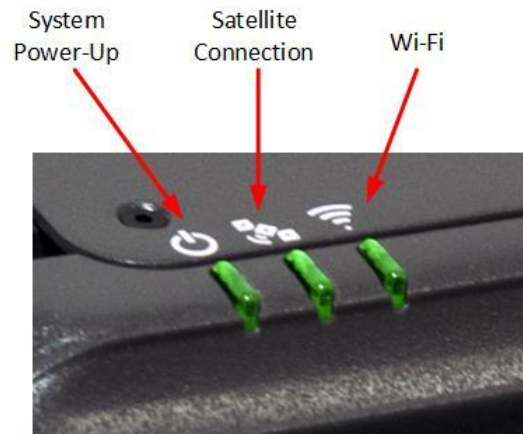
## Below Deck Unit (BDU)

The Below Deck Unit (BDU) supports voice and data communications in a marine environment. The BDU is capable of supporting wireless voice and data that links the user with the Iridium satellite network. As a wireless access point, the BDU 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 BDU, if desired. The Management Portal is a graphical user interface that can be used to modify system settings and indicate system status. The BDU is powered by either an AC/DC power supply or a DC power cable with a 10-32V input range and remote start wire accommodating all types of marine vessels, applications and power sources.






*Figure 2-4 Below Deck Unit (BDU)*

The BDU 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 Below Deck Unit (BDU) LEDs*

Table 2-1 Below Deck Unit (BDU) LED Status

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



**NOTE**

The Indicator Colors are:

Solid Green: Operational

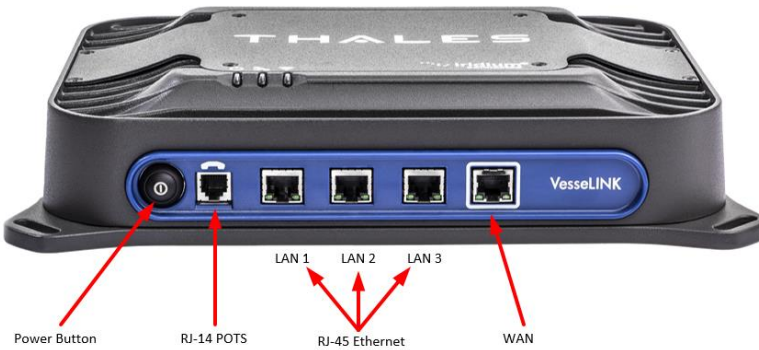
Flashing Green: start-up or in progress of configuring or acquiring service

Solid Red: fault requires user attention (Open Management Portal for Alerts)

Flashing Red: critical fault requiring immediate attention. For additional information, refer to Chapter 6 Troubleshooting



The BDU 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 Below Deck Unit (BDU) Front Panel Detail*

The BDU 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 Below Deck Unit (BDU) Back Panel Detail*

## Antenna Unit

The Above Deck Unit (ADU) or Antenna is a standalone unit that connects to the BDU through a single coaxial cable. DC power, RF transmit and receive signals, control data and GPS data are communicated between the ADU and BDU using this single coaxial cable.



Figure 2-8 Above Deck Unit (ADU) / Antenna 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 VesseLINK system. These include:

- **RF Cable loss** - The VesseLINK 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 VesseLINK 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 VesseLINK 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
25 meters LMR-300 FR	855023-082
50 meters LMR-400 FR	855033-164



### NOTE

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

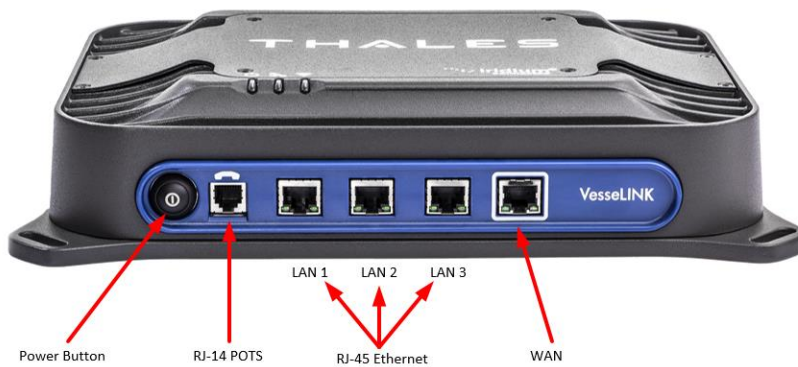
**THIS PAGE INTENTIONALLY LEFT BLANK**

## CHAPTER 3 GETTING STARTED

### GETTING STARTED

#### STEP 1: Connect Phone (standard POTS handset) or Ethernet VoIP Phone to BDU.

The BDU 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 BDU 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 BDU 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 BDU POTS connector.

#### VoIP or Thales SureLINK IP Phone connection

By default the BDU has three (3) extensions preconfigured for use with POTS phones, VoIP phones, or the 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 VesseLINK™. Other brands and models may be supported but functionality cannot be guaranteed.

Follow your VoIP phone configuration guide to setup the VoIP phone and connect to the BDU 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 21, so it will automatically work the same as the first POTS line.

## STEP 2: Know your VesseLINK™

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

IMEI is unique to each unit and can be found on the back plate of the BDU. 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 BDU and the computer viewing the Thales Management Portal.



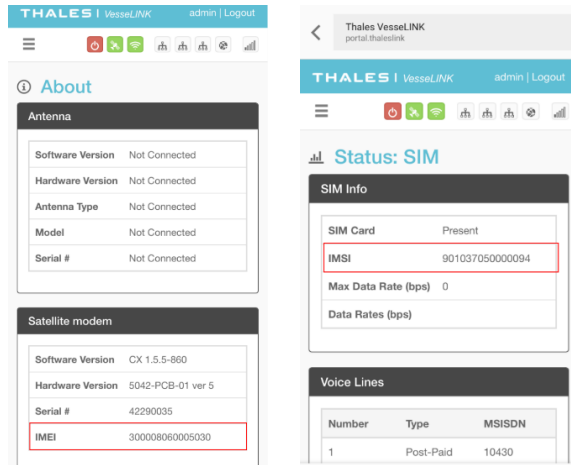


Figure 3-2 VesseLINK™ IMEI and IMSI from Mobile Device

### STEP 3: Install SIM

1. Open the SIM Card protective cover by pulling it away from the BDU 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 VesseLINK™ 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 BDU. If using the AC/DC power supply, connect one end to the BDU's 12V DC input and connect the power cord to a 120V or 240V AC outlet. The antenna must also be connected per the system installation manual. Power the unit by pressing and releasing the power button on the BDU (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.

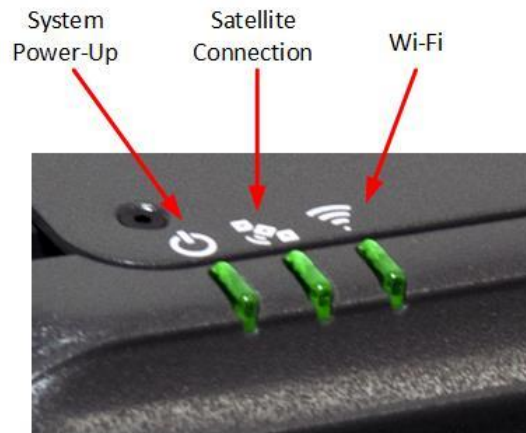





Figure 3-6 System, Satellite and Wi-Fi Status LEDs

Table 3-2 Below Deck Unit (BDU) LED Status

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

## STEP 5: Connect to VesseLINK™ portal to configure system.



### NOTE

Thales uses a self-signed certificate for encryption between the terminal and the browser when viewing the Management Portal (<https://portal.theseslink>). 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.

Reference Figure 3-7. There are a couple options to login to the Management Portal.

### Option A: Via Wi-Fi.

1. Power on the VesseLINK™ BDU 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.theseslink> (or <https://portal.theseslink>) (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.

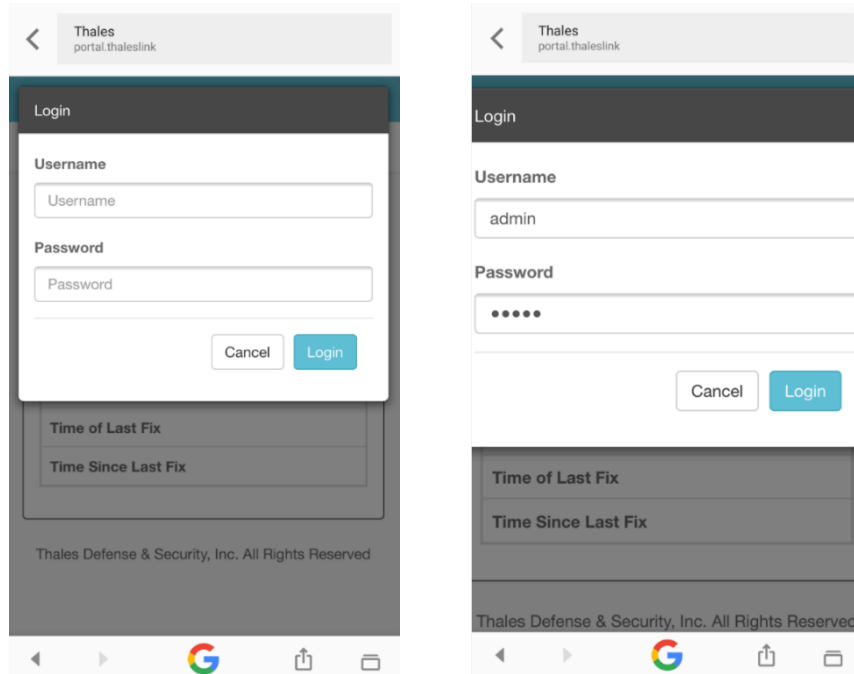
### Option B: Via (PC, Mac or Linux) Ethernet connection

1. Power on the VesseLINK™ BDU and let it boot up (may take a few minutes)
2. Via the network settings on your computer’s operating system, enable the VesseLINK™ connection.
3. Open a web browser and type: <http://portal.theseslink> (or <https://portal.theseslink>) (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 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 VesseLINK™ User Interface Login*



## STEP 6: Place a phone call.



### NOTE

The VesseLINK™ 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 BDU, open the Management Portal <http://portal.theslink> (or <https://portal.theslink>) 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 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](http://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 VesseLINK™ BDU 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 VesseLINK™ BDU 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 VesseLINK™ 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 BDU 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 VesseLINK™ system. There are four access levels to the system. Three 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 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 three other access levels are password protected. Passwords can be controlled and changed by the administrator in the SETTINGS → GENERAL menu, where the local administrator is denoted as “admin”, the remote user is denoted by “wan\_user” and the remote administrator is denoted by “wan\_admin”. By password control, the local system administrator can enable or prevent any remote access to the system.

Administrators, after initially logging in to the admin account with default password (admin), can view all data and also make changes to all the configuration settings to customize the VesseLINK™ 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.

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

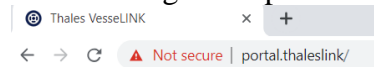
When you first enter into the Thales Management Portal, menu items appear on the left side of the screen (see Figure 4-1). Each of these menu items is discussed in the following sections. A short description of each menu item is below.

- 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.
- 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 VesseLINK™ 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 that is useful to the user. When selecting these icons by clicking or pressing on them, they provide addition screen(s) of information and a quick way to make certain configuration setting changes by the administrator.

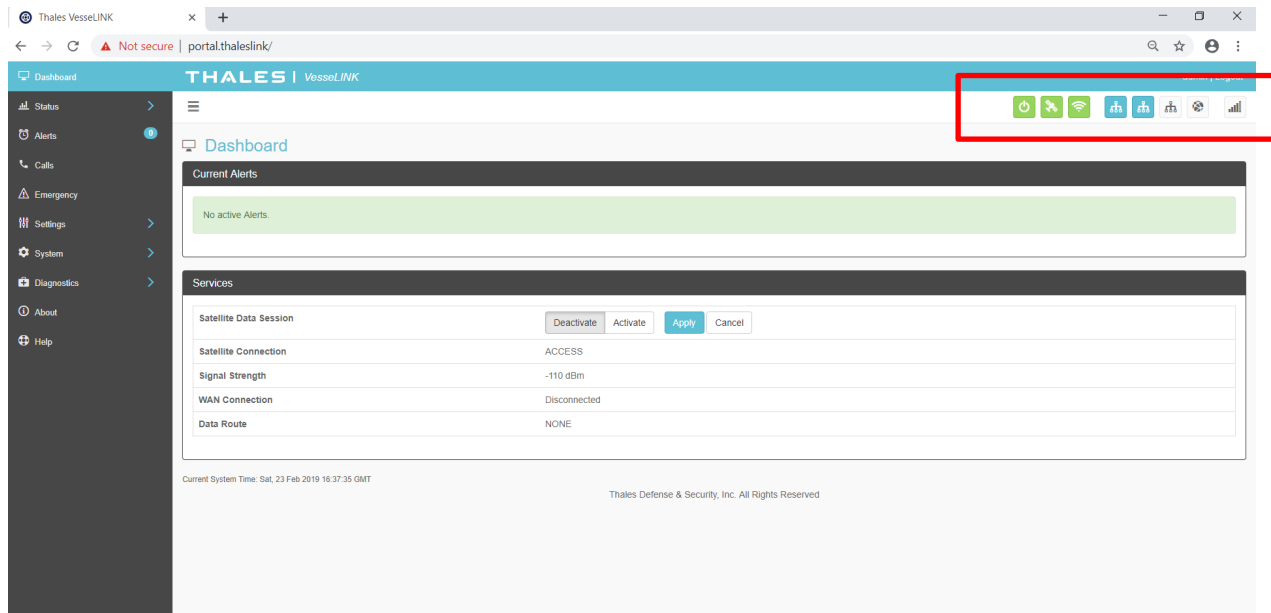








Figure 4-1 Quick Link Icons



## NOTE

Status icons on the GUI may lag those on the BDU, 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
	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 BDU. Selecting the System Status icon brings up the additional information in Figure 4-2.
  - **STATUS** shows the current condition of the system.
  - **UPTIME** indicates how long the terminal has been in use.
  - The **RESTART** button allows an administrator to reboot the terminal.
  - Selecting **VIEW ALERTS** opens the **ALERTS** window and displays any Current Alerts.



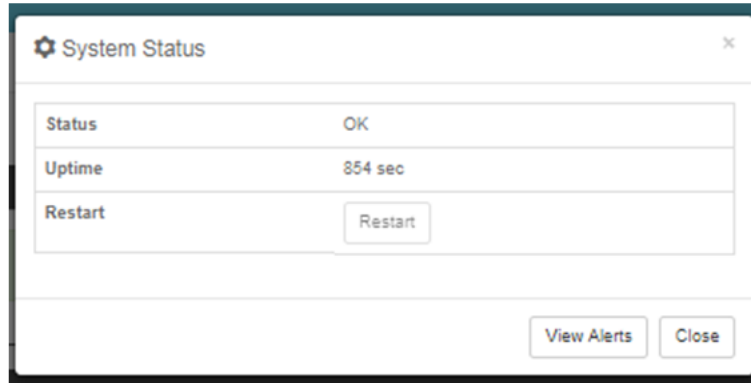


Figure 4-2 Quick Link – System Status



## 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 re-entering 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 BDU. 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.

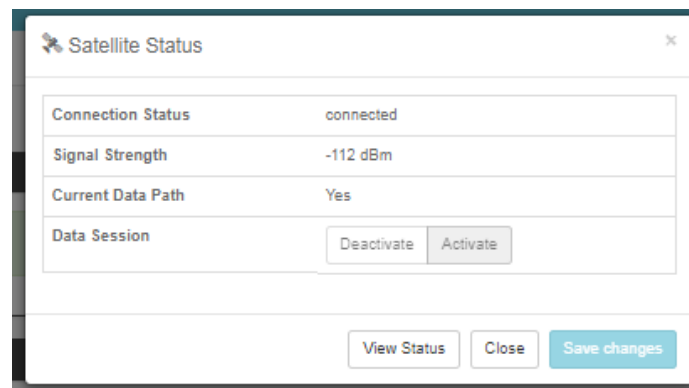


Figure 4-3 Quick Link – Satellite Status

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



## NOTE

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

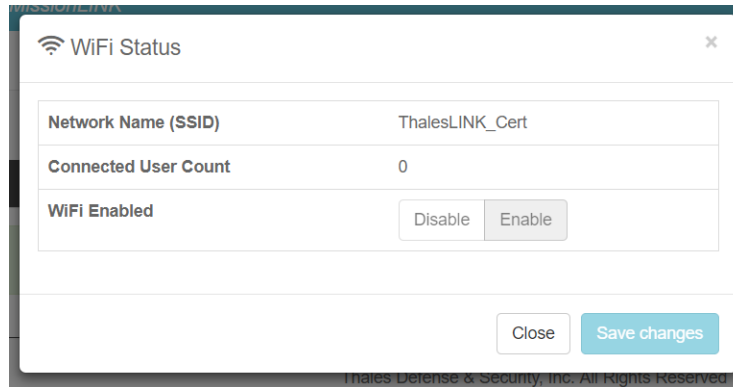


Figure 4-4 Quick Link – Wi-Fi Status

- 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 **Error! Reference source not found.** 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.

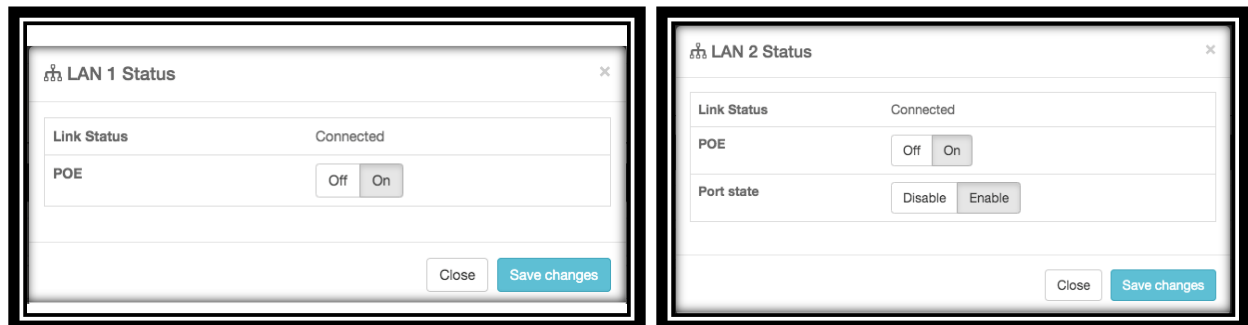


Figure 4-5 Quick Link – LAN 1 and Lan 2 Status (LAN 3 similar)

- 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"

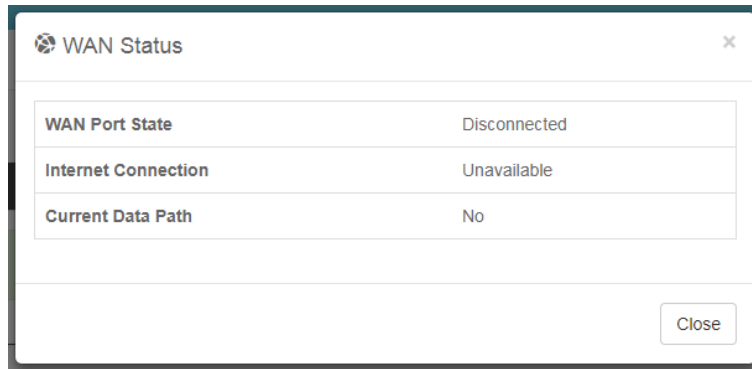


Figure 4-6 Quick Link – WAN Status

- 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>), the Dashboard screen comes up by default. The Dashboard also appears 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

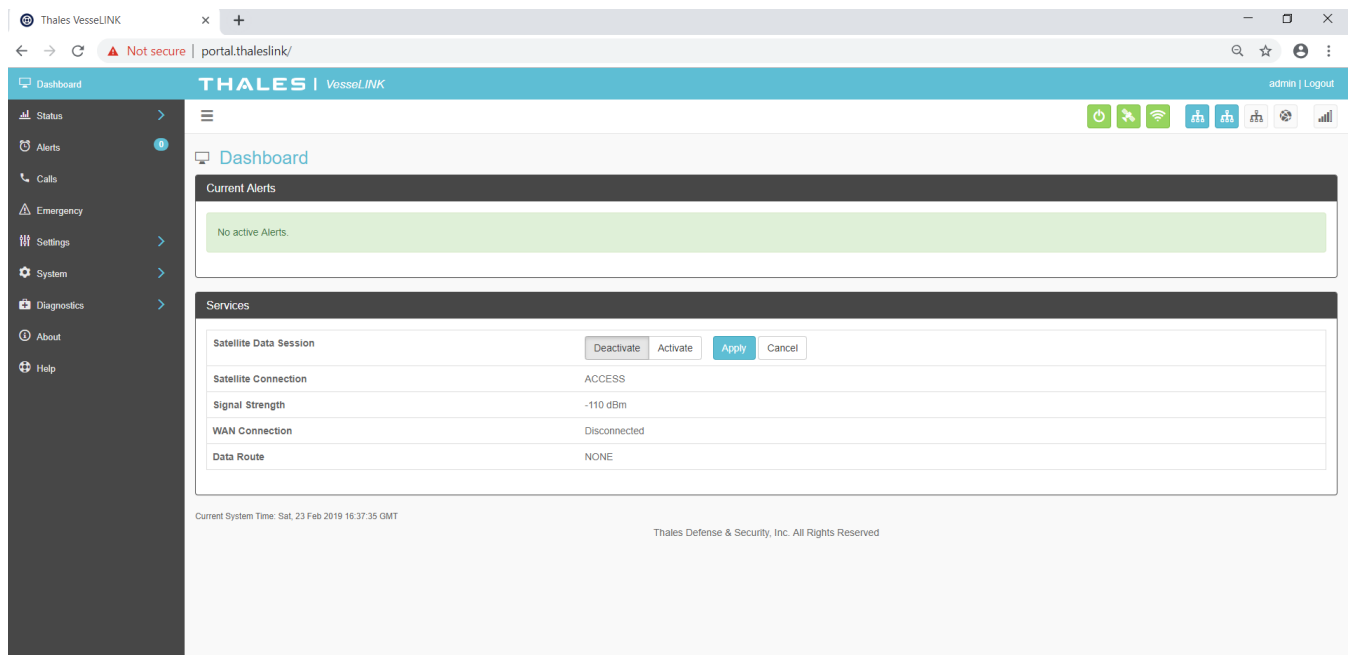


Figure 4-7 Thales VesseLINK™ Dashboard - Main Screen

Table 4-2 Thales VesseLINK™ Dashboard - Main Screen

Section	Value	Description
<b>Current Alerts (When shown on dashboard)</b>		
Alert Name	Text	Provides information relating all system issues summarized for easy reporting and debug/troubleshooting. For additional information, refer to Chapter 6 Troubleshooting
<b>Services</b>		
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 BDU and is connected to the internet
Data Route	Satellite or WAN	Displays the data route

## Status



### NOTE

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

### Current Devices:

Displays all devices currently connected to the Below Deck Unit (BDU), 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 BDU.

