



BETTER CONNECTIONS. EVERYWHERE. ALWAYS.

Iridium Certus MissionLink and VesseLink Terminals

Pivotel Quick Start Guide

Table of Contents


Using Data.....	2
Voice call	5
WiFi Connection.....	6
Firmware upgrade.....	7

Using Data

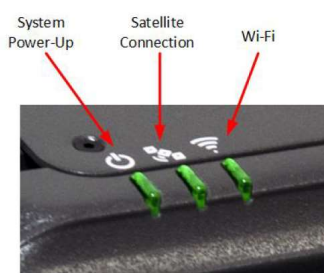
The data connection of the Certus terminal can be set to one of two modes.

1. Manual activation: requires the user to manually enable and disable a data session each time a data session is required. (This is the default setup for the terminal).
2. Automatic activation: a data session is activated upon power up or will attempt to activate a data session automatically after any period of network outage. The data session will remain continually active and cannot be manually disabled.

To activate a data session when in manual mode.

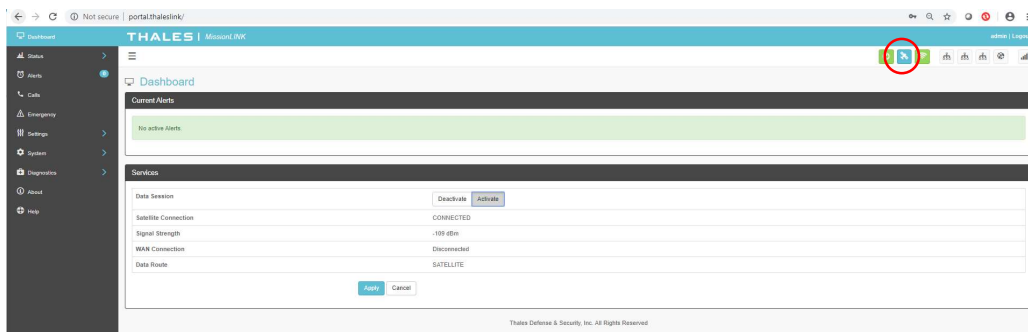
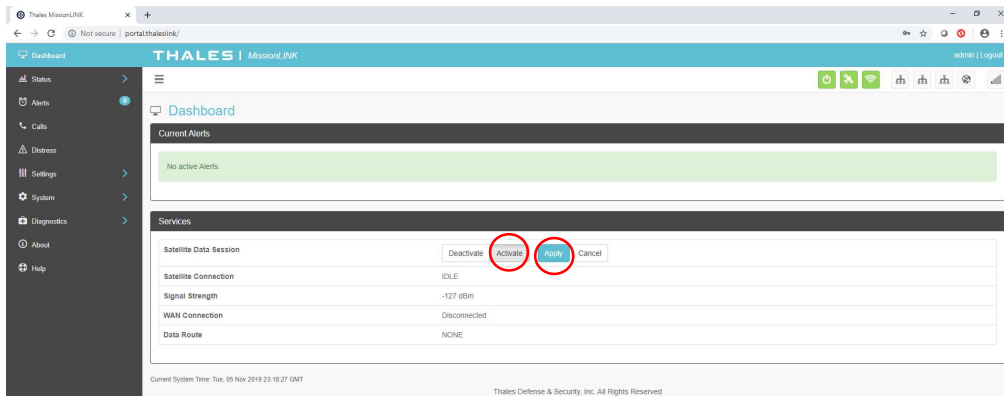
1. Connect your computer or smart phone to the terminal via Wi-Fi or Ethernet cable.
2. Open a web browser and enter <http://portal.thaleslink/> (do not type .com or any other extension). Default login details are as below:
Login name: admin
Login password: admin
3. Go to Dashboard using the left hand menu. On the top right corner, you will see the status of three LED  : System, Satellite and WiFi.
 - a. First LED (System) in solid green means terminal is functioning properly.
 - b. Second LED (Satellite) in solid green means satellite network is connected but data is not ready.
 - c. Third LED (WiFi) in solid green means WiFi is ready and OK.

You can also observe the same LED on the terminal. LED on Thales terminal: System, Satellite and WiFi.



