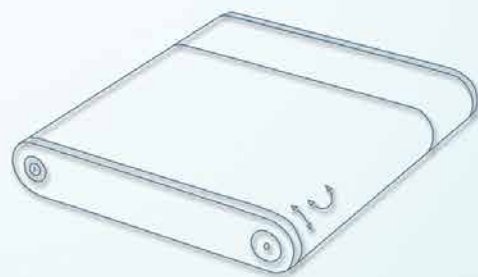




iSaviTM
Model: SH-100
User Guide
Version 5.0



SAFETY INSTRUCTIONS	01
COPYRIGHT	03
WARRANTY	03
TRADEMARKS	03
REGULATORY INFORMATION	04
1 INTRODUCTION	06
Key features	06
Configuration interface	06
System requirements	06
2 GETTING STARTED	07
Connect to the network	10
Method 1: LED Visual Pointing Mode	10
Magnetometer interference	11
Method 2: Audio Assisted Pointing Mode	12
Method 3: IsatHub Control app	13
Access data and calls	14
Power down and remove battery	16
3 NAVIGATING THE WEB CONSOLE	17
Menu overview	17
Terminal status	17
Data	18
Data profile settings	18
BGAN Streaming	20
Firewall protection settings	21
Access rights setting according to MAC address	27
Data settings	28
Telephony	29
SIP settings	29
SMS	29
Compose new SMS	29
View received SMS	30
View sent SMS	30
View draft SMS	31

Settings	31
Create account for Web Console access	31
Change SSID and Wi-Fi password	32
Configure security settings	34
Terminal settings	35
Upgrade firmware	35
Antenna pointing LED configuration	36
Terminal Information and log files	37
Select language	37
Technical support	37
4 WEB CONSOLE IN SAFE MODE	
Enable Safe Mode	38
Menu overview	38
Upgrade firmware	39
Factory reset of Safe Mode	40
Terminal Information and log files	40
Calibrate the magnetometer	41
Access Safe Mode through Micro USB Connection	45
Install Micro USB driver for Windows XP/Windows 7	45
Install Micro USB driver for Windows 8	46
Install Micro USB driver for MAC OS X	49
5 METHODS OF DATA OPTIMISATION	
Data access and cost management	52
Method 1: Use IsatHub Control app	52
Method 2: Use iSavi firewall	53
Method 3: Use smart devices settings	54
Method 4: Computer settings	54
Method 5: Use network support	55
6 TROUBLESHOOTING AND FAQ	56
7 CARE AND MAINTENANCE	62
Appendix A: ANTENNA POINTING LED STATUS TABLE	63
Appendix B: TECHNICAL SPECIFICATIONS	67
Appendix C: ISATHUB COVERAGE MAP	69

SAFETY INSTRUCTIONS

For safety and protection, please read the user guide before using the Satellite Terminal iSavi™ Model: SH-100. In particular, do read this safety section carefully. Keep this safety information where you can refer to it, if necessary.

The following general safety precautions must be observed during all phases of operation, service and repair of this equipment. Failure to comply with these precautions or with specific warnings elsewhere in this user guide violates safety standards of design, manufacture and intended use of the equipment.

Addvalue Innovation Pte Ltd assumes no liability for customer's failure to comply with these requirements.

HAZARD SYMBOLS

Your iSavi™ terminal can generate a significant amount of heat depending on the system activities such as continuous transmission over a period of time and the underside surface will be hot.

Note: Reduce the risk of heat related injury by adhering to the following:

1. Handle with caution when touching the underside surface of the terminal, especially when in use or just after powering down.
2. Wait for the terminal to cool after powering down before stowing the device in an unventilated manner.
3. Do not leave children unattended within reach of the terminal.

Votre récepteur/terminal "iSavi"™ peut générer une grande quantité de chaleur selon les activités du système, telles que la transmission continue pour une longue période, et la surface inférieure sera chaud.