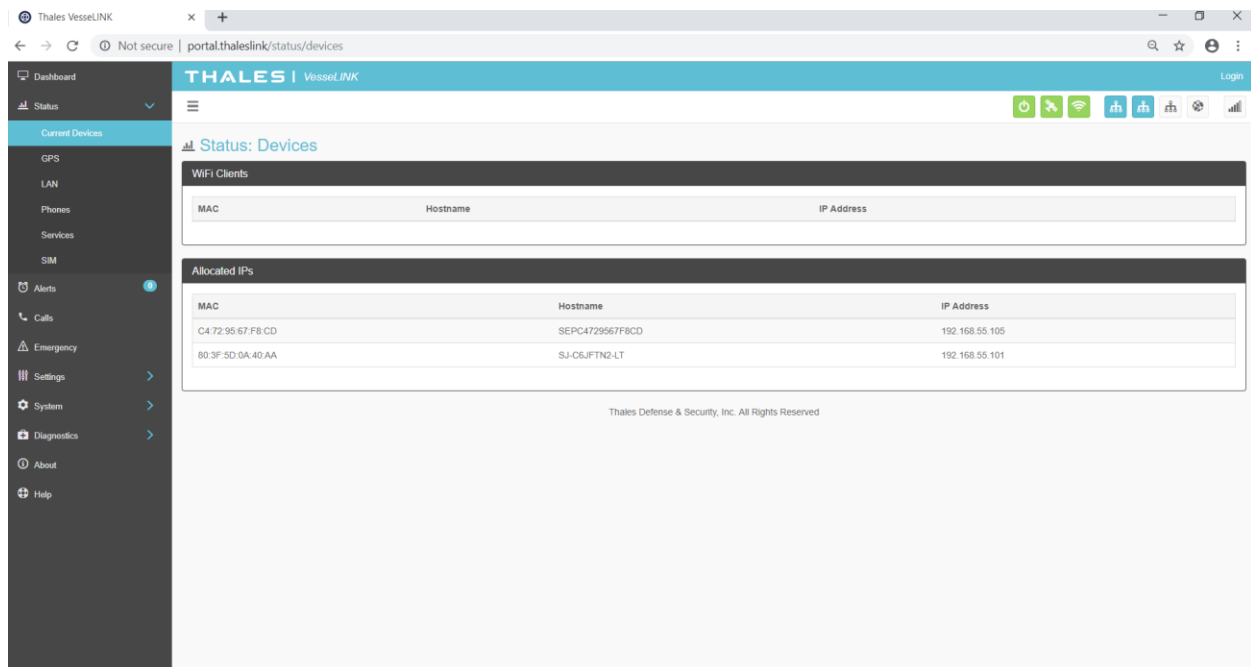


Figure 4-8 Status → Current Devices Screen

## GPS

From the GPS page, the operator will have access to detailed GPS information as shown in Figure 4-9.

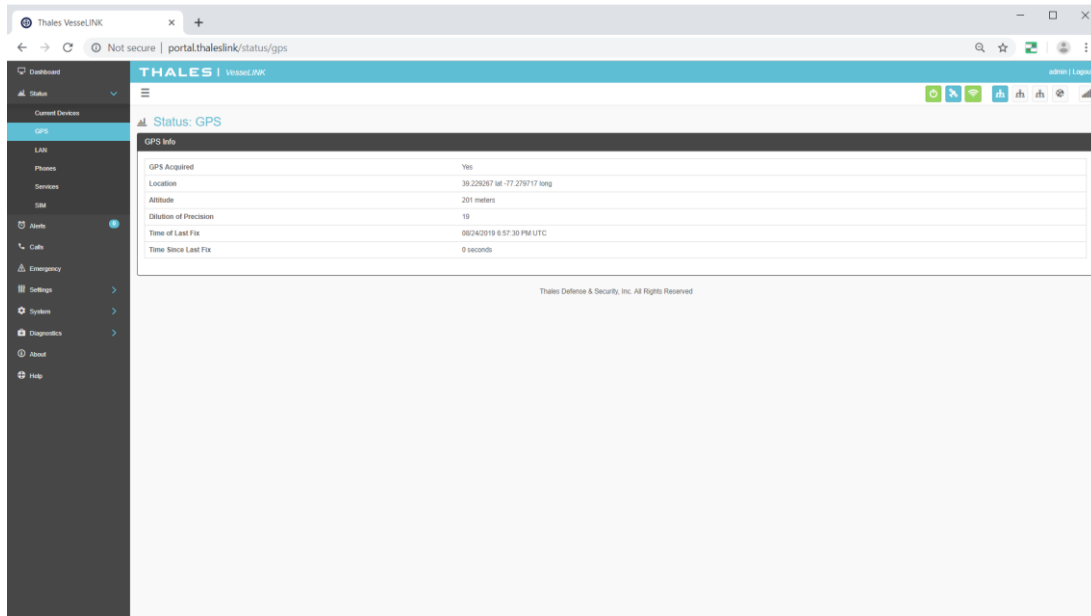


Figure 4-9 Status → GPS Screen

## 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.

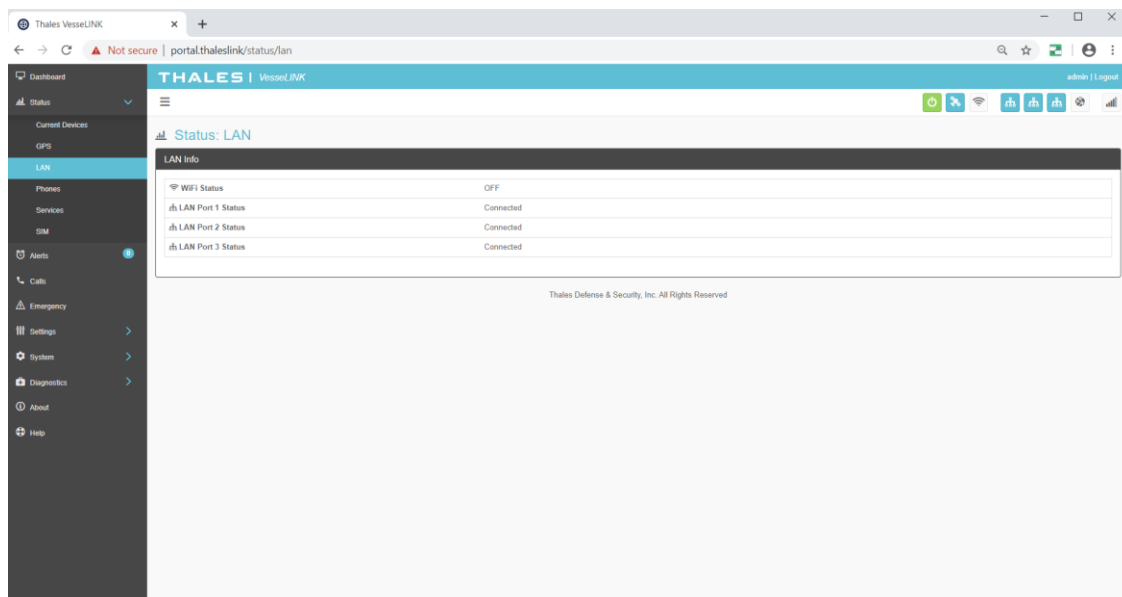


Figure 4-10 Status → LAN Screen





## 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.

The screenshot shows the THALES VesseLINK interface. The left sidebar contains navigation options: Dashboard, Status, Current Devices, GPS, LAN, Phones, Services, SIM (selected), Alerts, Calls, Emergency, Settings, System, Diagnostics, About, and Help. The main content area is titled 'Status: SIM' and contains three sections:

- SIM Info**: A table with the following data:
 

Field	Value
SIM Card	Present
IMSI	901037710001588
Private IP Address	172.30.1.23
- Voice Lines**: A table with the following data:
 

Number	Type	MSISDN
1	Post-Paid	881677100232
- Secondary Data Flows**: A table with the following data:
 

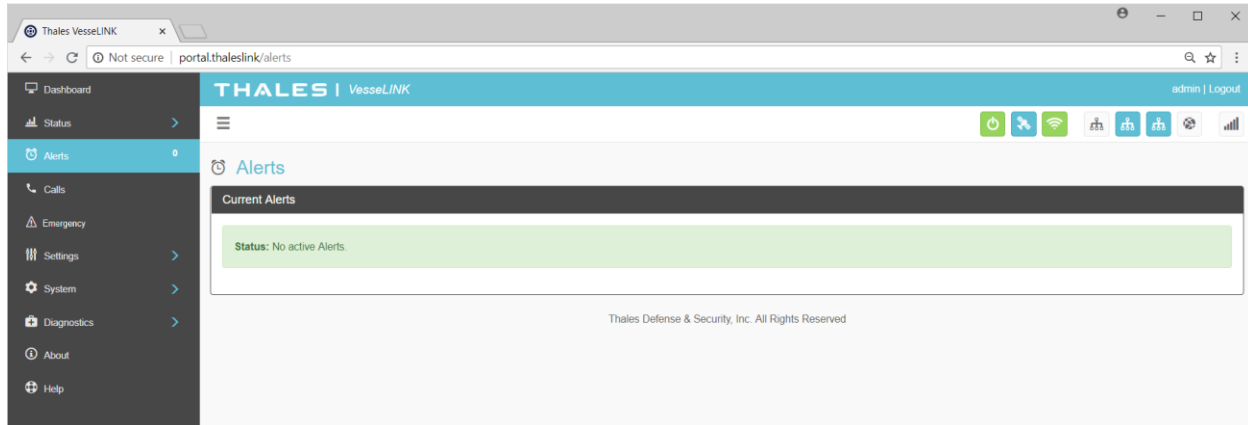
SDF Number	Provisioning	GW Subnet
1	unprovisioned	N/A
2	unprovisioned	N/A
3	unprovisioned	N/A
4	unprovisioned	N/A

At the bottom of the screen, it says 'Thales Defense & Security, Inc. All Rights Reserved'.

*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)



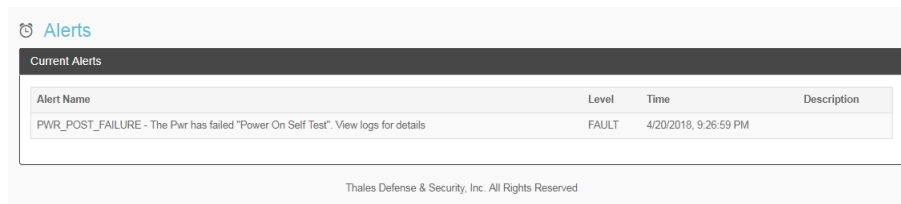
*Figure 4-14 ALERTS Screen (Example Shown with No Active Alerts)*



For additional information, refer to Chapter 6 Troubleshooting

### NOTE

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)*

## Calls

Selecting the Calls menu item (Figure 4-16) provides the call logs for active and past calls.

The screenshot shows the THALES VesselLINK portal interface. The left sidebar contains a navigation menu with items: Dashboard, Status, Alerts, Calls (selected), Emergency, Settings, System, Diagnostics, About, and Help. The main content area is titled 'Calls' and includes a 'Call Log Management' section with a 'Clear Log' button. Below this is a section for 'Active Calls' with a table header: Source, Destination, Start Time, Details, and Type. The 'Call History' section displays a table of call logs.

Source	Destination	Start Time	Duration (sec)	Details	Type
12403084666	1003	08/16/2019 2:28:17 PM UTC	30		Inbound
12403084666	1003	08/16/2019 2:28:43 PM UTC	73		Inbound
12403084666	1003	08/16/2019 2:23:58 PM UTC	9		Inbound
12403084666	1003	08/16/2019 2:22:36 PM UTC	26		Inbound
12403084666	1003	08/16/2019 2:21:45 PM UTC	35		Inbound
12403084666	1003	08/15/2019 1:36:14 PM UTC	31		Inbound
12403084666	1003	08/15/2019 1:35:30 PM UTC	27		Inbound
12403084666	1003	08/15/2019 1:33:58 PM UTC	72		Inbound
1001	1003	07/29/2019 3:12:24 PM UTC	68		Local
1003	1001	07/29/2019 3:11:00 PM UTC	13		Local
1001	1003	07/29/2019 3:07:24 PM UTC	192		Local
12408647885	1002	07/25/2019 9:02:46 PM UTC	28		Inbound
1002	12408942226	07/25/2019 9:00:36 PM UTC	18	Request Terminated	Outbound
1002	12408942226	07/25/2019 9:00:12 PM UTC	0	Not Found	Local
1002	14807525105	07/24/2019 5:20:52 PM UTC	15		Outbound
1002	1001	07/24/2019 5:20:13 PM UTC	1		Local
1002	14807525105	07/24/2019 5:19:31 PM UTC	14		Outbound
1001	1002	07/24/2019 5:18:27 PM UTC	7		Local
1002	1001	07/24/2019 5:15:25 PM UTC	23		Local

Figure 4-16 Call Log Screen

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

The screenshot shows the 'Call Log Management' section of the interface. It features a 'Clear Log' button. Below the button is a confirmation dialog with the text 'Confirmation Required' and 'Do you wish to clear the call log?'. The dialog has two buttons: 'Yes, Clear Log' (highlighted in red) and 'No, Cancel'.

Figure 4-17 CLEAR Call Log



CALL HISTORY displays the last 100 calls that were made.

## 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 4-22). 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.

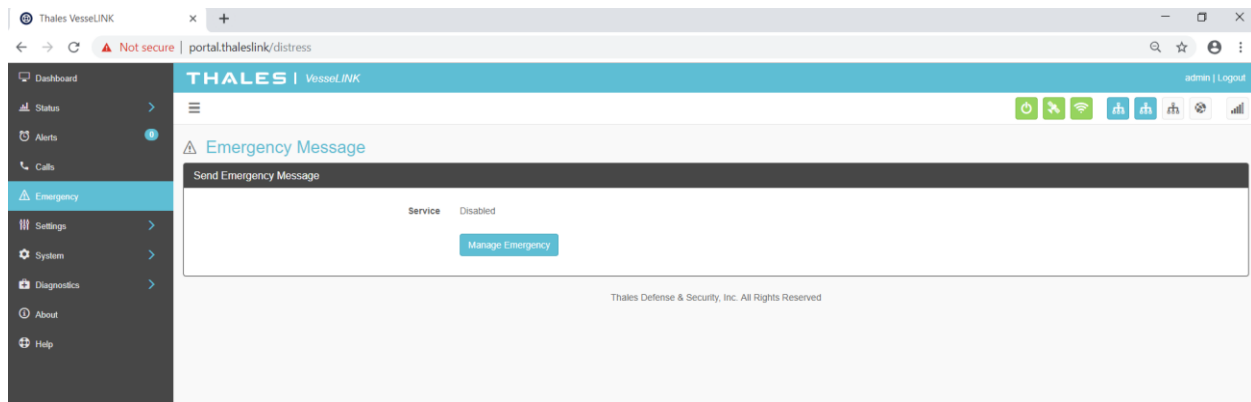


Figure 4-18 EMERGENCY (Disabled View)

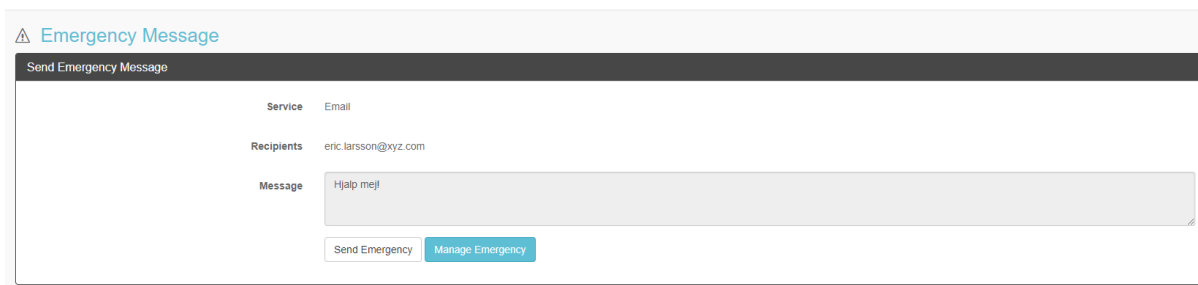


Figure 4-19 EMERGENCY (Enabled View)

## Sending an EMERGENCYMESSAGE:

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.



*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 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.

## Settings

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

### General

From the General page, change passwords and enable (or disable) external API access, as shown in Figure 4-21 and Table 4-3.

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

- GUEST: User only account, no password, read only access.
- 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.





The following default passwords for ADMIN, WAN\_ADMIN, and WAN\_USER are as follows:

## NOTE

### 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.

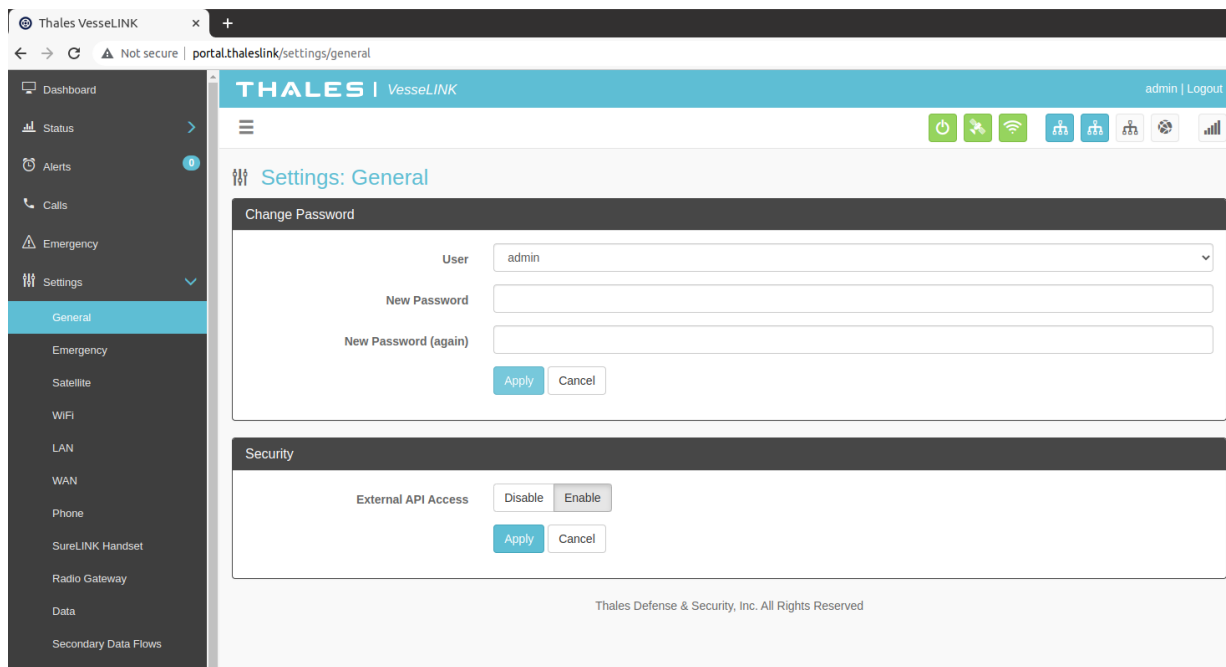



Figure 4-21 Settings → General Screen

Table 4-3 Settings → General Settings

Section	Parameters
Change Password	<ul style="list-style-type: none"> <li>Select User, Currently there are 3 choices (Admin, WAN_Admin, and WAN_User)</li> <li>Enter NEW Password and confirm the new password (Note: Minimum of 8 characters with a lowercase letter, an uppercase letter, a number, and a special character)</li> </ul>
Security	<ul style="list-style-type: none"> <li><b>Enable</b> / Disable the external API Access. (<b>Enable</b> is the default setting)</li> </ul>

## 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.

On the Emergency page, the admin can set up an emergency message. The Management Portal configuration is restricted to a distress email only. Select EMAIL from the pull down list (Figure 4-22). Enter the required information shown in Table 4-4 (example data shown in Figure 4-23) along with the message to be sent and select APPLY. NOTE: Selecting APPLY does not send a distress message. It saves the settings and message. Sending the emergency message is done through the EMERGENCY menu item.