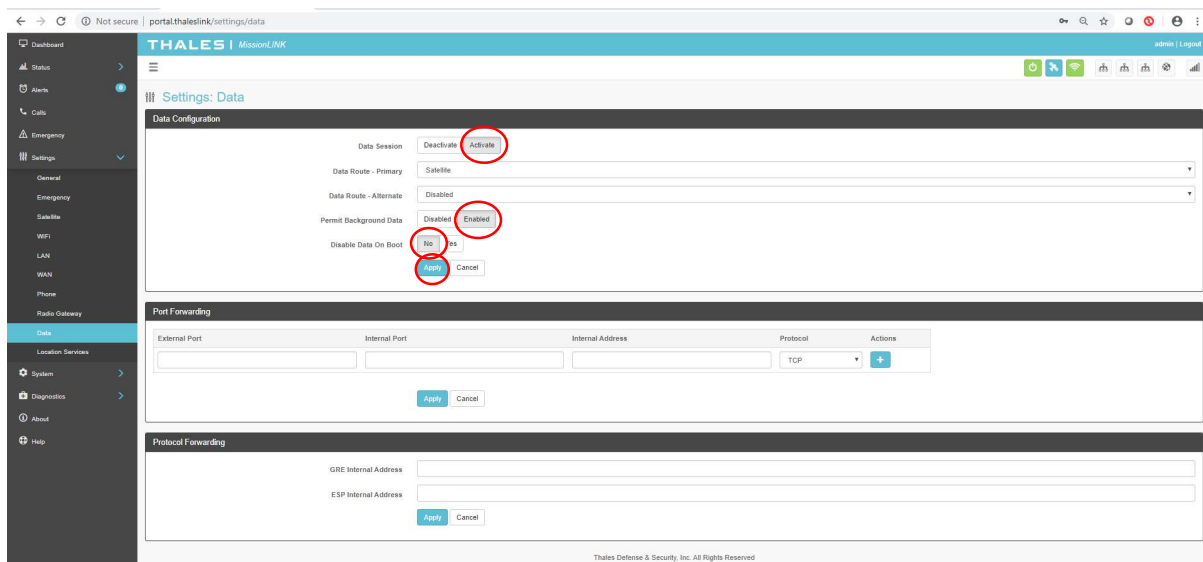
4. In the Services section, set the followings:

- a. Satellite Data Session: select 'Activate' (grey)
- b. Click 'Apply' to enable the data connection
- c. Observe the Satellite LED changes from solid green to solid blue. Data is now connected.



To configure automatic data enabled at start up.

1. Go to Settings → Data → Data Configuration.
2. Set the followings
 - a. Satellite Data Session: select 'Activate' (grey)
 - b. Data Route Primary: Select 'Satellite'
 - c. Permit Background Data: Select 'Enabled' (grey)
 - d. Disable Data on Boot: Select 'No' (grey)
3. Click 'Apply' to save.
4. Reboot the terminal for the new setting to take effect. Data should now be connected automatically after start up. You can open a website on a browser to test the connectivity.



Voice call

You can make and receive calls using a POTS phone. Connect your analogue / POTS phone to the RJ11 phone port. Just plug and play. No setup is required. The POTS phone is assigned with Pivotel service number by default.



Making a call from the Certus service

To make an outgoing call, dial 9 followed by <country code><area code><phone number>. For example, to call Australia, mobile number 0404123456, dial 961404123456 or to call California, USA number 415-768-0596, dial 914157680596.

Making a call to the Certus service

To make a call to the Pivotel Iridium Certus service, your caller just needs to dial the service number assigned to your service as they would to any other Australian mobile number.

WiFi Connection

WiFi Name: ThalesLINK

WiFi password: no password by default (Pivotal strongly encourage you to setup a password for the Wi-Fi to avoid unauthorised use)

You can go to the Thales management portal to setup the WiFi Password

1. Go to Settings → WiFi and set the followings:
 - a. SSID – enter a WiFi name if you would like to change from ‘ThalesLINK’.
 - b. Security Mode – select ‘WPA2’ (Open means no password is setup)
 - c. Security Key – enter your WiFi Password. Password must be at least eight characters (character, numbers, etc).
 - d. Click ‘Apply’ to save