Veuillez noter qu'on peut diminuer le risque d'une blessure causée par la chaleur en vous conformant aux directives suivantes:

1. Manipuler avec précaution lorsqu'on touche la surface inférieure du récepteur/terminal, en particulier au moment de l'utilisation ou juste après avoir éteint le récepteur/terminal.
2. Attendre jusqu'à le récepteur/terminal se soit refroidi après l'avoir éteint, avant l'entreposage dans un espace non ventilé.
3. Ne laissez pas les enfants sans surveillance à portée du récepteur/terminal.



ANTENNA RADIATION WARNING

During operation, iSavi™ radiates radio frequency energy within the safe MPE (Maximum Permissible Exposure) level.

However, it is highly recommended that for safety reasons, keep a distance of 1 metre or more from iSavi™.



SERVICE

Users should not attempt to access the interior of the transceiver. Only qualified personnel authorized by its manufacturer may service the device. Failure to comply with this rule will result in the warranty being void.

BATTERY SAFETY

Use only Addvalue-supplied or approved AC adapters with the terminal and for recharging the batteries. The use of batteries that are not Addvalue-supplied or approved may pose increased safety risks.

Do not dispose of batteries in a fire, as they may explode.

Batteries may burn or explode if damaged.

Do not dismantle, open, bend or cut cells or batteries.

Do not attempt to modify or remanufacture the battery.

Do not immerse or expose the battery to water or other liquids.

In the event of a battery leak, avoid the contents coming into contact with the skin or the eyes. If this happen, flush the affected areas with water and seek medical help as appropriate.

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

ATTENTION

IL Y A DANGER D'EXPLOSION S'IL Y A REMPLACEMENT INCORRECT DE LA BATTERIE, REMPLACER UNIQUEMENT AVEC UNE BATTERIE DU MEME TYPE OU D'UN TYPE ÉQUIVALENT RECOMMANDÉ PAR LE CONSTRUCTEUR.

METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS DU FABRICANT.

COPYRIGHT

© Copyright 2017 Addvalue Innovation Pte Ltd.

All rights reserved. This publication and its contents are proprietary to Addvalue Innovation Pte Ltd. No part of this publication may be reproduced in any form or by any means without the written permission of Addvalue Innovation Pte Ltd., 8, Tai Seng Link, Level 5 (Wing 2), Singapore 534158.

WARRANTY

Addvalue Innovation Pte Ltd has made every effort to ensure the correctness and completeness of the material in this document. Addvalue Innovation Pte Ltd shall not be liable for errors contained herein. The information in this document is subjected to changes without prior notice. Addvalue Innovation Pte Ltd makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

TRADEMARKS

All trademarks, marks, names, or product names referenced in this publication are the property of their respective owners, and Addvalue Innovation Pte Ltd neither endorses nor otherwise sponsors any such products or services referred to herein.

Wideye, the Wideye logo, iSavi and iSavi logo are either trademarks or registered trademarks of Addvalue Innovation Pte Ltd and/or its affiliates in Singapore and/or other countries.

Microsoft, Windows and Internet Explorer are registered trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Inmarsat is a trademark of The International Mobile Satellite Organisation and is licensed exclusively to Inmarsat. The Inmarsat logo, IsatHub and the IsatHub logo are trademarks of Inmarsat. Inmarsat, the Inmarsat logo, IsatHub and the IsatHub logo are used by Addvalue Innovation Pte Ltd under licence from Inmarsat.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

Android and Google Chrome are either trademarks or registered trademarks of Google Inc.

Macintosh, Mac OS, iPhone, iPad and Safari are trademarks or registered trademarks of Apple Inc., registered in the U.S. and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Firefox is a registered trademark of Mozilla Foundation.

All other company and product names may be the registered trademarks or trademarks of their respective owners.

iSavi™ Model: SH-100 User's Guide [APRIL 2017]

This user manual is prepared based on Firmware Version R02.0.0

REGULATORY INFORMATION



Federal Communication Commission Notice

FCC Identifier: **QO4-ISAVISH100**

USE CONDITIONS:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference, and this device must accept any interference received, including interference that may cause undesired operation.