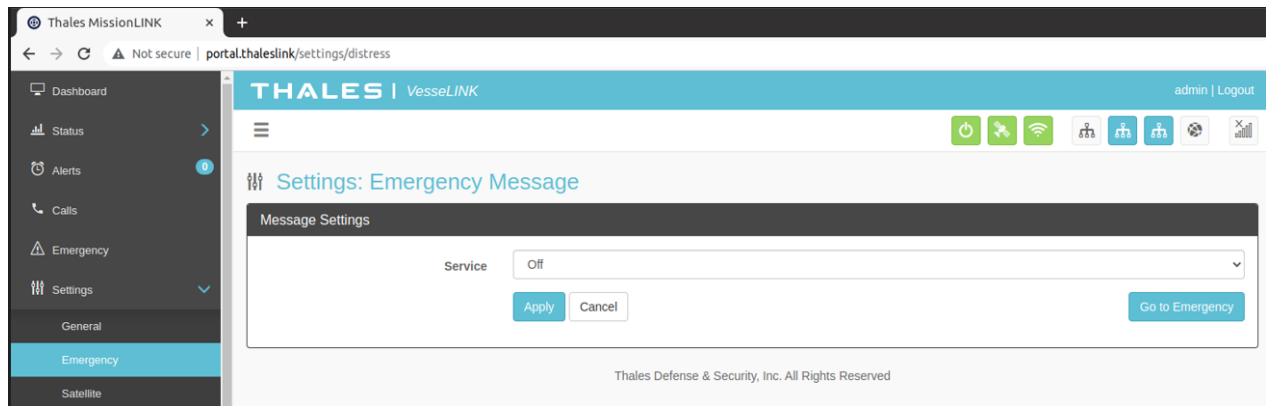


Figure 4-22 Settings → Emergency (Initial Screen)

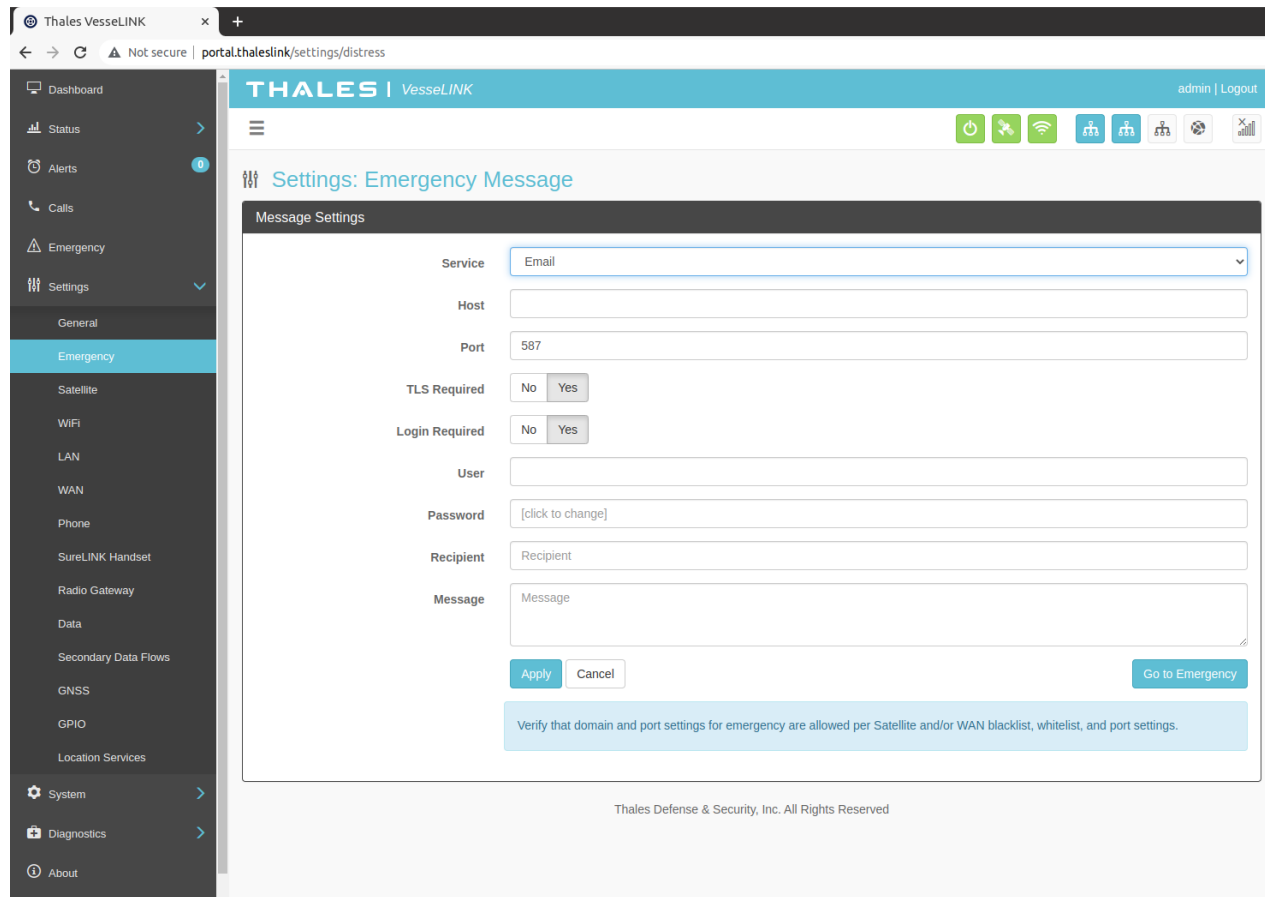









Figure 4-23 Settings → Emergency

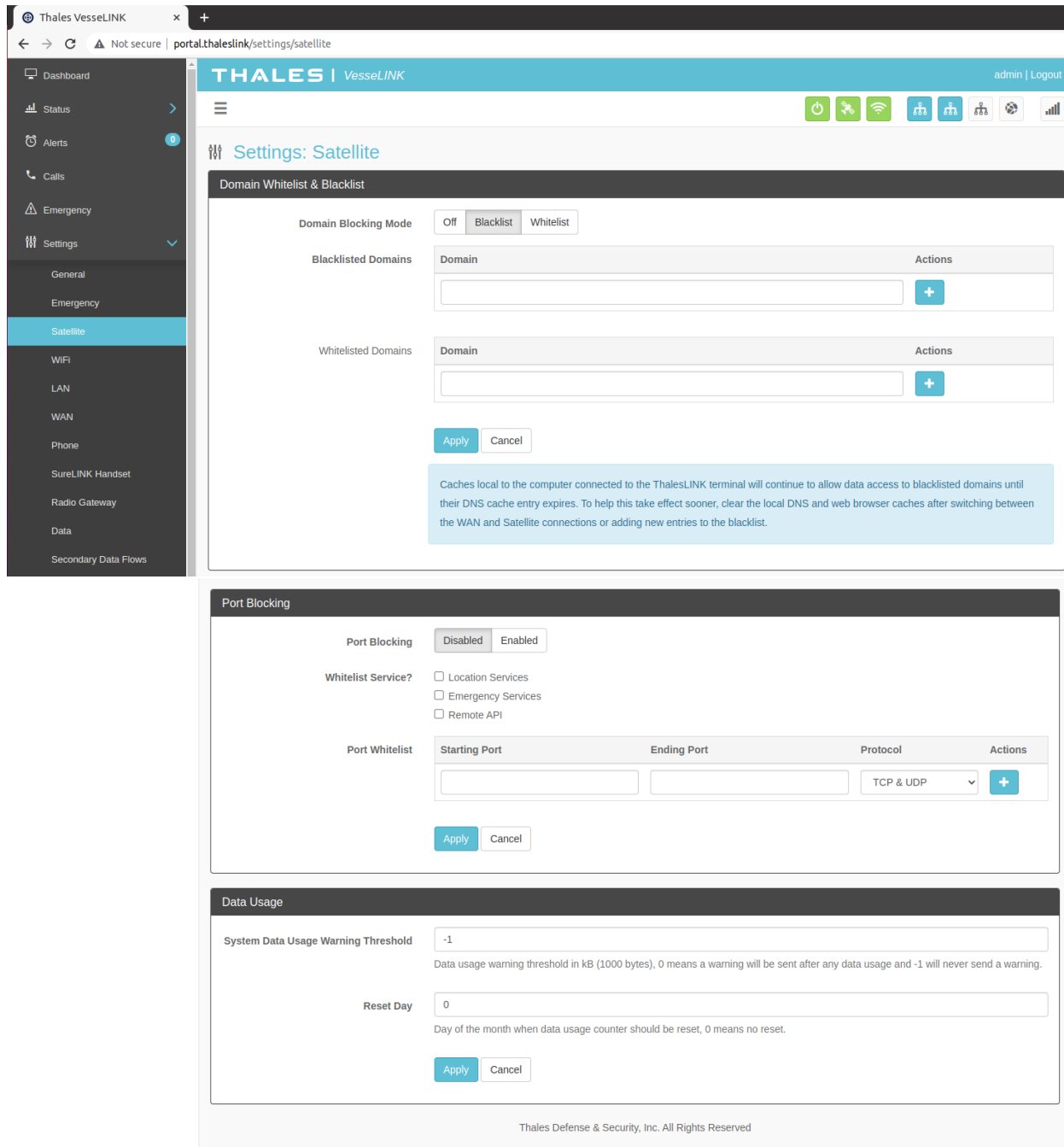
Table 4-4 Settings → Emergency

Section	Parameters
Service	Select either Email or <b>OFF</b> ( <b>OFF</b> is the default setting)
Host	Enter the host name (example: smtp.gmail.com)
Port	Enter the port number (example: 587)
TLS Required	Select either <b>YES</b> or <b>NO</b> ( <b>YES</b> is the default setting)
Login Required	Select either <b>YES</b> or <b>NO</b> ( <b>YES</b> is the default setting)
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 4-24, 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 Black/Whitelist it is always necessary to first select the  button BEFORE selecting the  button. After selecting the  button, the domain can always be edited or deleted using the   buttons BEFORE selecting the  button to save. If the  button is not selected before leaving the Satellite menu item, the data will not be saved.



Thales VesseLINK

portal.thaleslink/settings/satellite


admin | Logout

## Settings: Satellite


### Domain Whitelist & Blacklist



Domain Blocking Mode: ☐ Off ☒ Blacklist ☐ Whitelist

**Blacklisted Domains**

Domain	Actions
<input type="text"/>	

**Whitelisted Domains**

Domain	Actions
<input type="text"/>	

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.

### Port Blocking

Port Blocking: ☒ Disabled ☐ Enabled


Whitelist Service?



☐ Location Services

☐ Emergency Services

☐ Remote API

**Port Whitelist**

Starting Port	Ending Port	Protocol	Actions
<input type="text"/>	<input type="text"/>	TCP & UDP	



### Data Usage

System Data Usage Warning Threshold:

Data usage warning threshold in kB (1000 bytes), 0 means a warning will be sent after any data usage and -1 will never send a warning.

Reset Day:

Day of the month when data usage counter should be reset, 0 means no reset.

Thales Defense & Security, Inc. All Rights Reserved

Figure 4-24 Settings → Satellite Screen

Table 4-5 Settings → Satellite

Section	Value
<b>Domain Whitelist &amp; BlackList</b>	
Domain Blocking Mode	<b>OFF</b> / Blacklist / Whitelist ( <b>OFF</b> is the default setting)
Blacklisting	Enabling <u>allows ALL</u> websites EXCEPT those listed (very little restriction)
Whitelisting	Enabling <u>blocks ALL</u> websites EXCEPT those listed (the most restriction)
<b>Port Blocking</b>	
Port Blocking	<b>Disabled</b> / Enabled ( <b>Disabled</b> 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 ( <b>TCP &amp; UDP</b> or TCP only or UDP only) ( <b>TCP &amp; UDP</b> is the default setting)
<b>Data Usage</b>	
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 provided 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 4-25 allows setup of the Wi-Fi service.

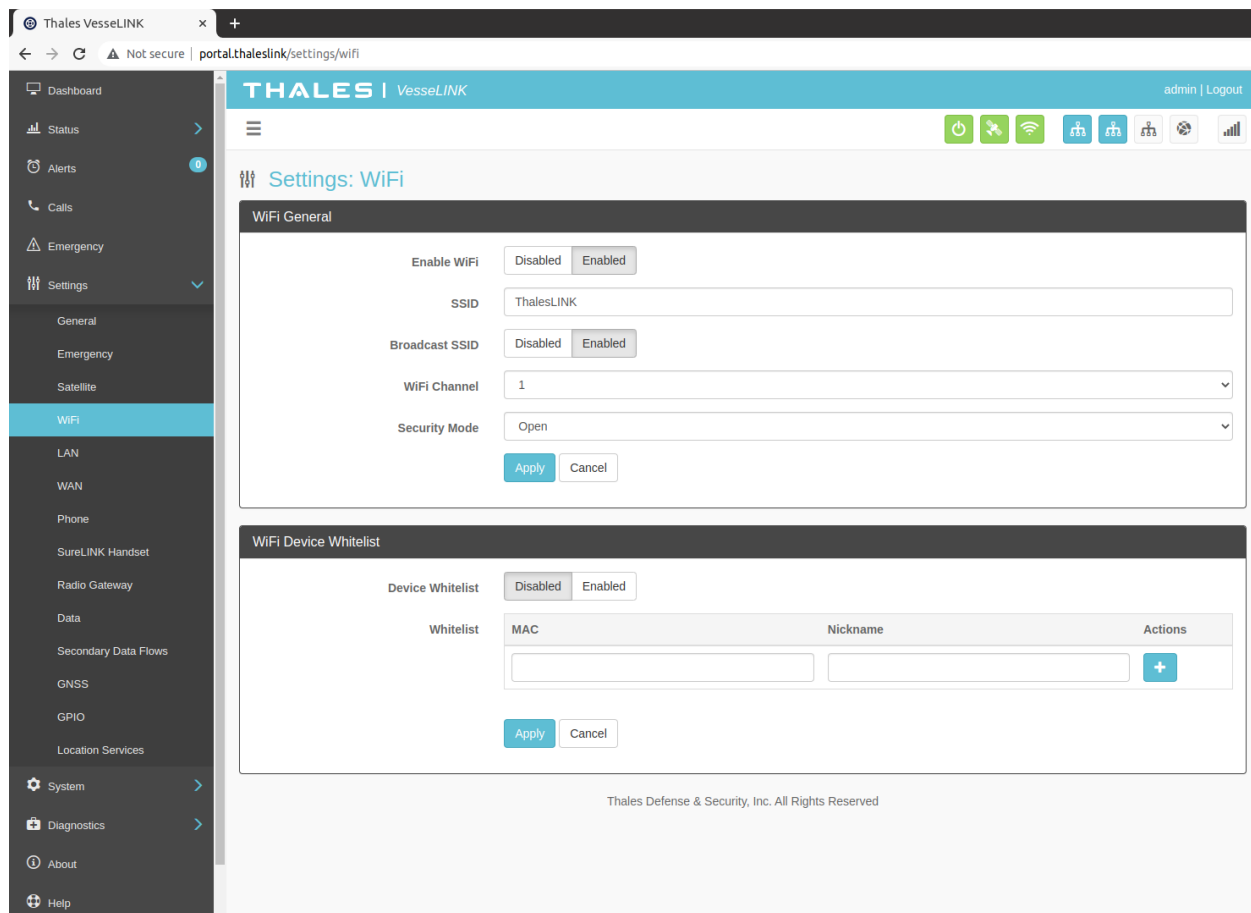


Figure 4-25 Settings → Wi-Fi Screen



Table 4-6 Settings → Wi-Fi

Section	Value
<b>WiFi General</b>	
Enable Wi-Fi	Disabled / <b>Enabled</b> ( <b>Enabled</b> is the default setting)
SSID	Enter the name of the SSID. ThalesLINK is default.
Broadcast SSID	Disabled / <b>Enabled</b> ( <b>Enabled</b> is the default setting)
Wi-Fi Channel	Set the Wi-Fi Channel 1 – 11
Security Mode	Set the security mode for the channel – <b>OPEN</b> or WPA2. <b>OPEN</b> 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.
<b>Wi-Fi Device Whitelist</b>	
Device Whitelist	<b>Disabled</b> / Enabled ( <b>Disabled</b> 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



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 can't be found, a simple way is that while the Device Whitelist is DISABLED, connect the device to be whitelisted to the Wi-Fi system by selecting the correct Wi-Fi Network (SSID) and typing in the Security Code if WPA2 is enabled. Once connected, go to STATUS → CURRENT DEVICES menu item and find the device Hostname in the list of Allocated IPs. The MAC address will be in the left column.




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.

## LAN



### **NOTE**

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

The LAN page, shown in Figure 4-26, 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 4-7 for more information on the information that is entered.



**NOTE**

Please use "portal.thaleslink" as the NTP server.

Thales VesseLINK

portal.thaleslink/settings/lan

Dashboard

Status

Alerts

Calls

Emergency

Settings

General

Emergency

Satellite

WiFi

LAN

WAN

Phone

SureLINK Handset

Radio Gateway

Data

Secondary Data Flows

GNSS

GPIO

Location Services

System

Diagnostics

About

THALES | VesseLINK

admin | Logout

Settings: Lan

LAN Ports

LAN Port 1

POE Off

POE On

LAN Port 2

POE Off

POE On

Disabled

Enabled

LAN Port 3

POE Off

POE On

Disabled

Enabled

Apply

Cancel

Static Routes

Name	Subnet IP	Subnet Prefix	Gateway IP	Actions
		/ 24	192.168.50.	+

Apply

Cancel

LAN MAC Address

MAC Address

18:39:19: 00:00:04

Apply

Cancel

DHCP

Enable DHCP

Disabled

Enabled

IP Address

192.168.50.1

Mask

255.255.255.0

Start

101

End

160

Lease Time

168

hr

0

min

Apply

Cancel

DHCP Reservations

Name	Duration	MAC	Address	Enabled	Actions		
	0	sec		192.168.50.	Disabled	Enabled	+

Apply

Cancel

Thales Defense & Security, Inc. All Rights Reserved

Figure 4-26 Settings → LAN Screen


Table 4-7 Settings → LAN

Section	Value
<b>LAN Ports</b>	
LAN Port 1 1	POE OFF / <b>POE ON</b> ( <b>POE ON</b> is the default setting)
LAN Port 2	Disable POE OFF / <b>POE ON</b> ( <b>POE ON</b> is the default setting) Disabled / <b>Enabled</b> ( <b>Enabled</b> is the default setting)
LAN Port 3	POE OFF / <b>POE ON</b> ( <b>POE ON</b> is the default setting) Disabled / <b>Enabled</b> ( <b>Enabled</b> is the default setting)
<b>Static Routes</b>	
Static Route	Enter the Name, Subnet IP Address, Subnet Prefix, and Gateway IP address for the static route (Note: The Gateway address assigned to the router that connects the terminal to the network.)
<b>LAN MAC Address</b>	
MAC Address	Enter the MAC address (same for all LAN switches)
<b>DHCP</b>	
Enable DHCP	Disabled / <b>Enabled</b> ( <b>Enabled</b> 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)
<b>DHCP Reservations</b>	
Name	Enter the name of the DHCP Reservation
Duration	Enter the length of time (in seconds, min of 120 seconds)
MAC	Enter the MAC address
Address	Enter the last digits of the IP Address
Enabled/Disabled	Disabled / <b>Enabled</b> ( <b>Enabled</b> is the default setting)








## 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 4-27, 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  button. After selecting the  button, the domain can always be edited or deleted using the   buttons BEFORE selecting the  button to save. If the  button is not selected before leaving the WAN menu item, the data will not be saved.



### 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.



### NOTE

If a WAN Modem connection is changed, it is important to remember that the terminal unit will need to re-started.

Additional details about these settings are described in Table 4-8.



Thales VesseLINK

admin | Logout

## Settings: WAN

### Configuration

Polling Interval: 30

Hostname: Certus

WAN Failover Ping Address: Default

Mode: ☒ DHCP ☐ Static

### Domain Whitelist & Blacklist

Domain Blocking Mode: ☐ Off ☒ Blacklist ☐ Whitelist

Blacklisted Domains

Domain	Actions
<input type="text"/>	<input type="button" value="+"/> <input type="button" value="x"/>

Whitelisted Domains

Domain	Actions
<input type="text"/>	<input type="button" value="+"/> <input type="button" value="x"/>

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.

### Port Blocking

Port Blocking: ☒ Disabled ☐ Enabled

Whitelist Service?