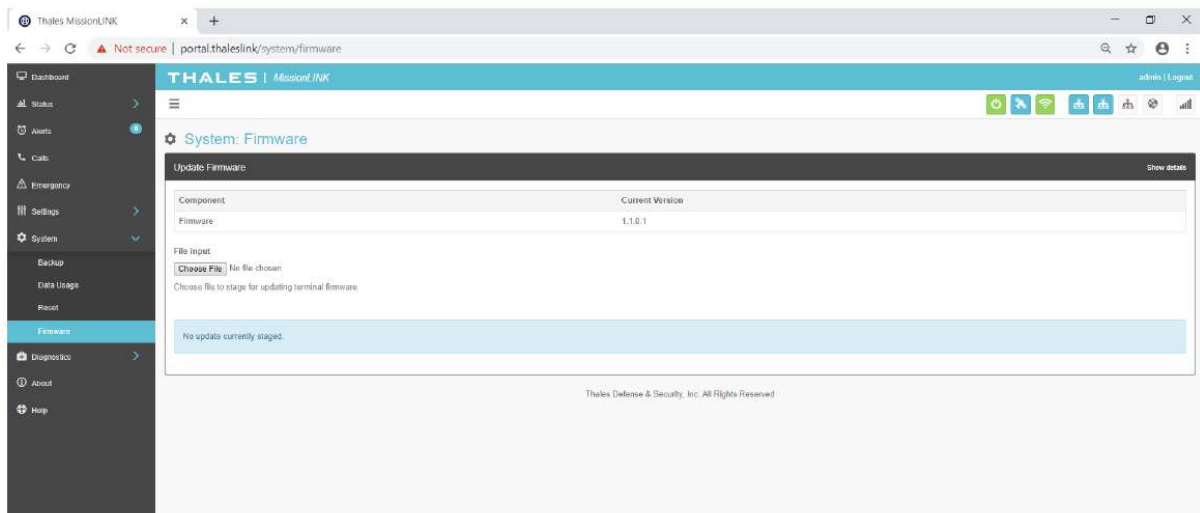
The screenshot shows the 'Settings: WiFi' page in the Thales MissionLINK management portal. The page is divided into two main sections: 'WiFi General' and 'WiFi Device Whitelist'. In the 'WiFi General' section, the 'Enable WiFi' toggle is set to 'Enabled'. The 'SSID' field contains 'ThalesLINK'. The 'Broadcast SSID' toggle is set to 'Disabled'. The 'WiFi Channel' is set to '1'. The 'Security Mode' dropdown menu is set to 'WPA2', and the 'Security Key' field is currently empty with a '(click to change)' prompt. The 'Apply' button is highlighted with a red circle. In the 'WiFi Device Whitelist' section, the 'Device Whitelist' toggle is set to 'Disabled'. Below this, there is a table with columns for 'Whitelist', 'MAC', 'Nickname', and 'Actions'. The 'Whitelist' column has an empty input field, and the 'Actions' column has a blue '+' button. At the bottom of the page, there is a footer that reads 'Thales Defense & Security, Inc. All Rights Reserved'.

Firmware upgrade

- The firmware upgrade is conducted in two phases:
 - Staging phase - transfer the new firmware file to the Missionlink terminal.
 - Upgrade phase- start the upgrade after the confirmation to upgrade the firmware. In this phase, the laptop is not required to be connected to MissionLink terminal.
- Suggest to connect your laptop to MissionLink using Ethernet cable to do the firmware upgrade if possible. If not, WiFi would work as well.
- The process may take up to 30min, typically 15min. Do not remove power during this firmware upgrade. The Power LED on the terminal will be blinking blue during firmware upgrade.
- Once firmware upgrade is completed, the terminal will automatically reboot.
- You must be login as admin to do the firmware upgrade.

1. Go to Systems – Firmware – Choose File: select the file – Click ‘Upload Firmware’ – Click ‘Yes, Update’.

2. After firmware upgrade is completed and terminal rebooted, go to the portal and check the firmware version for system and satellite modem.



The screenshots show the 'System: Firmware' update process in three stages:

- Stage 1:** The 'Update Firmware' section shows a 'File Input' area with a 'Choose File' button. A file named 'thaleslink_0.0.22.1 (1).tgz' has been selected. Below the file input is an 'Upload Firmware' button. A message states 'No update currently staged.'
- Stage 2:** The 'Update Firmware' section shows a yellow progress bar with the text 'Update is being staged.'
- Stage 3:** The 'Update Firmware' section shows a table with the following data:

Component	Show all	Current Version	New Version
Firmware		0.0.21.1	0.0.22.1

 Below the table, a green message states 'Update is completely staged.' A red 'Confirmation Required' dialog box is displayed with the text 'Do you wish to update the firmware?' and two buttons: 'Yes, Update' and 'No, Cancel'.