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 radiates 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 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.

IMPORTANT NOTE: EXPOSURE TO RADIO FREQUENCY RADIATION

This Device complies with FCC & IC radiation exposure limits set forth for an uncontrolled environment. The Antenna used for this transmitter must be installed to provide a separation distance of at least 1 metre from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC CAUTION:

Any Changes or modifications not expressly approved by the manufacturer could void the user's authority, which is granted by FCC, to operate this Satellite Terminal, iSavi™ Model: SH-100.

Industry Canada Statement:

IC Identifier: **5023B-SH100ISAVI**

This device complies with Industry Canada license-exempt RSS-170 and RSS-GEN210 standard(s). Operations 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.

IMPORTANT NOTE: Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This antenna used for this transmitter must be installed to provide a separation distance of at least 1 metre from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

NOTE IMPORTANTE: l'exposition aux radiations

Cet appareil est conforme aux limites d'exposition aux rayonnements définies pour un environnement non contrôlé. Cette antenne utilisée pour ce transmetteur doit être installée pour fournir une distance de séparation d'au moins 100cm de toutes les personnes et ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou émetteur.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a built-in patch and maximum 8dBi gain (or lesser) 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 8dBi 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.

Declaration of Conformity:

Addvalue Innovation Pte Ltd., 8, Tai Seng Link, Level 5 (Wing 2), Singapore 534158 declares under our sole responsibility that the Product, brand name as Wideye and model: SH-100 Satellite Terminal, iSavi™ to which this declaration relates, is in conformity with the following standards and/or other normative documents:

ETSI EN 301 489-1, -17, -19, -20, ETSI EN 301 681, ETSI EN 300 328, EN 50385, EN 62311, ITU-R M.1480, IEC 60950-1 and EN 60950-1.

We hereby declare that all essential radio test suites have been carried out and that the above named product is in conformity to all the essential requirements of Directive 1999/5/EC.

The Conformity Assessment procedure referred to Article 10 and detailed in Annex [III] or [IV] of Directive 1999/5/EC has been followed with involvement of the following notified body(ies):

TIMCO ENGINEERING, INC., P.O BOX 370, NEW BERRY, FLORIDA 32669, U.S.A.

Identification mark: 1177 (Notified Body number)

CE 1177 !

The technical documentation relevant to the above equipment is held at:

- Addvalue Innovation Pte Ltd., 8, Tai Seng Link, Level 5 (Wing 2), Singapore 534158.
- Signed by
Mr. Tan Khai Pang (Chief Technology Officer, July 17, 2014) and
Mr. Prabakar Kuttaniseeri (Manager-Quality Management, July 17, 2014).

01 INTRODUCTION

iSavi™ satellite terminal is specially designed to be compact and easy to use with a standby battery lifespan that is comparable to laptops and smart phones. Together with a corresponding service package from Inmarsat, iSavi™ can meet the data and voice communications needs for the modern global business traveller, NGO field workers and many more types of user.

KEY FEATURES

- Built-in 802.11 b/g/n access point with 30 metre range (with built in Wi-Fi antenna)
- Data connectivity using Wi-Fi
- Voice connectivity using VoIP over Wi-Fi
- iSavi™ terminal management via web console or smart phone and tablet Control app
- Detachable rechargeable battery module with built-in charging circuit
- Single unit with integrated antenna (all-in-one)
- Easy antenna pointing (with audio tone and LED feedback)
- Lightweight, robust, reliable
- IP65 Compliant (dust tight and protected against water jets)

CONFIGURATION INTERFACES

You can configure the iSavi™ terminal via three different interfaces:

- Web Console (through web browser)
- Smart phone and tablet Control app*
- Voice app* (VoIP configuration for voice calls)

*Supplied separately- Search for IsatHub on your iOS or Android device (iOS App Store or Google Play).