☐ Location Services

☐ Emergency Services

☐ Remote API

Port Whitelist

Starting Port	Ending Port	Protocol	Actions
<input type="text"/>	<input type="text"/>	TCP & UDP	<input type="button" value="+"/> <input type="button" value="x"/>

Thales Defense & Security, Inc. All Rights Reserved


Figure 4-27 Settings → WAN Screen

Table 4-8 Settings → WAN



Section	Value
<b>Configuration</b>	
Polling Intervals	Sets the length of polling intervals, 30 is the default setting
Hostname	Lists the Hostname. <b>Certus™</b> 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 <b>DHCP</b> or Static. ( <b>DHCP</b> is the default setting.)
<b>Domain Whitelist &amp; Black List</b>	
Domain Blocking Mode	<b>OFF</b> / Blacklist / Whitelist ( <b>OFF</b> is the default setting)
Blacklisting	Enabling <u>allows ALL</u> websites EXCEPT those listed (very little restriction)
Whitelisting	Enabling <u>blocks ALL</u> websites EXCEPT those listed (the most restriction)
<b>Port Blocking</b>	
Port Blocking	<b>Disabled</b> / Enabled ( <b>Disabled</b> 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 ( <b>TCP &amp; UDP</b> or TCP only or UDP only) ( <b>TCP &amp; UDP</b> is the default setting)

## Phone












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 4-28, allows configuration of phone extensions and mapping of those extensions to the outbound Iridium phone lines as well as which extension rings for each inbound Iridium line. 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. All changes are saved only after the APPLY button is selected.

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

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

When adding an extension, it is always necessary to first select the  button BEFORE selecting the  button. Several extensions can be added by selecting the  button multiple times, and then selecting the  button. After selecting the  button, the extension can always be edited or deleted selecting the   buttons BEFORE selecting the  button to save. If the  button is not selected before leaving the Phone menu item, the data will not be saved. Table 4-9 describes the settings in more detail.

Thales VesseLINK

portal.thaleslink/settings/phone

Dashboard

Status

Alerts

Calls

Emergency

Settings

General

Emergency

Satellite

WiFi

LAN

WAN

Phone

SureLINK Handset

Radio Gateway

Data

Secondary Data Flows

GNSS

GPIO

Location Services

System

Diagnostics

About

THALES | VesseLINK

admin | Logout

Settings: Phone

Extension Management

Dial Plan

Disable

Enable

Extensions

Extension	Outbound Lines	Password	Actions
1001	<div>Line 1</div> <div>Line 2</div> <div>Line 3</div>	[hidden]	<div></div> <div></div>
1002	<div>Line 1</div> <div>Line 2</div> <div>Line 3</div>	[hidden]	<div></div> <div></div>
1003	<div>Line 1</div> <div>Line 2</div> <div>Line 3</div>	[hidden]	<div></div> <div></div>
	<div>Line 1</div> <div>Line 2</div> <div>Line 3</div>		<div></div>

Inbound Iridium Lines

Line 1 (881677120829)

1001

Line 2 (881677120916)

1002

Line 3

1003

Device Mapping

Pots 1

1001

Pots 2

1002

Radio GW

<none>

Apply

Cancel

Phone Configuration

Enable Call Log

Disabled

Enabled

POTS Impedance

USA

POTS Compliance

USA

Apply

Cancel

Thales Defense & Security, Inc. All Rights Reserved

Figure 4-28 Settings → Phone Screen

Table 4-9 Settings → Phone

Section	Value
<b>Dial Plan</b>	
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.) ( <b>ENABLED</b> is the default setting)
<b>Extension Mapping</b>	
1-88888	Additional custom extensions of varying lengths can be added.
1001	Default extension that receives and makes calls on the first Iridium line. Connected to the first POTS line.
1002	Default extension that receives and makes calls on the second Iridium line. Connected to the second POTS line.
1003	Default extension-s that receives and makes calls on the third Iridium line.
<b>Inbound Iridium Lines</b>	
1-88888	Maps each inbound Iridium line to a single extension previously set up.
1001 - 1003	Default extensions 1001, 1002 and 1003 are mapped to Line 1, Line 2 and Line 3 respectively

Section	Value
<b>Device Mapping</b>	
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
<b>Phone Configuration</b>	
Enable Call Log	Disabled / <b>Enabled</b> ( <b>Enabled</b> is the default setting). Call logs display Active Calls and Call History when the Calls menu item is selected.
POTS Impedance	Sets the dynamic output of the POTS system to match regional Phone types ( <b>USA</b> , Australia, Europe, UK, USA-Loaded) ( <b>USA</b> is the default setting)
POTS Compliance	Sets the POTS Compliance to match regional phone types. (USA or Brazil). ( <b>USA</b> is the default setting)



**NOTE**

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

## VoIP Phone Settings



Please use "portal.theslink" as the NTP server.

### NOTE

The two VoIP phones that Thales recommends include the CISCO SPA504G and the Grand Stream GXP2140. Other phones may work with the VesseLINK 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 VesseLINK 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 VesseLINK Terminal.
- 2.) View the Management Portal <http://portal.theslink> (or <https://portal.theslink>)). Note that the SETTINGS →PHONE extensions 1001, 1002, and 1003 are pre-configured as shown in Figure 4-29.

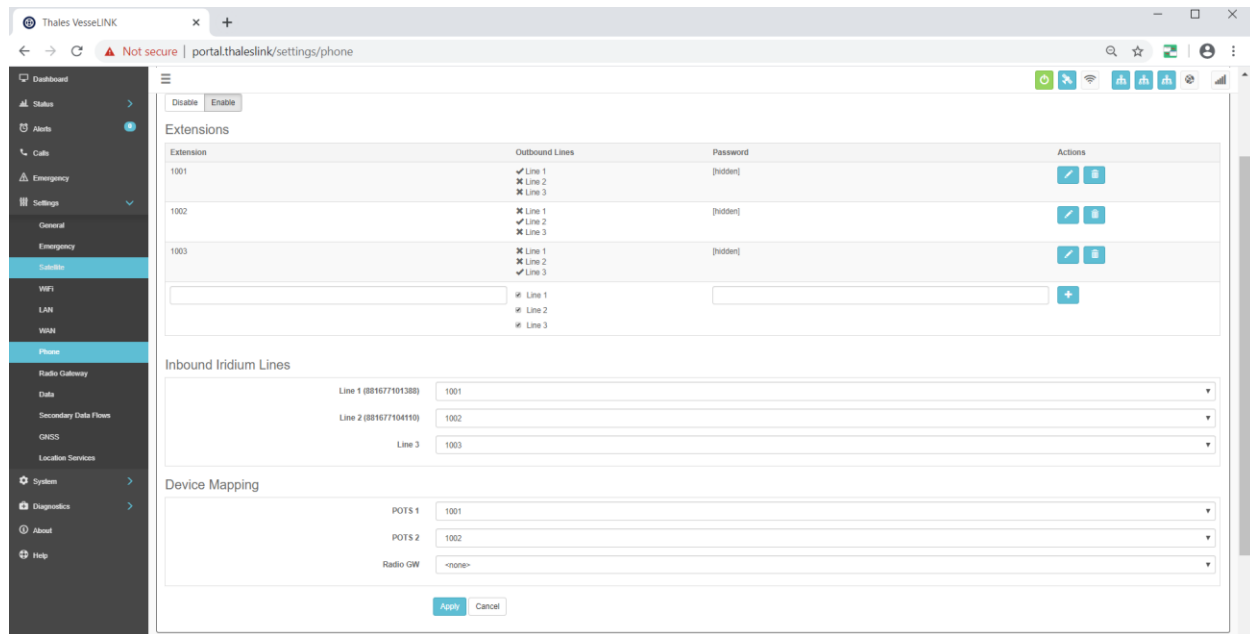


Figure 4-29 VOIP Phone Settings

- 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 4-30 below.

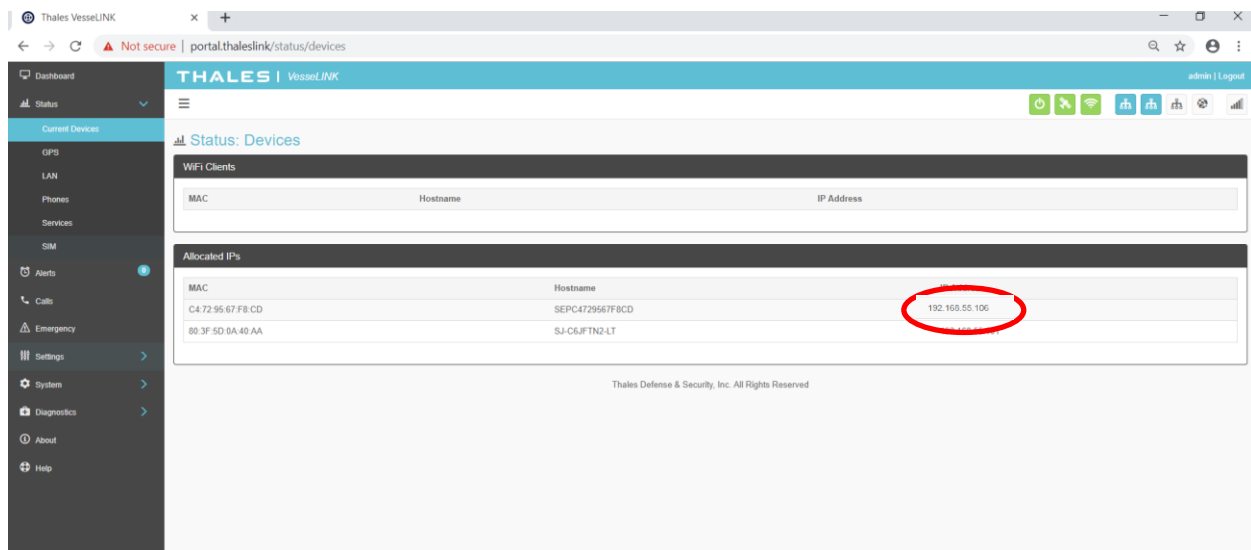


Figure 4-30 CISCO SPA504G IP Address

- 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”.



- 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 4-31 for the entries above.

The screenshot shows the Cisco SPA504G Configuration Utility web interface. The browser address bar shows the URL `192.168.55.106/admin/basic`. The interface has a top navigation bar with tabs: Info, System, SIP, Regional, Phone, and User. The 'User' tab is selected. Below the tabs, there are sections for General, NAT Settings, SIP Settings, Call Feature Settings, Proxy and Registration, Subscriber Information, and Audio Configuration. In the 'Subscriber Information' section, the 'Display Name', 'User ID', and 'Password' fields are all set to '1001'. The 'Auth ID' field is empty. In the 'Proxy and Registration' section, the 'Proxy' field is set to 'sip:thaleslink'. At the bottom of the form, there are two buttons: 'Undo All Changes' and 'Submit All Changes'. The 'Submit All Changes' button is circled in blue.

Figure 4-31 SPA504G Configuration Utility

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

## GRAND STREAM GXP2140

This procedure assumes that the VesseLINK 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 VesseLINK Terminal.
- 2.) View the Management Portal (<http://portal.theslink> or <https://portal.theslink>). Note that the SETTINGS → PHONE extensions 1001, 1002, and 1003 are pre-configured as shown in Figure 4-31 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 4-30 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 4-32 Grand Stream GXP2140 Configuration Page below.
  - a. In the SIP Server field, enter "sip.theslink".
  - 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 4-32 below for the entries above.

*Figure 4-32 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.

This section of the manual details how to install, update, or uninstall SureLINK apps that are provided in the VesseLINK system through software updates. Figure 4-33 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.



### **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 VesseLINK system is listed here along with the option to change its installation status.

The screenshot displays the 'Settings: SureLINK Handset' page in the Thales VesseLINK web interface. The interface includes a sidebar with navigation options: Dashboard, Status, Alerts, Calls, Emergency, Settings, SureLINK Handset, Radio Gateway, Data, Secondary Data Flows, GNSS, GPIO, Location Services, System, Diagnostics, About, and Help. The main content area is titled 'Settings: SureLINK Handset' and features a 'General' section with 'Application Configuration' set to 'Automatic'. Below this is the 'Automatic Settings' section, which contains a table with columns for Name, Version, and Desired Status. The table lists 'ESChat' with version '25.10' and a 'Desired Status' of 'No Change'. At the bottom of the page, the 'Devices' section shows a table with columns for Name, IP Address, MAC Address, Status, and Type, listing a device with ID 'android-65c3ce354065e631' and status 'online'. The footer of the page reads 'Thales Defense & Security, Inc. All Rights Reserved'.

Name	Version	Desired Status
ESChat	25.10	No Change

Name	IP Address	MAC Address	Status	Type
android-65c3ce354065e631	192.168.50.102	6A-CF-6A-98-B9-28	online	SureLINK

Figure 4-33 Settings → SureLINK Handset Automatic App Configuration

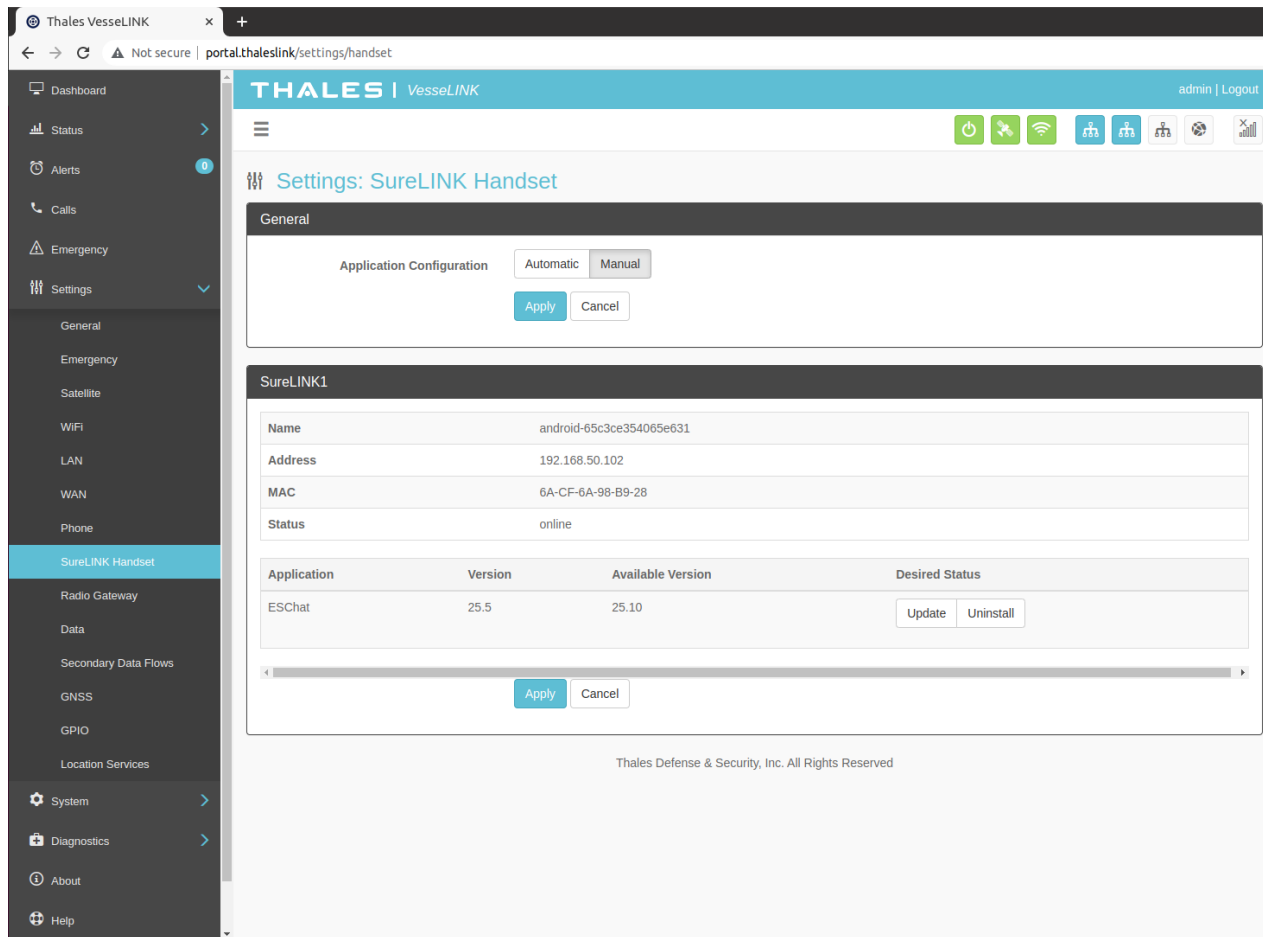


Figure 4-34 Settings → SureLINK Handset Manual App Configuration



In Figure 4-33 and Figure 4-34, 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 4-10 Settings → SureLINK Handset


Section	Value
<b>General</b>	
Application Configuration	<b>Automatic</b> / Manual
<b>Automatic Settings</b>	
Name	The name of the Application as it appears on the VesseLINK
Version	Version of the App as it appears on the VesseLINK.
Desired Status	<b>No Change</b> , 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

Section	Value
	upgrades as well. Uninstall will always uninstall the app if it is seen on the SureLINK, no matter the version.
<b>Devices (Automatic Configuration)</b>	
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
<b>SureLINK 1 (Manual Configuration)</b>	
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 VesseLINK
Version	Version of the App as it appears on the VesseLINK.
Available Version	Version of the App as it appears on the VesseLINK
Desired Status	<p>Install/Update, or Uninstall</p> <p><i>Install/Update</i> will put the latest available version of software on the SureLINK. If the Application is not already on the SureLINK, <i>Install</i> will be seen instead of <i>Update</i> 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 VesseLINK, the <i>Install/Update</i> button will be grayed out and not selectable.</p> <p><i>Uninstall</i> removes the specific App from the SureLINK and will always be an available option.</p>

## Radio Gateway



### 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 screenshot displays the 'Settings: Radio Gateway' configuration page in the Thales VesseLINK web interface. The left sidebar contains navigation options: Dashboard, Status, Alerts, Calls, Emergency, Settings (selected), System, Diagnostics, About, and Help. The 'Settings' menu is expanded, showing sub-options: General, Emergency, Satellite, WiFi, LAN, WAN, Phone, SureLINK Handset, Radio Gateway (selected), Data, Secondary Data Flows, GNSS, GPIO, and Location Services.

The main content area is titled 'Settings: Radio Gateway' and includes a 'Configuration' section. The settings are organized into several sections:

- Transmit VoIP Control:**
  - Mode: VAD (dropdown)
  - DTMF: 'On': \*
  - DTMF: 'Off': #
  - VAD: Voice Hangtime: 500 (Milliseconds)
- Transmit Audio:**
  - Delay: 300 (Milliseconds)
  - Analog Gain: -20 (dB)
  - Digital Gains: -20 (dB)
  - VAD: Threshold: -35 (dBFS)
- Transmit/Radio PTT:**
  - Active Level: High (radio button), Low (radio button)
  - Timeout: 300 (seconds)
- Receive Activity:**
  - Mode: VAD (dropdown)
  - VAD: Voice Hangtime: 500 (Milliseconds)
  - GPIO: Active Level: High (radio button), Low (radio button)
- Receive Audio:**
  - DTMF Threshold: -25 (dBFS)
  - VAD: Threshold: -35 (dBFS)
  - Analog Gain: 0 (dB)
  - Digital Gains: 0 (dB)
- Calling:**
  - DTMF Dialing Process: \*\*
  - DTMF Disconnect Phrase: ##
  - Answer Timeout: 3 (seconds)
  - Max Digits: 20
  - Dialing Duration: 1000 (Milliseconds)
  - Disconnect Duration: 2000 (Milliseconds)
  - Error Duration: 2000 (Milliseconds)
  - Answer Timeout: 60 (seconds)

At the bottom of the 'Calling' section, there are 'Apply' and 'Cancel' buttons.

Figure 4-35 Settings → Radio Gateway



Table 4-11 Settings → Radio Gateway

Section	Value
<b>Configuration</b>	
<b>Transmit VoIP Gateway</b>	
Mode	DTMF or Voice Activated Dialing ( <b>VAD</b> ) ( <b>VAD</b> 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 <b>500</b> msec).
<b>Transmit Audio</b>	
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 <b>300</b> 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 <b>-20</b> 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 <b>-20</b> 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 <b>-35</b> dBFS)
<b>Transmit / Radio PTT</b>	
Active Level	<b>Enabled</b> / Disabled ( <b>ENABLED</b> 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.
<b>Receive Activity</b>	
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 <b>VAD</b> or GPIO (Default setting is <b>VAD</b> ).


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 <b>500</b> msec).
GPIO: Active Low	If Receive Activity Mode is set to “GPIO”, set the GPIO Active Level to either High or <b>Low</b> (Default setting is <b>Low</b> ).
<b>Receive Audio</b>	
DTMF: Threshold	For DTMF mode, controls the sensitivity of tone detection on incoming DTMF. Acceptable values -35 to 0 dBFS. (Default setting is <b>-20</b> dBFS)
VAD: Threshold	For VAD mode, controls the sensitivity of voice detection on incoming audio. Acceptable values -40 to 20 dBFS. (Default setting is <b>-35</b> 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 <b>0</b> 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 <b>-20</b> dB).
<b>Calling</b>	
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 $\geq 0$ sec. (Default setting is <b>3 sec</b> )
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 <b>not</b> count towards the maximum number of digits. Acceptable values $\geq 0$ . (Default setting is <b>20</b> )
Dialing Duration	When a radio-initiated outbound call is being placed, a burst of ring back tone is transmitted to the radio user for this amount of time as confirmation. Acceptable values $\geq 0$ msec. (Default value is <b>1000</b> 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 $\geq 0$ msec. (Default value is <b>2000</b> 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 $\geq 0$ msec. (Default value is <b>2000</b> 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 $\geq 0$ sec. (Default value is <b>60</b> 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-, 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.

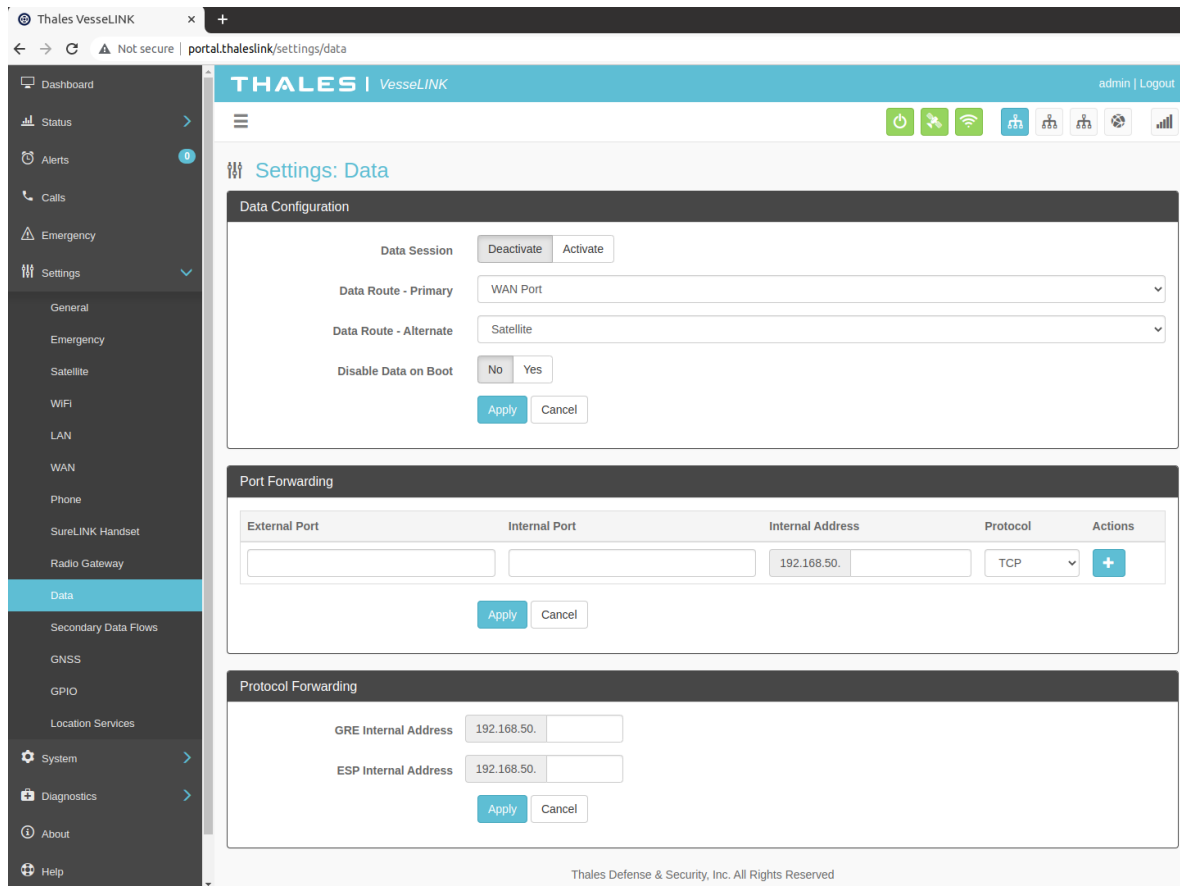


Figure 4-36 Settings → Data Screen

Table 4-12 Settings → Data

Section	Value
<b>Data Configuration</b>	
Data Session	<b>Deactivate</b> / Activate (deactivate is the default setting)
Data Route - Primary	Select the desired data route ( <b>WAN</b> or Satellite Port) (WAN is the default setting).
Data Route - Alternate	Select the desired alternate data route. ( <b>Satellite</b> 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	<b>NO</b> / YES ( <b>NO</b> is the default setting). Determines the default data operations state when the system is restarted.
<b>Port Forwarding</b>	
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.

Section	Value
<b>Protocol Forwarding</b>	
Protocol Forwarding	Enter the GRE Internal IP Address and/or the ESP Internal IP Address.




“Disable Data on Boot” allows the operator to manually set the data session to ON whenever the unit is powered on.

## NOTE

### Secondary Data Flow (SDF)



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.



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



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



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

## NOTE

Thales VesseLINK

portal.thaleslink/settings/sdf

Dashboard

Status

Alerts

Calls

Emergency

Settings

General

Emergency

Satellite

WiFi

LAN

WAN

Phone

SureLINK Handset

Radio Gateway

Data

Secondary Data Flows

GNSS

GPIO

Location Services

System

THALES | VesseLINK

admin | Logout

Settings: Secondary Data Flows

Port and Service Mapping

Ports

LAN Port 1

Default

VLAN Tag

Map

LAN Port 2

Default

VLAN Tag

Map

LAN Port 3

Default

VLAN Tag

Map

WiFi

Default

VLAN Tag

Map

Services

Location Services

(Default data route)

Emergency Services

(Default data route)

Remote Control (API)

SDF 3

Ports in VLAN Tag mode will not be connected to SDFs on Services

Apply

Cancel

SDF 1

VLAN Tag 5

State

Deactivate

Activate

Port Forwarding

External Port	Internal Port	Internal Address	Protocol	Actions
		192.168.11.	TCP	+

GRE Internal Address

192.168.11.

ESP Internal Address

192.168.11.

DHCP

Gateway	Start	End	Lease Time	Enabled
192.168.11.1/24	100	150	168 hr 0 min	Disabled Enabled

Apply

Cancel

SDF 3

State

Deactivate

Activate

Service Networks

Name	Destination	Prefix	Actions
		/ 24	+

Apply

Cancel

Figure 4-37 Settings → Secondary Data Flows

Table 4-13 Settings → Secondary Data Flows

Section	Value
Port and Service Mapping	
LAN Port 1	Default / VLAN Tag / Map  Select the mode for each port.  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. <b>Note:</b> The SDF must be activated by your Service Provider to be valid.
LAN Port 2	
LAN Port 3	
Wi-Fi	
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. <b>Note:</b> The SDF must be activated by your Service Provider to be valid.
Emergency Services	
Remote Control (API)	
External Port Configuration (Example SDF1 in Figure 4-35 above)	
State	Deactivate/ <b>Activate</b> , Turns on or off SDF X
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. <b>Enable</b> or Disable DHCP.
Internal Port Configuration (Example SDF3 in Figure 4-35 above)	
State	Deactivate/ <b>Activate</b> , 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.



**NOTE**

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

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.



## NOTE


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

Port and Service Mapping	
LAN Port 2	SDF 2
LAN Port 3	(Default data route)
WiFi	(Default data route)
Location Services	SDF 4
Emergency Services	(Default data route)
Remote Control (API)	SDF 1 SDF 2 SDF 3 SDF 4

## Global Navigation Satellite System (GNSS)



## 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.



## 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.



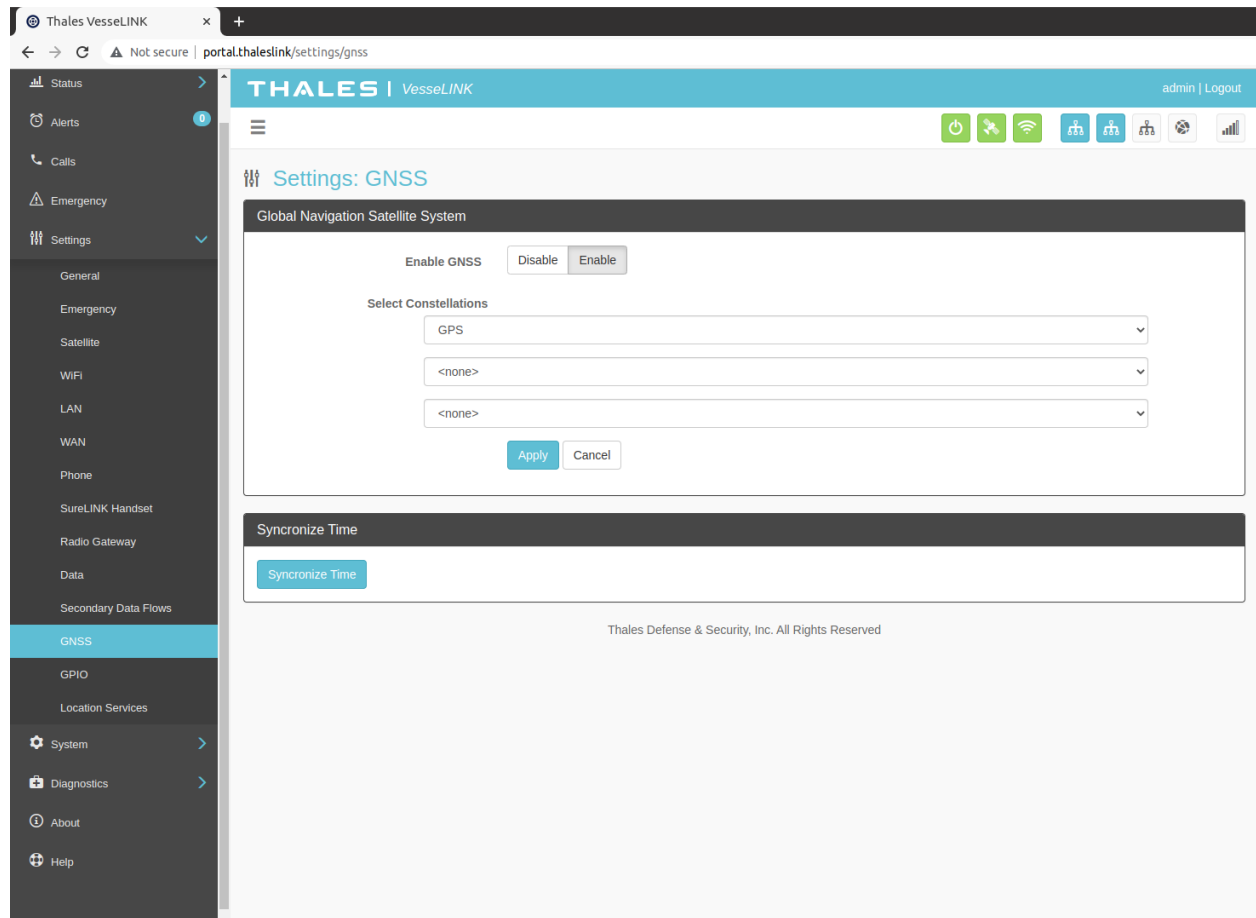


Figure 4-38 Settings → Global Navigation Satellite System

Table 4-14 Settings → Global Navigation Satellite System

Section	Value
<b>Global Navigation Satellite System</b>	
Enable GNSS	Select Disable or <b>Enable</b> . ( <b>Enable</b> is the default setting) When the setting is changed, the system requires a reboot (refer to Figure 4-).
Select Constellations	<p>Select up to three GNSS satellite constellations to receive positioning and timing data from. <b>GPS</b> is the default. When multiple constellations are chosen, the terminal uses the system with the best signal for position data.</p> <p>Note: When BeiDou and GLONASS are both selected, no other constellations can be selected.</p>
<b>Synchronize Time</b>	
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 4-39 Enable GNSS Reboot Notification Screen*




*Figure 4-40 Synchronize Time Confirmation Screen*

## GPIO



### **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.



### **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.

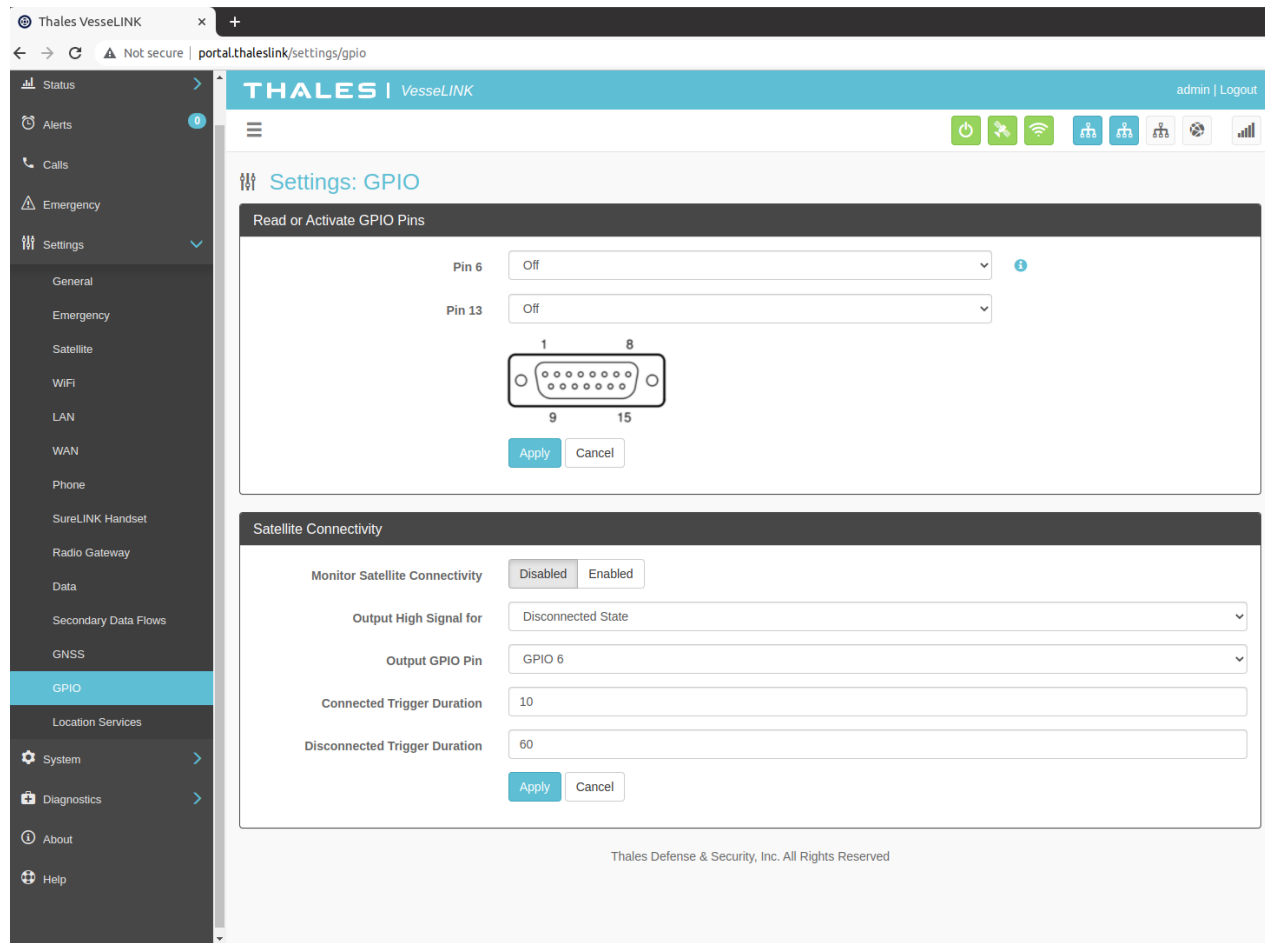


Figure 4-41 Settings → GPIO



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.

Table 4-15 Settings → GPIO

Section	Value
<b>Read or Activate GPIO Pins</b>	
Pin 6	<b>Off</b> / Input / Active. If <i>Input</i> is selected, the pin will be configured to read voltage applied to it, and if <i>Active</i> is selected, the pin will be powered with about 3.3.V.
Pin 13	<b>Off</b> / Input / Active. If <i>Input</i> is selected, the pin will be configured to read voltage applied to it, and if <i>Active</i> is selected, the pin will be powered with about 3.3.V.
<b>Satellite Connectivity</b>	
Monitor Satellite Connectivity	<b>Disabled</b> / Enabled
Output High Signal for	Connected State / <b>Disconnected State</b> (choose whether a high output signal represents a connected or disconnected state regarding the satellite )

Section	Value
Output GPIO Pin	<b>GPIO 6 / GPIO 13</b>
Connected Trigger Duration	Integer in seconds. Multiples of 5 are valid with a minimum of 5. Default is <b>10</b> .
Disconnected Trigger Duration	Integer in seconds. Multiples of 5 are valid with a minimum of 5. Default is <b>60</b> .

## Location Services

From the Location Services page, shown in Figure 4-, 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.

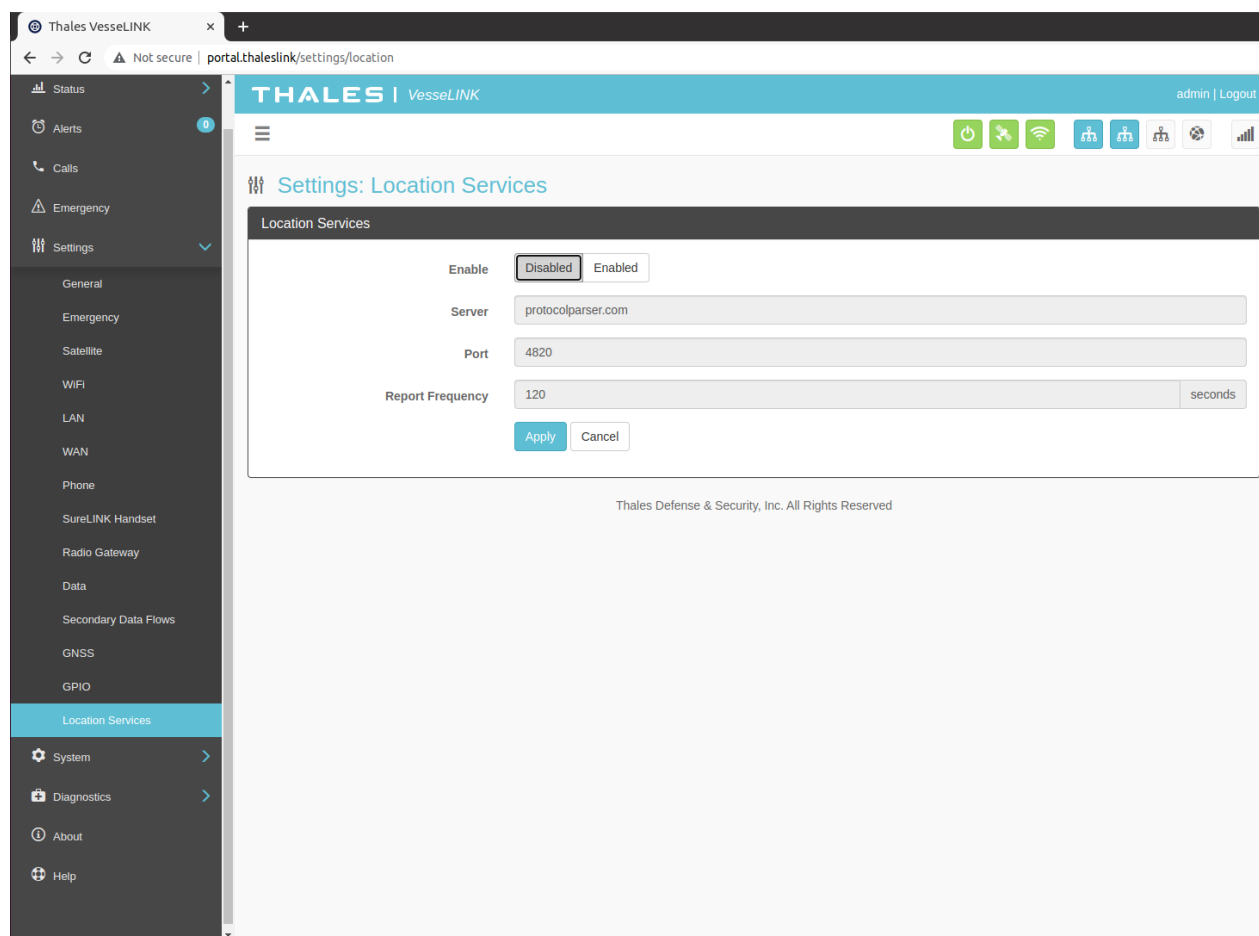


Figure 4-42 Settings → Location Services Screen

Table 4-16 Settings → Location Services


Section	Value
<b>Location Services</b>	
Enable	<b>Disabled</b> / Enabled ( <b>Disabled</b> 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.

## 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.

Refer to Figure 4-. When performing a firmware update, replacing a BDU, 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.