SYSTEM REQUIREMENTS

Network Requirements

- IEEE 802.11b/g/n wireless clients
- Inmarsat IsatHub/BGAN Micro-SIM card

Browser based Web Console Requirements

Smart devices or personal computer with the following operating systems:

- iOS or Android™ ,
- Windows®, Macintosh®, or Linux-based operating system

Recommended Browsers:

- Google Chrome™
- Safari®
- Firefox®
- Internet Explorer®

Users have to ensure they have the latest version of Java™ installed where necessary. Visit www.java.com to download the latest version.

IsatHub Control app and Voice app Requirements

Smart phone or tablet:

iOS 6 or higher (minimum requirement: iPhone 4 / iPad 2)
Android 4.1 or higher

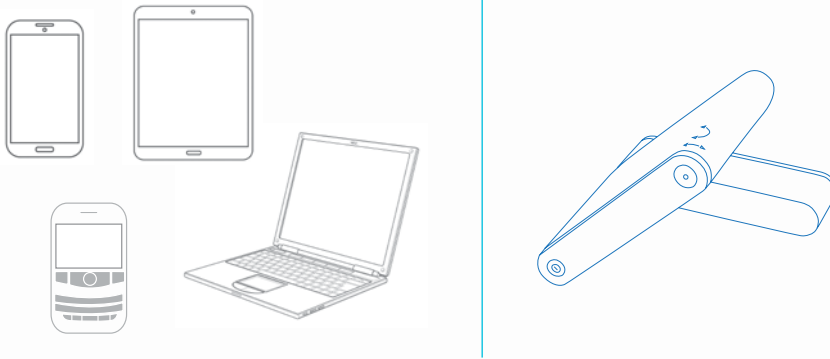
02 GETTING STARTED

WELCOME

Congratulations on purchasing Addvalue's Wideye™ iSavi™ satellite terminal.

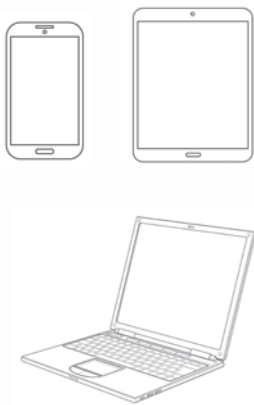
SHARED ACCESS TO DATA CONNECTIVITY

Devices connected to your iSavi™ satellite terminal over Wi-Fi can access data and telephone calls.



CONTROL SHARED ACCESS

The features of iSavi™ terminal can be conveniently controlled remotely.



Use a tablet or smart phone to share and control data access*.



For control of your iSavi™: IsatHub Control app
For satellite calls: IsatHub Voice app

DOWNLOAD NOW

Apps are available on App Store & Google Play for iOS & Android.

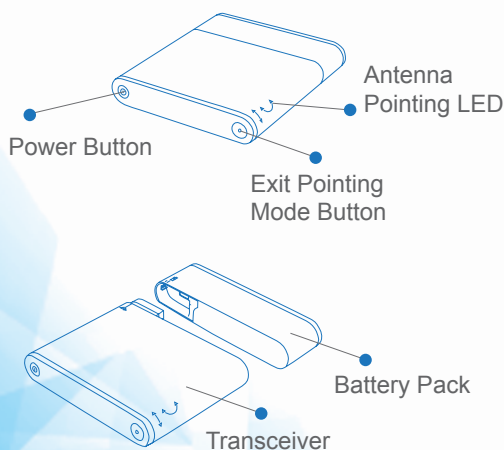
Alternatively use any web browser (<http://iSavi> or <http://192.168.1.35>) to control your iSavi™ satellite terminal.