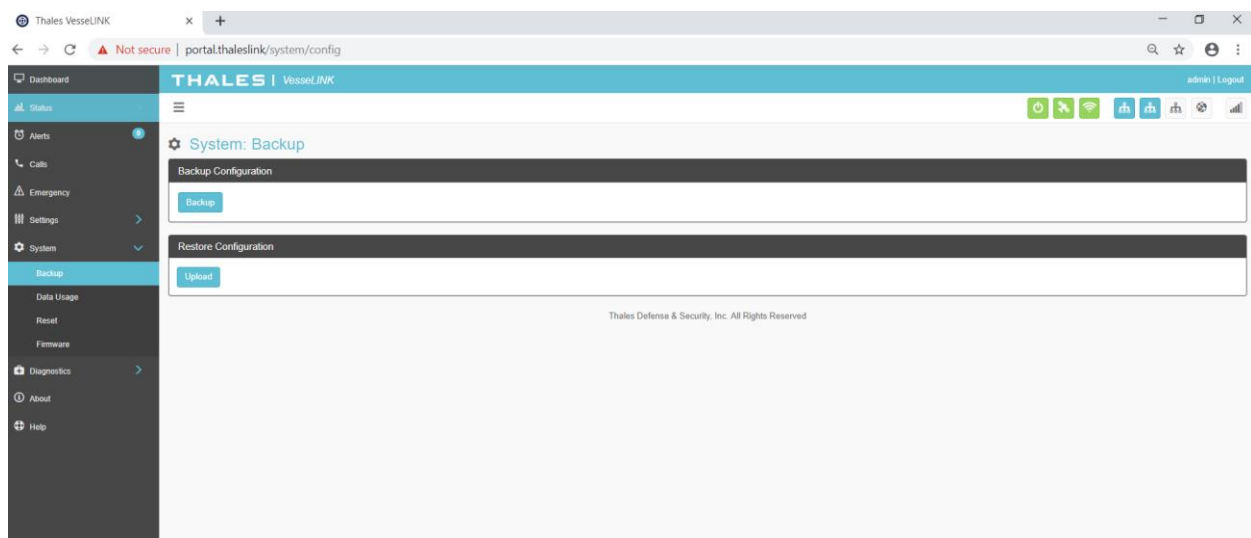


Figure 4-43 System → Backup Screen

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




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

**NOTE**

## Data Usage



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**

Refer to Figure 4-. 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-). For Satellite Data Limits – pressing the VIEW SATELLITE SETTINGS button, will bring up the SETTINGS → SATELLITE Screen (Figure 4-24).



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.

**NOTE**

Thales VesseLINK

admin | Logout

## System: Satellite Data Usage

NOTE: Usage numbers are estimates only.

System Satellite Data Usage	
Satellite Data Session	1455 KB
Satellite Data Total	198754 KB
Next Reset	Disabled
Warning Enabled	No

Satellite Data Session refers to usage since start-up, and Satellite Data Total refers to usage since last reset.

### Configure Satellite Data Usage

To monitor the usage of satellite data, go to "Settings: Satellite".

[Visit Satellite Settings](#)

### Reset Data Usage

Reset system data usage:

[Reset](#)

Thales Defense & Security, Inc. All Rights Reserved

Figure 4-44 System → Data Usage Screen

### Reset Data Usage

Reset system data usage:

[Reset](#)

**Confirmation Required**

Do you wish to reset all data usage?


[Yes, Reset](#) [No, Cancel](#)

Figure 4-45 Reset Data Usage Screen



## Reset



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

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

Backup Version will revert the system to the previous software version.

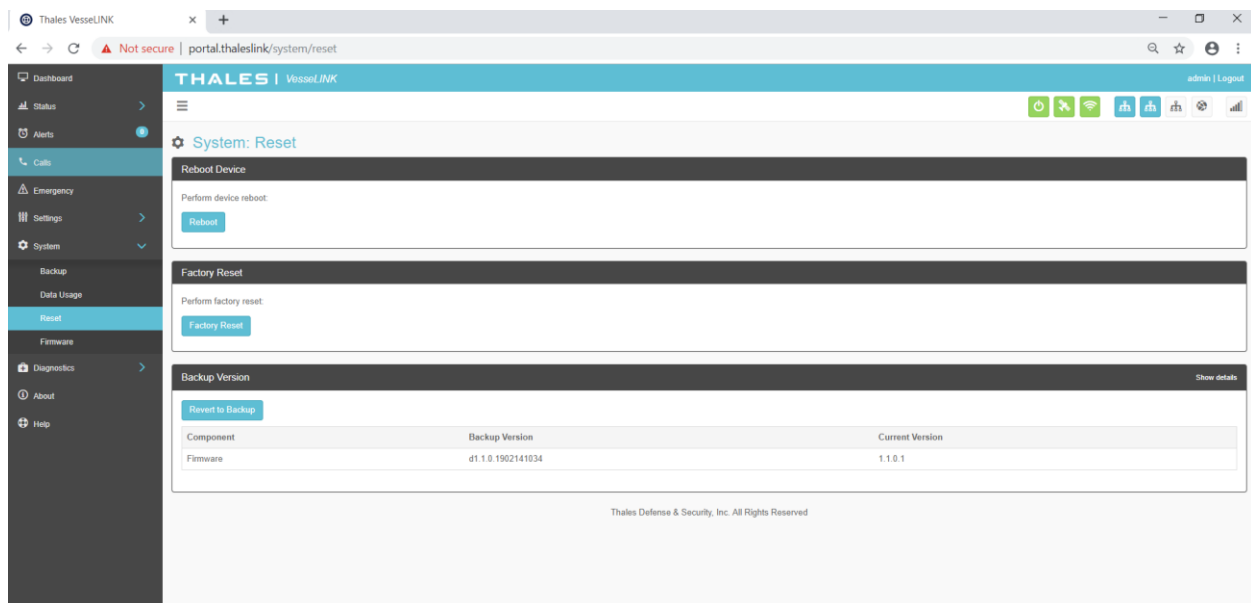


Figure 4-46 System → RESET



## NOTE

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 Figure 4- for configuration backup and restore.

## Firmware

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

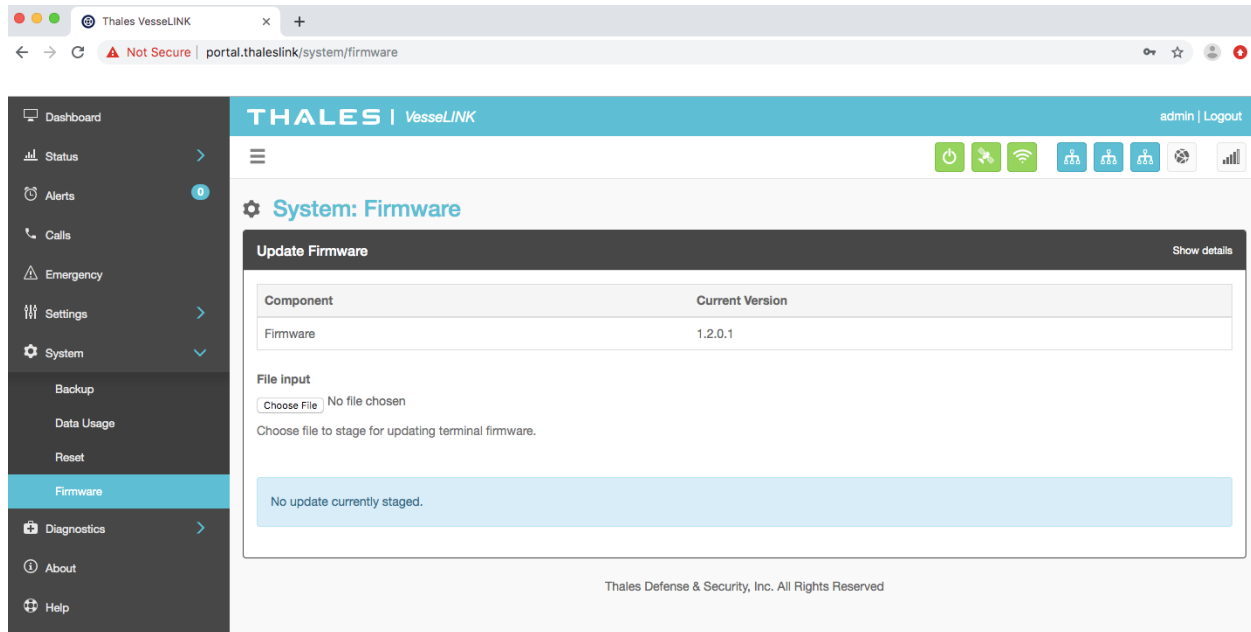


Figure 4-47 System → Firmware Screen

Selecting the SHOW DETAILS will display system level information (Figure 4-).

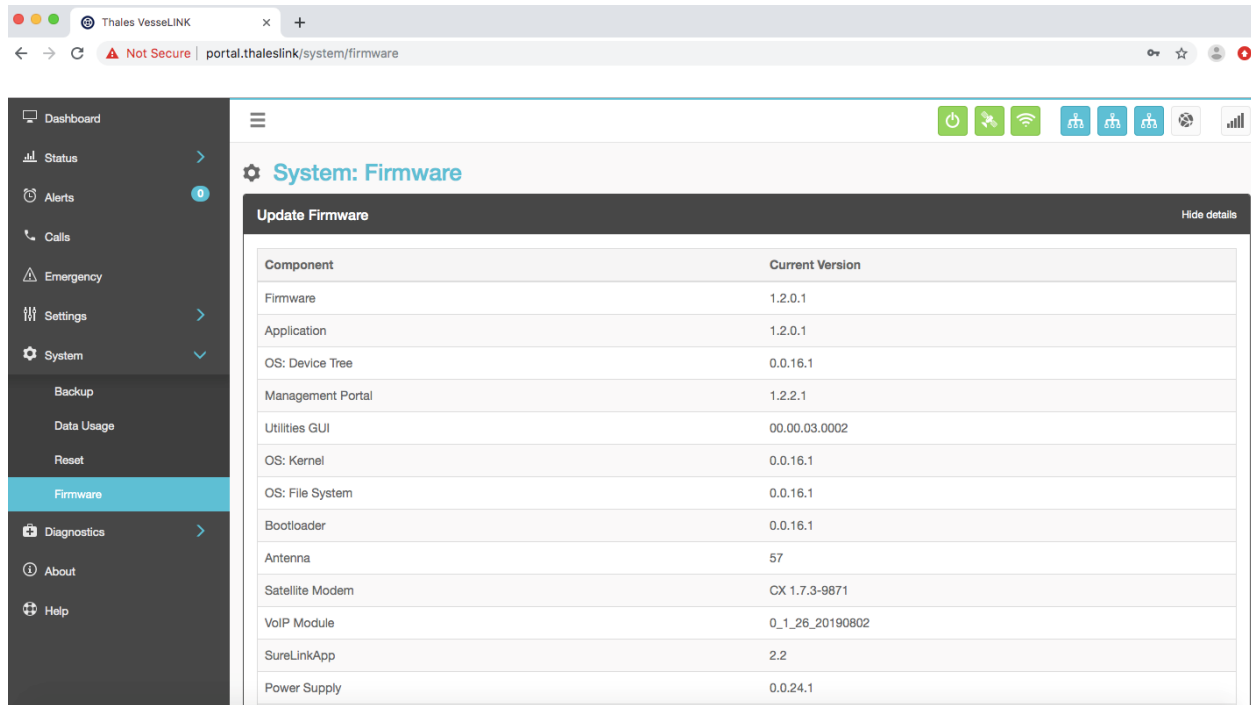


Figure 4-48 Firmware Screen – SHOW DETAILS




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

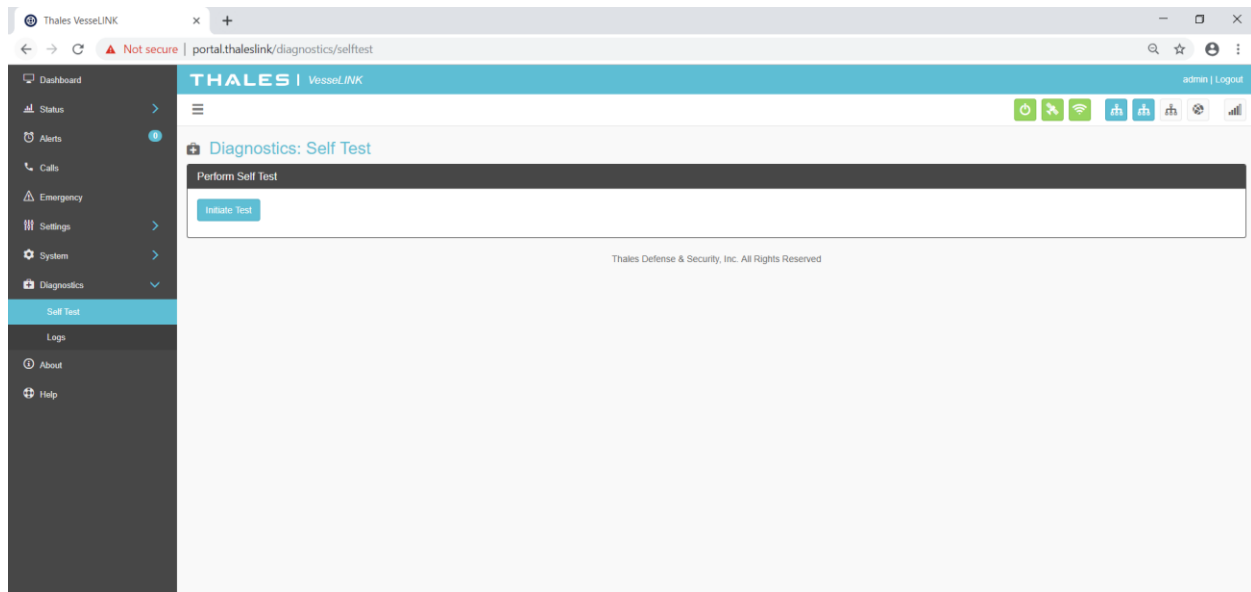
## Diagnostics

### Self-Test



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

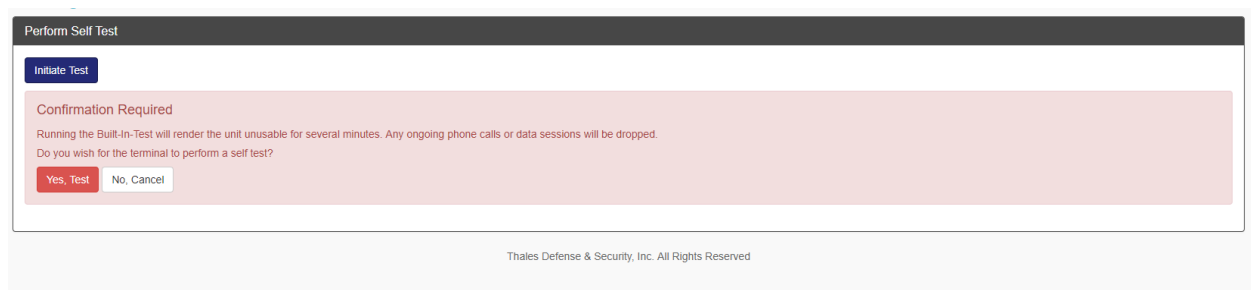


*Figure 4-49 Diagnostics → Self-Test Screen*

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



Running the Built-in-Test will render the unit unusable for several minutes. Any on-going calls or data sessions will be dropped.



*Figure 4-50 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-).

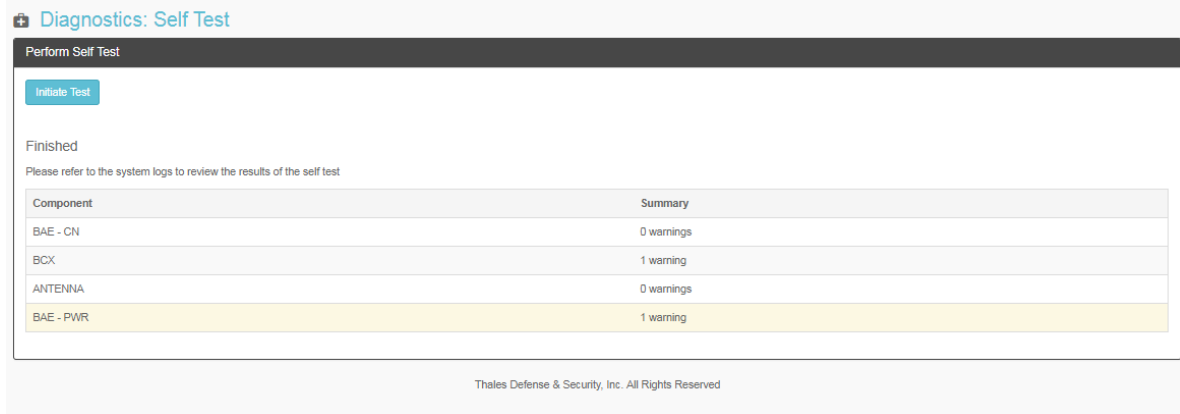


Figure 4-51 Perform Self-Test Completed Screen

## Diagnostics Logs

Refer to Figure 4-. 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.

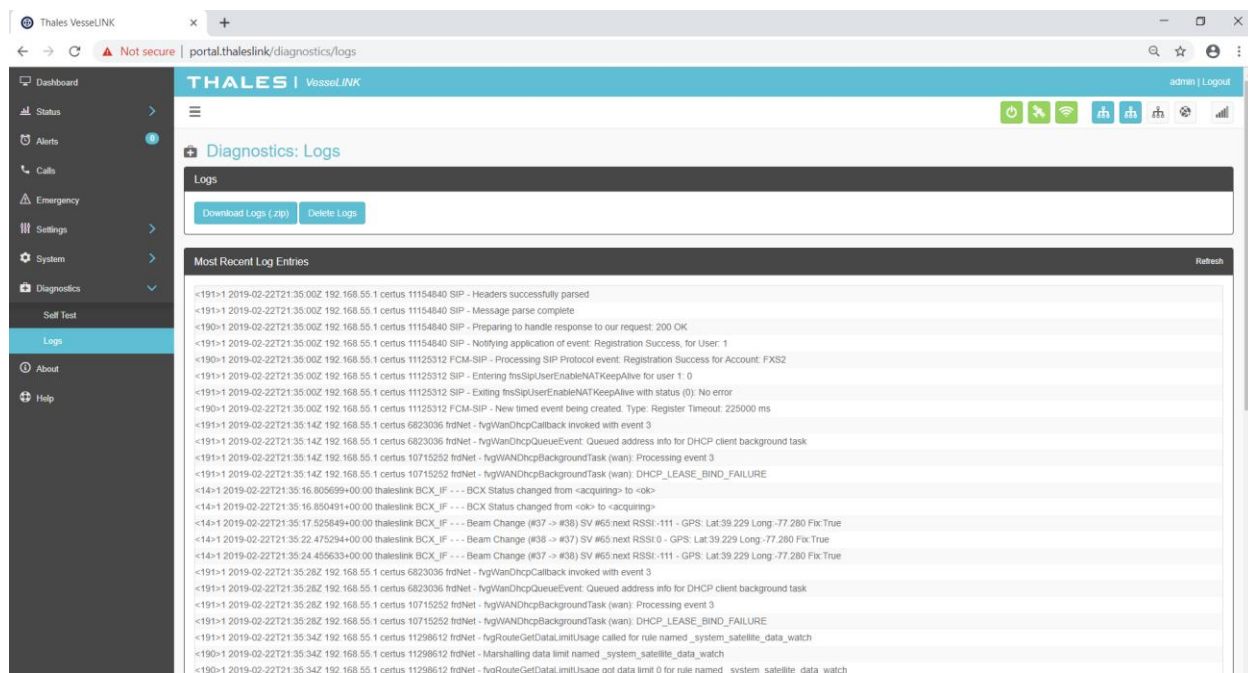


Figure 4-52 Diagnostics → Logs Screen



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

## About

Refer to Figure 4-. 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

The screenshot shows the 'About' page of the Thales VesselLINK interface. The page is divided into several sections, each containing a table of hardware and software details. The left sidebar contains navigation links: Dashboard, Status, Alerts, Calls, Emergency, Settings, System, Diagnostics, About (selected), and Help. The top right corner shows the user 'admin' and a 'Logout' link. The main content area is titled 'THALES | VesselLINK' and 'About'.

System	
Software Version	1.1.0.1
Application	1.1.0.1-1
OS	0.0.15-1-g93a0baf
Portal	1.0.3.1
Product Family	VesselLINK
Model Number	VF350BM
Serial #	10011
Hardware Version	5
System MAC Address	18:39:19:00:00:04

Antenna	
Software Version	57
Hardware Version	3
Antenna Type	H2
Model	5
Serial #	900030

Satellite modem	
Software Version	CX 1.7.2-7826
Hardware Version	5042-PCB-01 REV B/C
Serial #	IRD0007S
IMEI	300008060003140

Power Supply	
Software Version	24

VOIP Module	
Software Version	0.1.20.20190212
Hardware Version	5.3.0
Serial #	18:39:19:40:27:81
LAN MAC Address	18:39:19:00:00:04
WAN MAC Address	18:39:19:40:27:81

WiFi	
Software Version	1.4.2.37542
Hardware Version	5
WiFi MAC Address	88:6B:0F:33:6F:8C

These commodities, technology or software were exported from the U.S. in accordance with the Export Administration Regulations. Diversion contrary to U.S. law prohibited.

Thales Defense & Security, Inc. All Rights Reserved

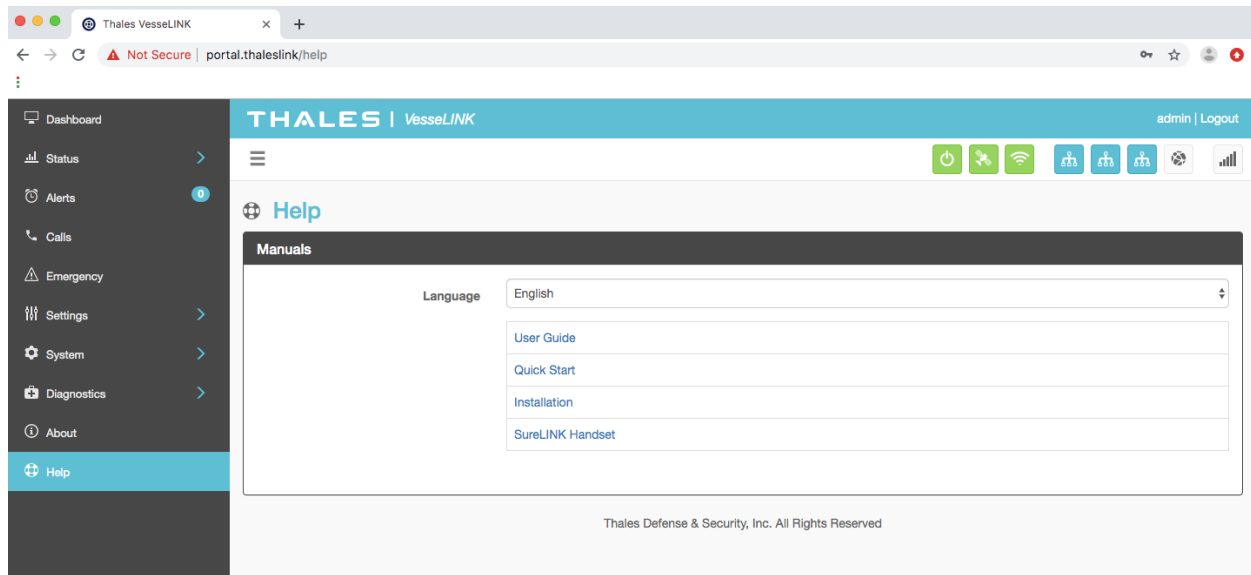
Figure 4-53 About Screen (Example)

## Help

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

This section includes:

- User Manual
- Quick Start Guide
- Installation Guide
- SureLINK Handset



*Figure 4-54 Help Screen (Example)*

## CHAPTER 5 FIRMWARE UPGRADE

On occasion it may be necessary to update VesseLINK™ 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 BDU 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 BDU 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.



### NOTE

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

## INSTALLING THE FIRMWARE ON VESSELINK™

### 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)

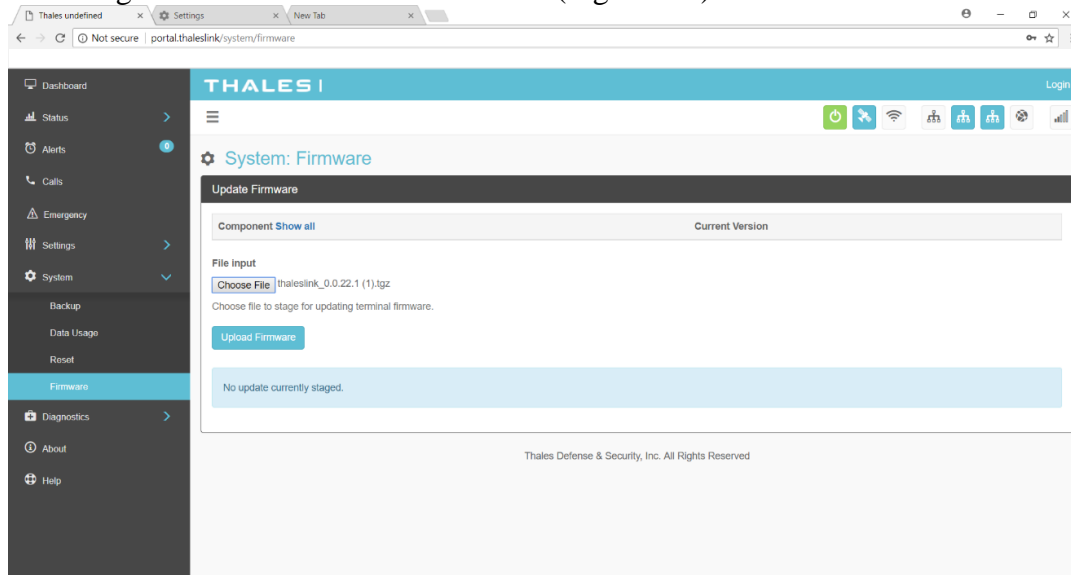
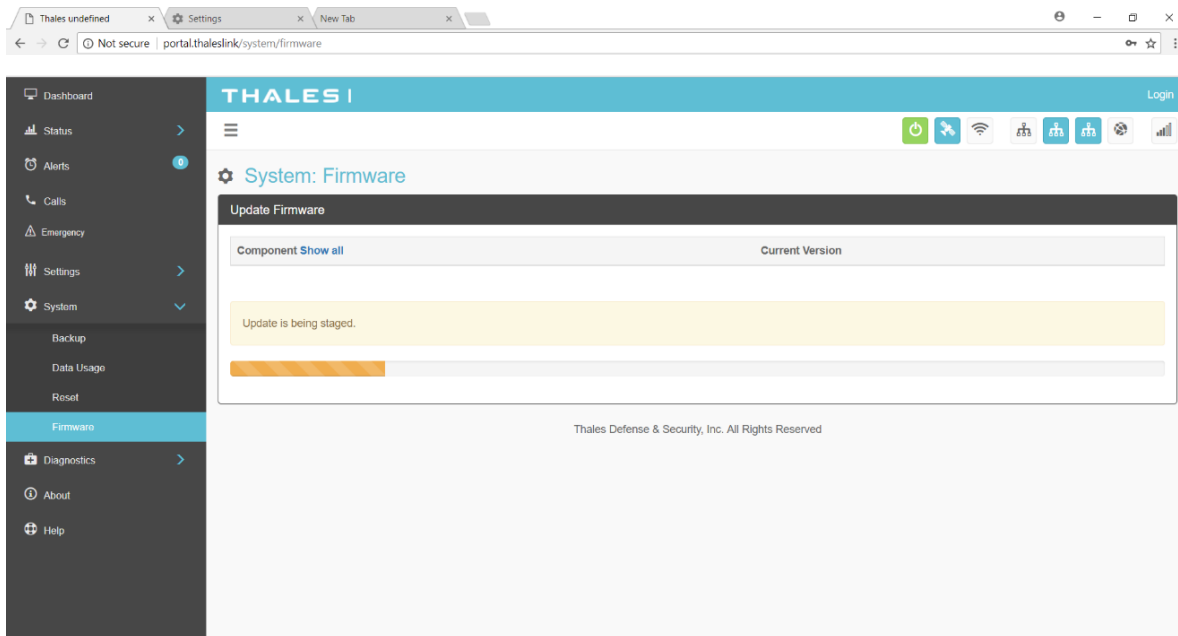


Figure 5-1 System → Firmware



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
  - 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 UPDATE button. This may take a few seconds as a progress bar moves across the page (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”.

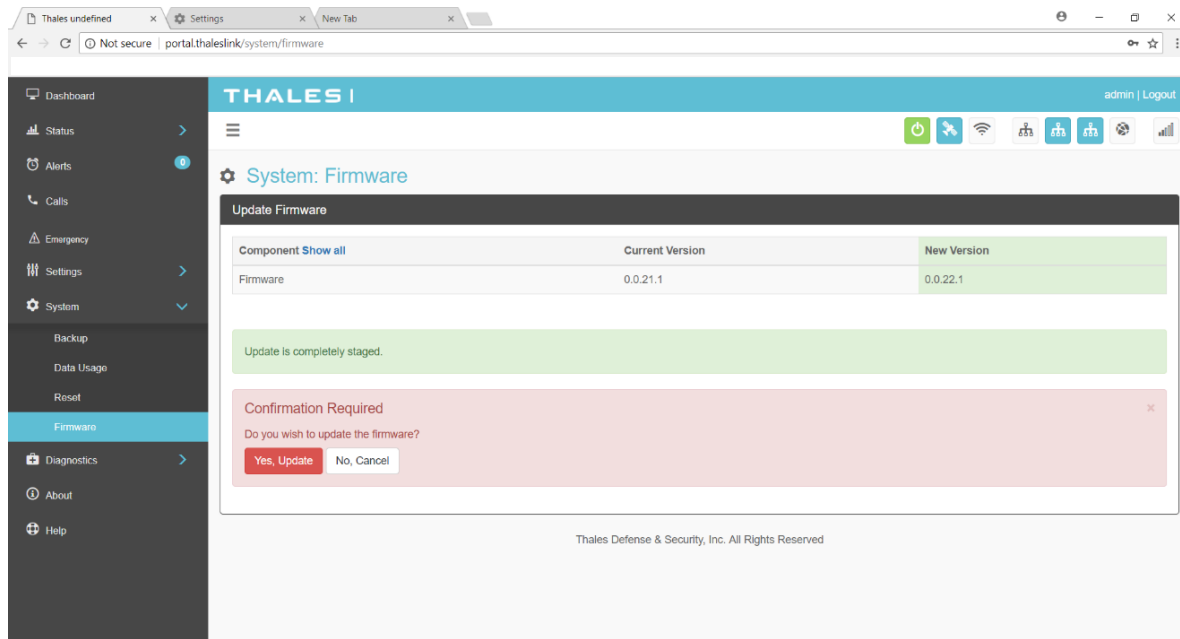


Figure 5-3 System → Firmware Update Confirm

- 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\***

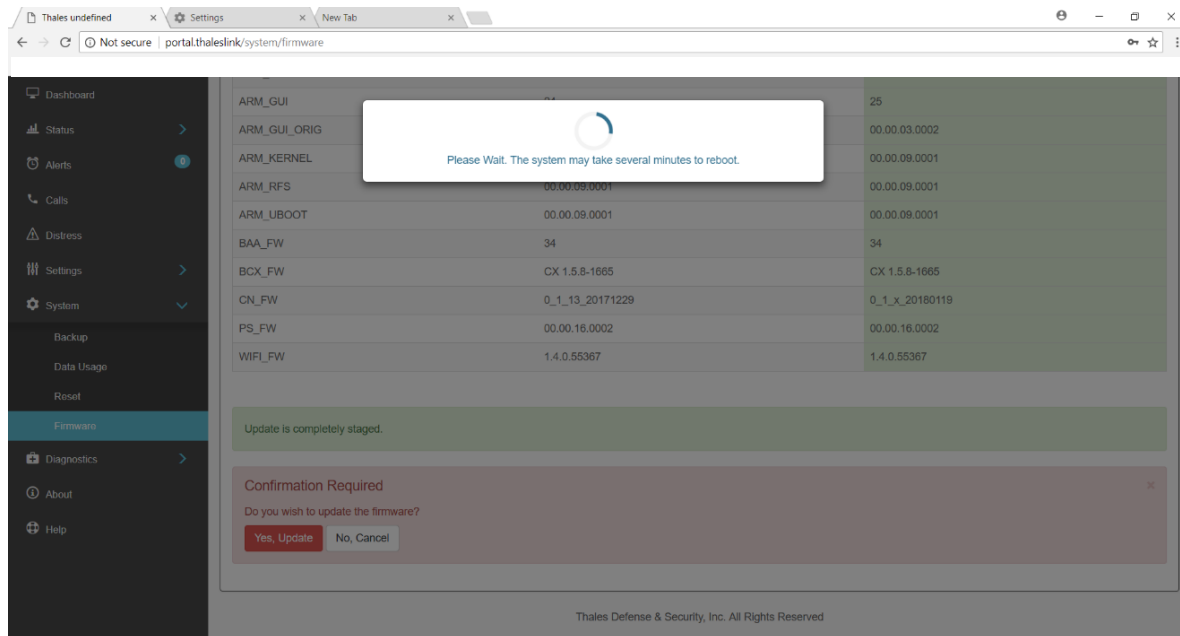
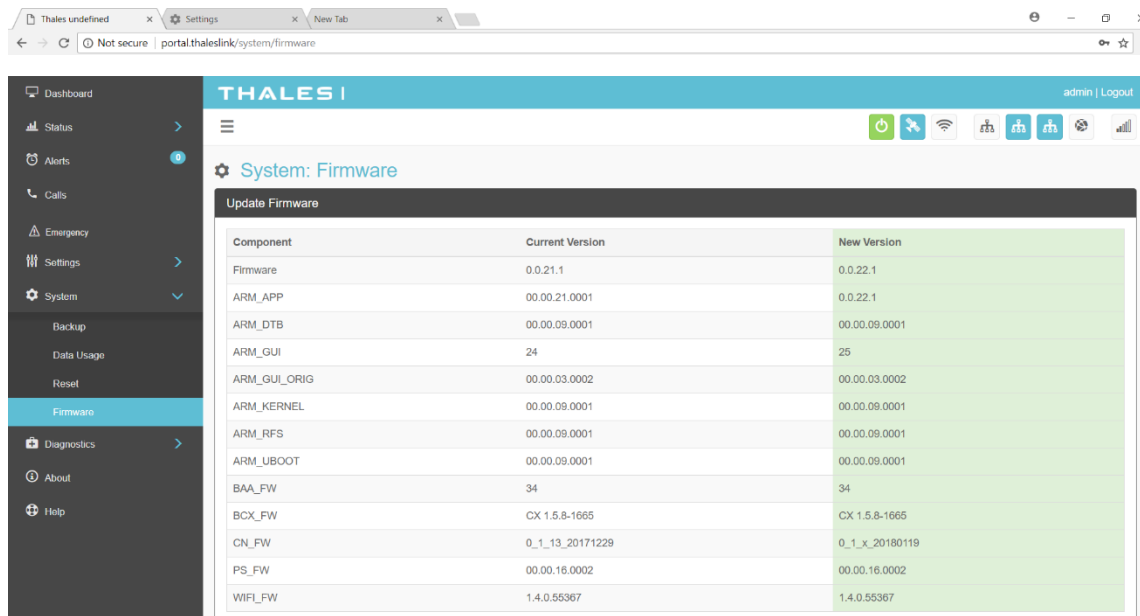


Figure 5-4 Firmware Update in Process

- Once completed and the system reboots, wait for all the Status LEDs 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 VesseLINK™) 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.)



Component	Current Version	New Version
Firmware	0.0.21.1	0.0.22.1
ARM_APP	00.00.21.0001	0.0.22.1
ARM_DTB	00.00.09.0001	00.00.09.0001
ARM_GUI	24	25
ARM_GUI_ORIG	00.00.03.0002	00.00.03.0002
ARM_KERNEL	00.00.09.0001	00.00.09.0001
ARM_RFS	00.00.09.0001	00.00.09.0001
ARM_UBOOT	00.00.09.0001	00.00.09.0001
BAA_FW	34	34
BCX_FW	CX 1.5.8-1665	CX 1.5.8-1665
CN_FW	0_1_13_20171229	0_1_x_20180119
PS_FW	00.00.16.0002	00.00.16.0002
WIFI_FW	1.4.0.55367	1.4.0.55367

*Figure 5-5 System → Firmware Update Completed*



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

## CHAPTER 6 MAINTENANCE

### GENERAL

This chapter provides operator maintenance instructions for the BDU and ADU. This includes, preventive maintenance and troubleshooting procedures.





### PREVENTIVE MAINTENANCE


#### Inspection and Cleaning

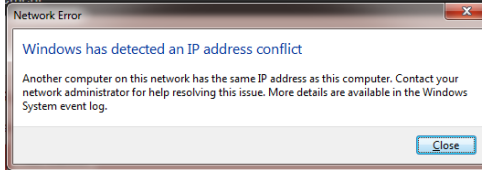
The equipment should be occasionally inspected for external damage, such as bent connectors and wear items, such as loose attaching hardware. The equipment should be cleaned periodically, particularly after exposure to salt water, sand, or mud. With the BDU turned off, use a slightly damp rag (water only) to clean the BDU and/or ADU. 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	<ul style="list-style-type: none"> <li>Flashing GREEN light indicates that it is acquiring the satellite. If it continues to flash for more than 5 minutes, check that the antenna has a clear view of the sky.</li> <li>Reboot BDU.</li> </ul>
 Satellite LED Flashing RED	<ul style="list-style-type: none"> <li>Critical Fault Detected. Open Management Portal <a href="http://portal.thaleslink">http://portal.thaleslink</a> (or <a href="https://portal.thaleslink">https://portal.thaleslink</a>) and check Alerts. Make any adjustments. (For example: check antenna connection, or GPS not acquired.)</li> <li>Turn unit off and on again. If same result, contact your service provider.</li> </ul>
 System LED Flashing Green	<ul style="list-style-type: none"> <li>Start-up in progress. Wait until unit has run diagnostics and completed start procedure. This may take more time than usual when acquiring satellites for the first time</li> <li>Switch power off and back on if the light does not turn solid green after 5 minutes.</li> </ul>
 System LED Flashing RED	<p>Fault Detected. Open Management Portal <a href="http://portal.thaleslink">http://portal.thaleslink</a> (or <a href="https://portal.thaleslink">https://portal.thaleslink</a>) and check for alerts. Make any adjustments. (For example: Common alerts include, but not limited to, are the SIM Card not installed, SIM Card not provisioned. Power-Up Test (POST) failure.)</p> <ul style="list-style-type: none"> <li>Turn unit off and on again. If same result, contact your service provider.</li> </ul>

PROBLEM	SOLUTION
 Wi-Fi LED	<p>OFF – Turn Wi-Fi ON using the Management Portal through a hardwired, PoE connection. ThalesLINK &gt; SETTINGS &gt; Wi-Fi</p> <p>Solid RED – Wi-Fi may need to be turned off and back on again from the Management Portal. If the LED does not turn to GREEN within a minute, reboot the BDU.</p> <p>Flashing GREEN – If this continues for more than a minute or two, check for NO OR WEAK Wi-Fi</p>
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.
Cannot connect to the Management Portal	<ul style="list-style-type: none"> <li>You may need to clear your browser cache.</li> <li>Ensure Terminal Unit is powered ON</li> <li>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 BDU 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</li> <li>Open web browser and type <a href="http://portal.thaleslink">http://portal.thaleslink</a> (or <a href="https://portal.thaleslink">https://portal.thaleslink</a>). Ensure network settings are correct on the connected device.</li> <li>Device's browser may be incompatible. Update or try different browser.</li> <li>You may need to reconnect via Ethernet or Wi-Fi to the BDU.</li> <li>Check to make sure the correct address is typed in <a href="http://portal.thaleslink">http://portal.thaleslink</a> (or <a href="https://portal.thaleslink">https://portal.thaleslink</a>)</li> <li>If system LED is flashing GREEN, wait until it turns solid GREEN, then try reconnecting to the portal.</li> </ul>

PROBLEM	SOLUTION
Cannot connect to Wi-Fi service	<ul style="list-style-type: none"> <li>• Check that the Wi-Fi antenna is attached and tightly screwed in.</li> <li>• Check that the BDU's Wi-Fi LED is solid GREEN.</li> <li>• Check to see if there's an available connection by checking the devices that are connected in Status → Current Devices page.</li> <li>• Only 3 simultaneous devices can connect to the Wi-Fi. Any additional connection attempts are blocked.</li> <li>• Remove one or more devices from the Wi-Fi and try again to connect.</li> <li>• Use the Wi-Fi Device Whitelist to limit access to specific wireless devices.</li> <li>• 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.</li> </ul>
Network Error	<p>If you receive a message similar to this, another user is attempting to use the same IP Address as your computer.</p> 
No or Weak Wi-Fi Signal	<ul style="list-style-type: none"> <li>• Connect Wi-Fi antenna and ensure it is secured tightly</li> <li>• If walls or metal obstructions are between the BDU and the Wi-Fi device, move closer to the BDU or move the BDU to a better location with less obstructions</li> <li>• Check to make sure Wi-Fi device is connected to the TBDU's Wi-Fi and verify that you are connected to the ThalesLINK.</li> <li>• Check the Management Portal to make sure the Wi-Fi device is registered as a user.</li> </ul>
VesseLINK is not obtaining a satellite signal (Satellite LED is red)	<ul style="list-style-type: none"> <li>• Check signal bars at the top of the Management Portal. If no bars are highlighted, the satellite is not being detected. Wait a few minutes to see if the signal strength improves as another satellite comes into view.</li> <li>• Check antenna connection at the BDU and antenna. Make sure no corrosion has occurred on the cable connections to the antenna and that the connectors are screwed in tightly.</li> <li>• Check antenna for a clear view of the sky with no obstructions. Relocate antenna if needed.</li> <li>• Check for interferers in the area that could be affecting the signal such as active radars, VSAT systems and other radio antennas. Turn those off and retest.</li> <li>• Move vehicle to a new location and retest if other interfering vehicles are in the area</li> <li>• Reboot BDU and check the Alerts.</li> <li>• Call Service Provider if the satellite connection is still not working.</li> </ul>

PROBLEM	SOLUTION
BDU does not Power-ON	<ul style="list-style-type: none"> <li>• Check BDU for Green lights, If green light is on Unit has Power</li> <li>• Push power button on front of BDU.</li> <li>• Check that the power source is providing 10-32V and is not current limited.</li> <li>• Check connection of the 10-32V DC cable has correct polarity.</li> <li>• Check to ensure Ignition line is connected to switched line or connected to Red (Positive line) for continuous operation.</li> <li>• Check that ignition or remote switch is turned on if ignition line is connected.</li> <li>• 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 BDU.</li> </ul>
BDU has power but accessories not working	<ul style="list-style-type: none"> <li>• Remove power from accessories and disconnect from BDU. Restart BDU using the power button or remove power from BDU for 10 seconds. After BDU has rebooted re-attach accessories. (Note: This applies to all accessories, EXCEPT the antenna. Do not disconnect the antenna while booting up the system.)</li> <li>• If PoE accessory not receiving power, make sure PoE is enabled for that port.</li> <li>• PoE is not available on WAN port. Any device on WAN port needs its own power source.</li> <li>• Check VoIP phone manuals for proper configuration. Each phone may have a different configuration method.</li> </ul>
BDU is not responding	<ul style="list-style-type: none"> <li>• Check LED status on BDU or on Management Portal. Make sure there are no RED LEDs. Check for Alerts in Management Portal by selecting the Alerts menu item</li> <li>• Reboot the system and recheck for any Alerts that may have been generated.</li> <li>• Call Service Provider if the BDU is still not responding.</li> <li>• As a last resort, use the manual reset button, located below Wi-Fi antenna port, using a straightened paper clip or similar sized article insert into port and push reset button.</li> </ul> <p><u>NOTE:</u> This is not recommended as a routine troubleshooting measure. All user data and debug information will be lost and factory defaults returned.</p>

## SYSTEM RESETS

In a rare situation where the VesseLINK™ 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

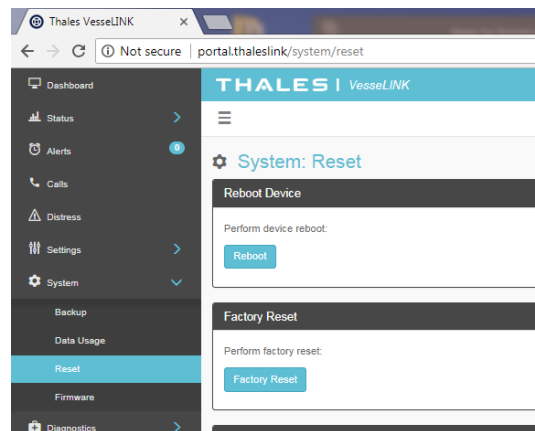
There are three (3) ways to power cycle the system:

- 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 BDU*

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



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

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

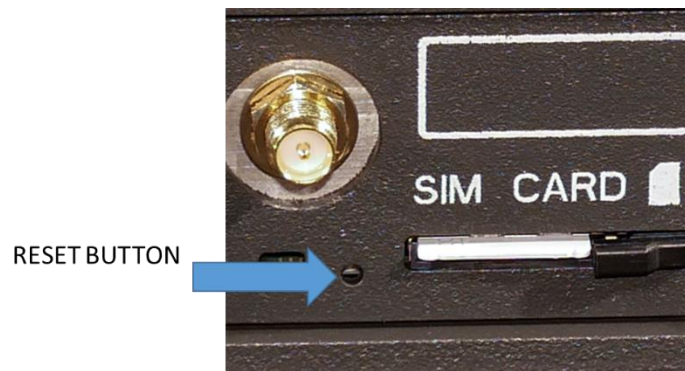


## Factory Reset

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



### 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 BDU 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.
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 terminal 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 BDU. Contact representative if problem persists for more than 4 hours.