* Apps are supplied by Inmarsat

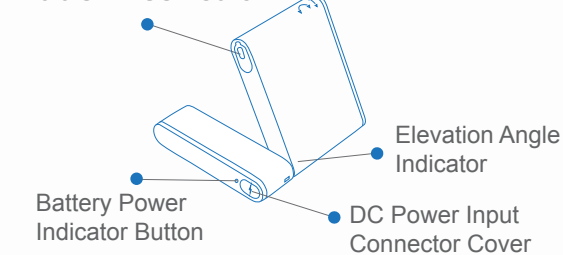
Note:

Downloading applications using Isathub services will incur satellite airtime charges.

QUICK REFERENCE



Micro SIM / USB Cover



Other contents in the box



Charger
& Adapters



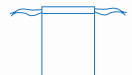
Micro USB
Cable



USB Drive
(User Guide)



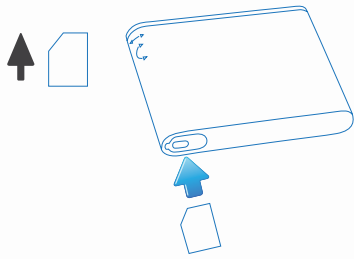
Quick Start
Guide



My iSavi™
Bag

Note:
The antenna is embedded inside the transceiver.

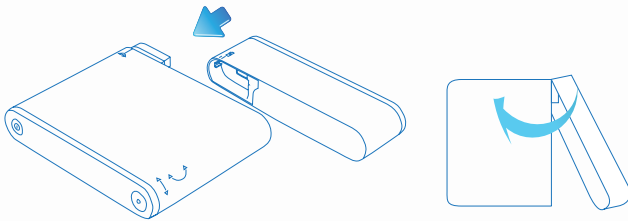
Insert the Micro-SIM card with its gold-contacts facing down.



Note:

Ensure iSavi™ is switched OFF before removing or installing the SIM card.

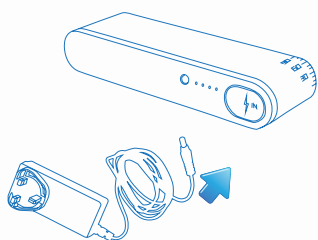
ATTACH BATTERY



Attach the battery gently in the direction as shown.



Use a finger to press the latch until you heard a 'click' sound. Ensure that the transceiver is properly attached to the terminal.



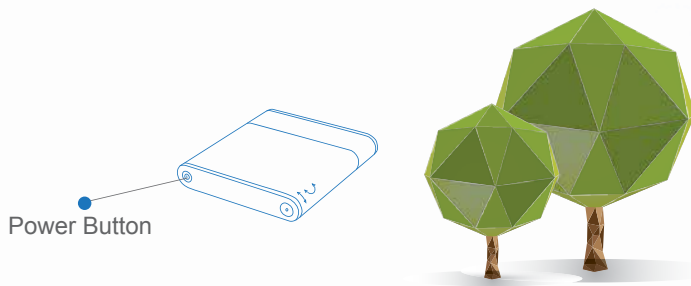
- ● ● ● 76% - 100% Capacity
- ● ● ○ 51% - 75% Capacity
- ● ○ ○ 26% - 50% Capacity
- ○ ○ ○ 1% - 25% Capacity

Note:

The charging time will be longer when iSavi™ is switched ON

Insert charger lead and then plug the adapter into a power source.
iSavi™ should be charged 8 hours before first use.

Charging will cease automatically once the battery is fully charged. Battery LEDs stop flashing.
You can check the battery level by pressing the 'Battery Power Indicator Button'.



After charging, place iSavi™ outside at a position with an unobstructed view of the sky.

Press and hold Power Button for 5 seconds to turn On iSavi™.

Leave it for at least 1 minute so that the terminal is powered up properly.

Refer to page 63, Appendix A: Antenna Pointing LED Status Table for the status of iSavi™.

To connect iSavi™ to the satellite network, you need to acquire a Global Positioning System (GPS).

Note:

The GPS location information is required for the iSavi™ to assist you in pointing It correctly to the satellite.

iSavi™ TERMINAL CONTROL

Your iSavi™ can be configured in 2 ways:

- IsatHub Control app:

You use this application to configure the terminal settings, including monitor and manage the data usage. It has fewer configurations option compare to the Web Console.