Alert Name	Description	Level	Additional Information	Corrective Action
BCX_IBIT_FAILURE	The BCX has failed “Initiated Built In Self-Test” View Logs for details.	Fault		Open <a href="http://portal.theseslink">http://portal.theseslink</a> (or <a href="https://portal.theseslink">https://portal.theseslink</a> ) and review Self-Test logs. Restart the BDU. If problem persists, contact representative.
BCX_SIM	Modem failed to read SIM card	Warning		Remove, clean and re-insert SIM. Contact service provider if problem persists.
CN_OFF	Core Node is powered off, restart required	Critical	Core Node is noticed to be unexpectedly off.	Restart BDU. Contact representative if problem persists.
CN_REBOOT	Core Node Reboot has occurred, full system restart is required.	Critical	Core Node Module restarts while the system is up and running.	Restart BDU. Contact representative if problem persists.
MODEM_ACT	Modem returned an unknown error – cannot activate	Fault		Restart BDU. Contact representative if problem persists.
MUX_PLL_UNLOCKED	Antenna mux out-of-lock with the modem.	Critical	PLL failed to acquire	Restart BDU. Contact representative if problem persists.
PWR_IBIT_FAILURE	The power has failed “Initiated Built In Self-Test” View Logs for details.	Fault		Open <a href="http://portal.theseslink">http://portal.theseslink</a> (or <a href="https://portal.theseslink">https://portal.theseslink</a> ) 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 <a href="http://portal.theslink">http://portal.theslink</a> (or <a href="https://portal.theslink">https://portal.theslink</a> ) and review Self-Test Logs. Contact representative.
SIM_MISSING	SIM card not detected	Fault	SIM Card is physically missing	Insert or replace SIM card

## 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
	VesseLINK coverage	-12° to 90° elevation	-12° 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			
Description		Certus 200	Certus 350
ADU	Operating Temp	-40°C to +55°C	
	IP Rating	IP67	
BDU	Operating Temp	-30°C to +55°C	
	IP Rating	IP31	
Mechanical		Certus 200	Certus 350
ADU	Dimensions	5" D x 5.5" H (12.5 cm x 14 cm)	14.5" x 7.8" (36.8cm x 19.8cm)
	Weight	1 lb. (0.45 kg)	6.2 lbs. (2.8 kg)
BDU	Dimensions	12" L x 9" W x 3" H (30.5 cm x 23 cm x 7.6 cm)	
	Weight	7.5 lbs (3.4 kg)	
AC Power Brick	Length	6.6" (16.7cm)	
	Width	2.6" (6.7cm)	
	Height	1.4"(3.5cm)	
	Weight	1.37lbs (0.62 kg)	
	AC Cable Length	~6ft (1.8m)	
	DC Cable Length	~3.9ft (1.2m)	
RF Cables	25 meter	LMR-300FR or Similar w/TNCM-TNCM	
	50 meter (optional)	LMR-400FR or Similar w/TNCM-TNCM	

## 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 BDU 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 on, it will increase frequency of transmission to every 10 seconds.**

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

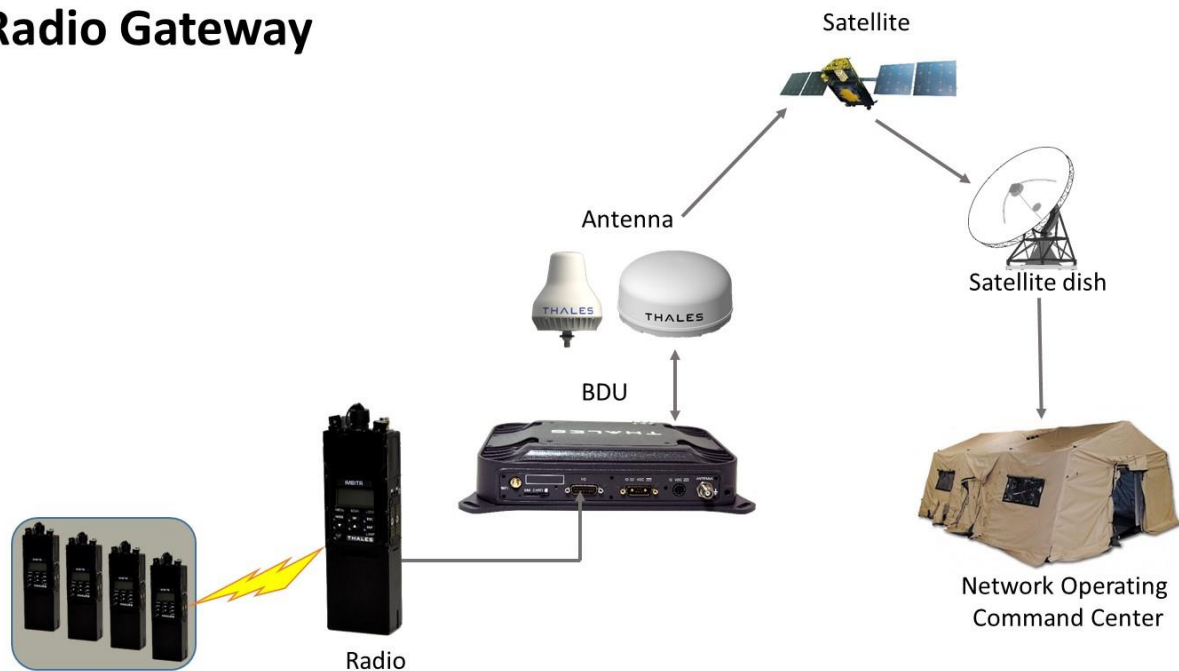
This security feature is for user protection. **The ONLY way to remove an active emergency message is to enter Management Portal under EMERGENCY TAB**

**Radio Gateway** → Advanced users can connect Land Mobile Radio I/O to send and receive voice and Push-To-Talk (PTT) calls over the VesseLINK™. 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 (Table 7-2) for creating the custom Radio Gateway cable. Refer to



2. Table 4- for settings related to the Radio Gateway.

## 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.

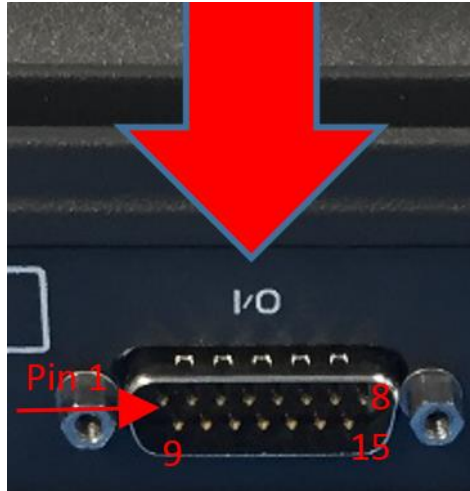


Figure 7-2 GPIO Connector Pin Detail

Table 7-2 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

## BDU 12V Connection Detail

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

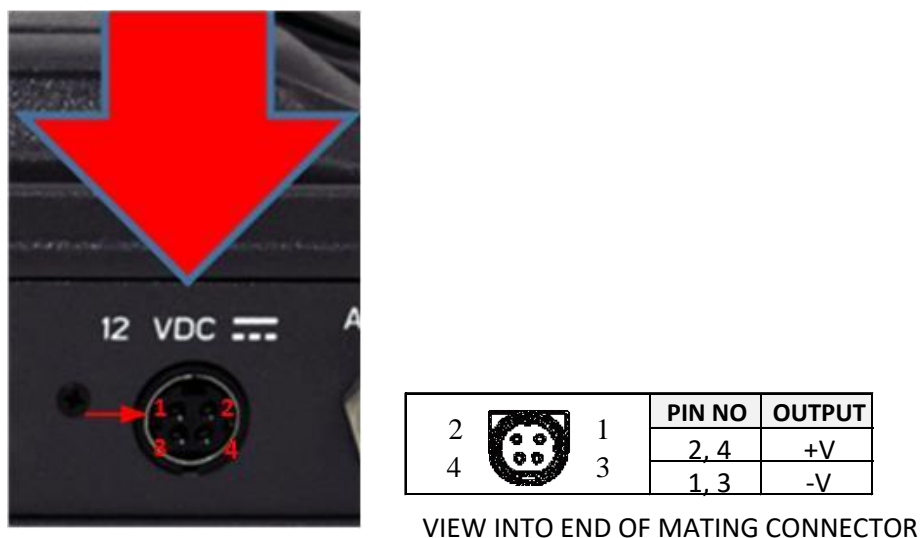


Figure 7-3 12V Input and Mating Connector Detail

## BDU 10-32VDC Connection Detail

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

A1 = V+ /10-32VDC

A2 =V- /GND

Pin 5 = Ignition

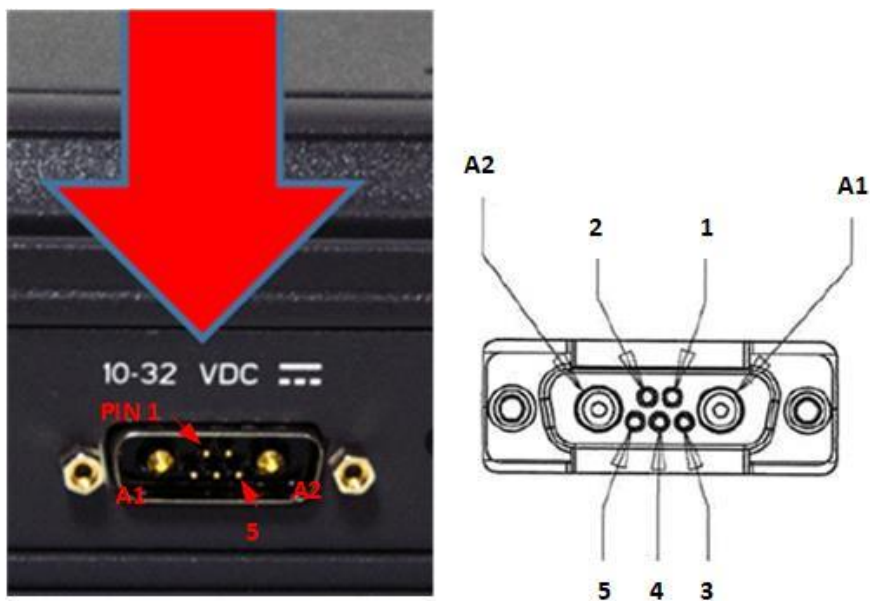


Figure 7-4 10-32 VDC and Mating Connector Detail

## CHAPTER 8 ACRONYMS / GLOSSARY

### ACRONYMS / GLOSSARY

*Table 8-1 List of Acronyms*

Acronym	Description
ADU	Above Deck Unit Antenna
API	Application Programming Interface
BAA	Broadband Active Antenna
BAE	Broadband Application Electronics
BCX	Broadband Core Transceiver
BDU	Below Deck Unit Terminal Unit
BIT	Built In Test
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
GRE	Generic Routing Encapsulation
HGA	High Gain Antenna
HRLP	High Speed Radio Link Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ICMP	Internet Control Message Protocol
ITU	International Telecommunications Union
LAN	Local Area Network
LED	Light Emitting Diode
LGA	Low Gain Antenna
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
PSTN	Public Switched Telephone Network
PTT	Two way radio term indicating the pressing of a button to initiate transmit before speaking
R/W	Read/Write

Acronym	Description
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
TU	Terminal Unit
UDP	User Datagram Protocol
UL/DL	Uplink/Downlink
VLAN	Virtual Local Area Network
VoIP	Voice of Internet Protocol
WAN	Wide Area Network
Wi-Fi	Wireless Network
WPA2-PSK	Wi-Fi Protected Access 2 – Pre-Shared Key

*Table 8-2 List of Definitions*

Acronym	Description	
API	Application Programming Interface	The Management Portal provides API to allow for the connection to the terminal remotely.
BAA	Broadband Active Antenna	The antenna and supporting electronics that interface an Iridium satellite terminal with the Iridium constellation
BAE	Broadband Application Electronics	Hardware and software platform resident in the BDU 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
DTMF	Dual Tone Multi-Frequency	Signals generated from phone keypad
EBB	Enhanced Broadband	EBB Mode is Iridium NEXT phase 1 EBBS (Enhanced Broadband Service)
ETSI	European Telecommunications Standards Institute	Organization that maintains standards for Information and Communications applicable to fixed and mobile radio platforms
GPIO	General Purpose Inputs/Outputs	General use pins
HGA	High Gain Antenna	External antenna that connects to the BDU 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

Acronym	Description	
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 BDU via a coaxial cable. The LGA supports the Certus <sup>SM</sup> 100 and Certus <sup>SM</sup> 200 capabilities
Management Portal		Management Portal: A web page served from the Terminal Unit that brings together the diverse status and configuration information of the LMC 350 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 BDU
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 involves multimedia elements such as video, voice, and chat
SV	Satellite Vehicle	Iridium Satellite
SMBus	System Management Bus	Two-wire bus for communications between devices such as a Terminal and a Smart Battery
TCP	Transmission Control Protocol	Core internet protocol that provides reliable delivery and error-checking
TU	Terminal Unit	Electronic equipment that contains the BCX and the BAE
UL/DL	Uplink/Downlink	To and from satellite communications

Acronym	Description	
UDP	User Datagram Protocol	Connectionless transmission model with minimum , no-handshaking protocol
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

### VESSELINK™ 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, VesseLINK™ Certus 350, List of Equipment*

Part Number			Description
VF350BM			Standard Kit, VesseLINK™ Certus 350**
Qty	Part Number	Description	
✓	1	1100789-501	Kit, Below Deck Unit (BDU), Mounting Hardware
✓	1	1100791-501	Kit, Antenna Maritime Mounting Hardware
✓	1	1600901-1	Above Deck Unit / Antenna, Certus 350
✓	1	3402131-1	Quick Start Guide (QSG) VesseLINK™
✓	1	3900011-1	Mounting Template, BDU
✓	1	3900014-1	Mounting Template, Antenna
✓	1	4102947-511	BDU, VesseLINK™
✓	1	84670-001	Power Supply, AC/DC 12V – 160W
✓	1	854024-001	Cable AC Power with USA Plug 6 ft.
✓	1	854025-001	Cable AC Power EURO Plug 6 ft.
✓	1	855023-082	Cable, Coaxial 25m LMR300 FR
✓	1	855026-010	Cable, RJ-45 Ethernet, 10 ft.
✓	1	85728-001	Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi

\*\* The VF350BM 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, VesseLINK™ Certus 350, List of Equipment

Part Number			Description
VF350BM-1			Base Kit, VesseLINK™ Certus 350
Qty	Part Number	Description	
✓	1	1600901-1	Above Deck Unit / Antenna, Certus 350
✓	1	3402131-1	Quick Start Guide (QSG) VesseLINK™
✓	1	3900011-1	Mounting Template, BDU
✓	1	3900014-1	Mounting Template, Antenna
✓	1	4102947-511	BDU, VesseLINK™
✓	1	85728-001	Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi

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

Part Number			Description
VF200BM-1			Base Kit, VesseLINK™ Certus 200
Qty	Part Number	Description	
✓	1	1600952-1	Above Deck Unit / Antenna, Certus 200
✓	1	3402131-1	Quick Start Guide (QSG) VesseLINK™
✓	1	3900011-1	Mounting Template, BDU
✓	1	4102947-521	BDU, VesseLINK™
✓	1	85728-001	Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi

Table 9-4 Available VesseLINK™ Accessories

Description	Part Number	Qty
19" Rack Mount Shelf Kit	1100796-501	1
Thales SureLINK IP Handset Kit	1100818-501	1
Kit, Below Deck Unit (BDU), Mounting Hardware	1100789-501	1
Kit, Antenna Maritime Mounting Hardware (Certus 350 only)	1100791-501	1
Mounting Template, BDU	3900011-1	1
Mounting Template, Antenna (Certus 350 only)	3900014-1	1
Power Supply, AC/DC 12V – 160W	84670-001	1
Cable AC Power with USA Plug Type B IEC 60320-C13 6 ft.	854024-001	1
Cable AC Power with Euro Plug Type E IEC 320-C14 6 ft.	854025-001	1
Cable AC Power with AUS Plug Type 1 IEC 320-C14 6 ft.	854026-001	1
Cable AC Power with UK Plug Type G IEC 320-C13 6 ft.	854027-001	1
Cable, Coaxial 25m LMR300 FR	855023-082	1
Cable, DC Power Harness	855024-003	1
Cable, RJ-45 Ethernet, 10 ft.	855026-010	1
Cable, Coaxial 50m LMR400 FR	855033-164	1
Wi-Fi Antenna, 2.4 GHz Dipole 2 dBi	85728-001	1
Antenna Basic L-Bracket Pole Mount Kit (Certus 200 only)	1100855-501	1
Antenna Premium Pole Top Mount Kit (Certus 200 only)	1100855-502	1
Antenna Premium L-Bracket Pole Mount Kit (Certus 200 only)	1100855-503	1
Antenna Mounting Plate, Small (Certus 350 only)	85736-001	1
Antenna Mounting Plate, Large (Certus 350 only)	85739-001	1

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

## INDEX

<b>A</b>	
About This Manual .....	1-1
Acronyms / Glossary.....	8-1
<b>C</b>	
Connector Details	
GPIO Connector .....	7-3
TU 10-32VDC Connector .....	7-6
TU 12V Connector .....	7-6
<b>F</b>	
Firmware Upgrade .....	5-1
<b>G</b>	
Getting Started .....	3-1
<b>I</b>	
Introduction	
Iridium Satellite Network .....	1-1
<b>M</b>	
Maintenance	
Alerts / Error Messages .....	6-8
Preventative Maintenance.....	6-1
System Resets .....	6-5
Troubleshooting.....	6-1
<b>S</b>	
System Overview	
Above Deck Antenna Unit .....	2-7
Below Deck Unit (BDU) .....	2-4
Description .....	2-1

## T

Technical Specifications .....	7-1
Thales Management Portal	
About .....	4-63
Alerts .....	4-13
Calls .....	4-14
Diagnostics .....	4-60
Emergency .....	4-15
Getting to know .....	4-2
Help .....	4-64
Main Dashboard .....	4-7
Menu Components .....	4-3
Settings .....	4-16
Status .....	4-9
System .....	4-55

## V

VesseLINK Kit Contents and Accessories .....	9-1
--	-----





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