The app for smart phones and tablets are available from iOS App Store or Google Play for iOS or Android devices respectively.

- Web console:

Any browser provides access to configure and operate the terminal.

Refer to page 17, Navigating the web console.

CONNECT TO THE NETWORK

Make sure you place your iSavi™ in the open air, with an unobstructed view of the sky. Next, you point iSavi™ towards the satellite in the correct direction for connection.

Press and hold the Power button for five seconds to turn it On.

It takes around one to two minutes for iSavi™ to power up and enter antenna pointing mode.

There are three methods for antenna pointing:

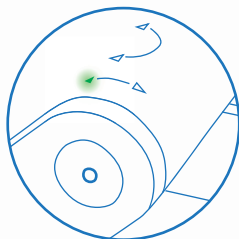
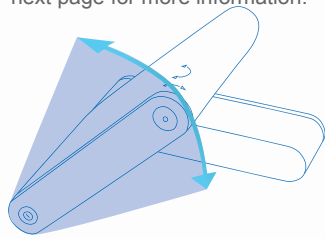
- LED visual pointing mode
- Audio assisted pointing mode
- IsatHub Control app

METHOD 1: LED VISUAL POINTING MODE

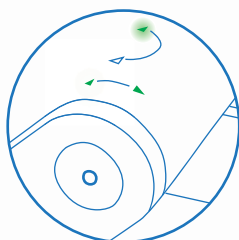
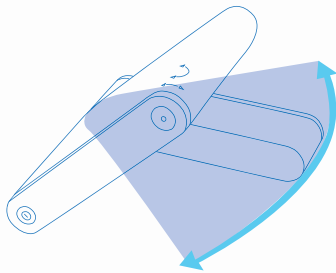
You can point iSavi™ terminal to the satellite network by using the Antenna Pointing LEDs.

Note:

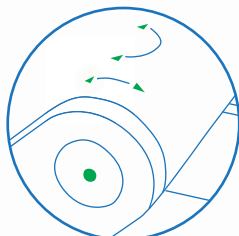
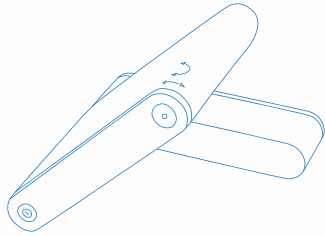
By default, the antenna pointing is in LED visual pointing mode. In some cases, you might encounter magnetic interference. Refer to the next page for more information.



Tilt iSavi™ up or down in the direction of the flashing green light until both 'up' and 'down' LEDs display in solid green.



Turn iSavi™ left or right in the direction of the flashing green light until both 'left' and 'right' LEDs display in solid green.



When all four tilt & turn LEDs are solid green, press the flashing 'Exit Pointing Mode' button. iSavi™ is now connected to the network.

Note:

Once the network is available, all four antenna pointing LEDs will be turned off after one minute.

The LEDs of 'Power' button and 'Exit Pointing Mode' button may sometimes be hard to see under bright sunlight.

Use the signal strength indicator in the Control app or web console in the bright environments.

If LEDs display any other pattern of illumination, please refer to Appendix A: Antenna Pointing LED Status Table on page 63 to understand the status of the iSavi™.



During operation, the iSavi radiates radio frequency energy within the safe MPE (Maximum Permissible Exposure) level.

However, it is highly recommended that for safety reasons, keep a distance of 1 metre or more from the iSavi™ when use.

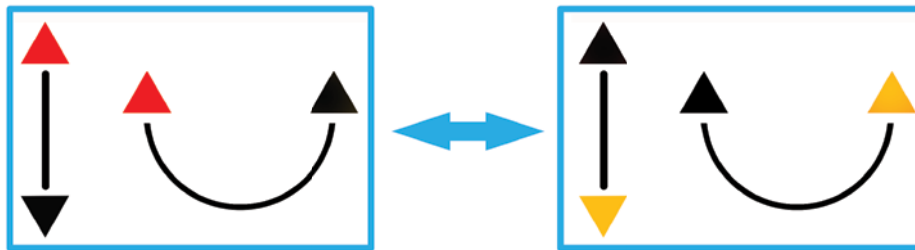


Handle with caution when touching the underside surface of the terminal, especially when in use or just after powering down.

Magnetometer interference

Occasionally, if your iSavi™ is in close proximity to any ferrous objects, the sensors will have difficulty determining its correct orientation.

When this happens, the LEDs will flash in the following sequence while the magnetic interference message will appear on your IsatHub Control app:



The following steps should resolve the issue.

Step 1: Move iSavi™ to a new location. Ensure the terminal is situated away from other electronic devices, metal objects and appliances that generate RF noise.

Step 2: Press the 'Exit Pointing Mode' Button once to exit from this state and repeat the steps of the LED Visual Pointing Mode procedure. The above LEDs status will appear again if the new location is still having magnetic interference. Repeat step 2 until the LEDs status indicates the LED Visual Pointing Mode.

If this does not solve the problem, please try **Method 2: Audio Assisted Pointing Mode** on next page.

Note:

You may need to perform a Magnetometer Calibration to obtain a better accuracy from the LED Visual Pointing. For details, please refer to page 41.

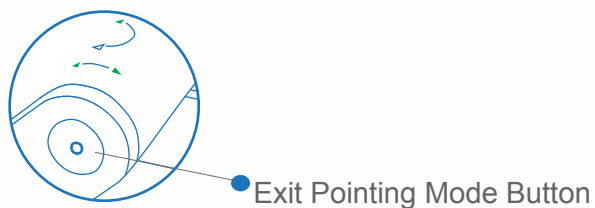
Magnetic Interference does not affect the basic operation of iSavi™.

METHOD 2: AUDIO ASSISTED POINTING MODE

You can point iSavi™ terminal to the satellite network by using the built-in buzzer.

STEP 1

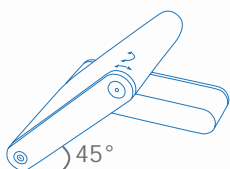
To switch into audio assisted pointing mode, press and hold the 'Exit Pointing Mode Button' for 5 seconds when your iSavi™ is in LED visual pointing mode .



All 4 LEDs will be flashing green when the audio assisted pointing mode is activated.
The beeping sound indicates the signal strength.
The frequency of the beeping will become higher when the signal is stronger.

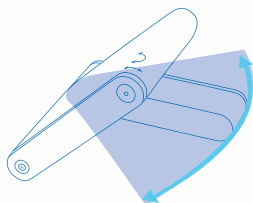
STEP 2

Tilt the terminal up to 45 degrees from the horizontal.



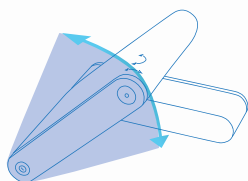
STEP 3

Turn the terminal slowly in clockwise or counterclockwise until the beeping frequency is maximised.



STEP 4

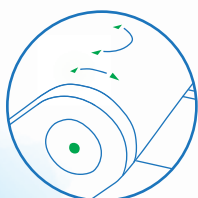
Tilt the terminal up or down slowly until the beeping frequency is maximised.
Fine tune the position until no further increase of the beeping frequency is heard.



'Exit Pointing Mode Button' will turn to flashing green when the signal strength is satisfactory for network registration.

STEP 5

Press the 'Exit Pointing Mode Button' to exit antenna pointing mode and start network registration.



METHOD 3: ISATHUB CONTROL APP

You can point iSavi™ terminal to the satellite network by using the IsatHub Control app.

STEP 1

Download the IsatHub Control app from the iOS App Store or Google Play on your smart device(s).



Note:

Data downloaded over the iSavi™ is chargeable.

Use a free data service to acquire these apps whenever possible.

For Android users in China, please download the application through Wandoujia.

STEP 2

Connect to iSavi™ over the Wi-Fi by selecting it from the list of available Wi-Fi networks.

The default Wi-Fi network name (SSID) and password can be obtained from the product label on the rear of iSavi™ or the label on the packaging box.

STEP 3

Open the IsatHub Control app on the smart phone or tablet.



STEP 4

Follow the on screen instructions and tap 'Pointing assist' for antenna pointing suggestion.



STEP 5

Tilt and turn iSavi™ terminal according to the suggested orientations.

STEP 6

Tap "Connect" on your smart phone or tablet to register with the network once you receive a minimum of 42dB signal strength. You can now carry out your incoming/outgoing voice calls, data and text messaging.

Note:

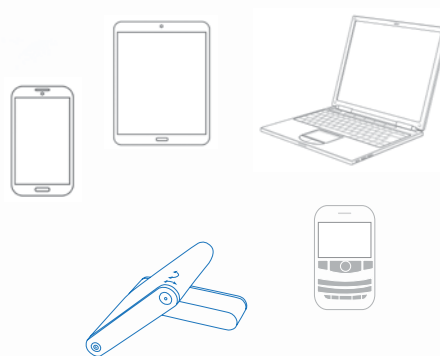
You need to allow GPS location access in the smart device for the 'Pointing assist' to work properly.

ACCESS DATA AND CALLS

STEP 1

Disable the 3G or 4G service from your smart devices. Connect to iSavi™ over the Wi-Fi by selecting it from the list of available Wi-Fi networks.

The default Wi-Fi network name (SSID) and password can be obtained from the product label on the rear of your iSavi™.



Note:
For added security, please change the Wi-Fi password at your earliest opportunity.

STEP 2

For smart device control of your iSavi™, open the IsatHub Control app and follow the instructions presented to get started. Refer to Pointing Assist functionality in IsatHub Control app.



iOS and Android apps are available from App Store and Google Play respectively.

For control of iSavi™ using your web browser, access the web console by opening any web browser and type **http://iSavi** or **http://192.168.1.35** into the address bar.



STEP 3

To access your chosen control interface, the default credentials are:

USERNAME: admin
PASSWORD: 1234

STEP 4

Once iSavi™ is connected to the network, you are ready to start making calls or sending text messages on any iOS or Android smart device with the IsatHub Voice app.

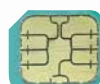
The IsatHub Voice app is available from the iOS App Store and Google Play. It is advised to install the application using a free data service before connecting to the iSavi™ satellite terminal.

Before you first access data over the network, you may need to enter the APN username and password supplied to you with your SIM card by your service provider. Please make sure you have these available.

Refer to the Data Profile section for the setting if required.



Note:
To get optimum data experience and avoid unwanted traffic over satellite, please get advice from your distributor. Please ensure the number format you dialed has included the full international prefix.



STEP 5

Once iSavi™ is connected to the network, you are ready to start a data session. Press the 'Connect data' button to begin and 'Disconnect data' to end all connection to the Internet.



The web console provides data access through the 'Activate data connection' button on the Home page when using a web browser.



To stop access to data press 'Deactivate data connection'

Note:

Signal strength needs to be at least 42dB and above for an acceptable service to commence. You may check the signal strength and registration status using the home page of the web console or the smart phone Control app.

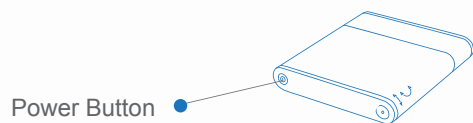
If the signal strength level indicated in the web console is low under registered conditions, you can slowly adjust the terminal angle and monitor the signal strength displayed in web console.

Turn off the terminal by pressing the 'Power' button for five seconds.

POWER DOWN AND REMOVE BATTERY

STEP 1

Press and hold the power button for 5 seconds to switch off iSavi™.

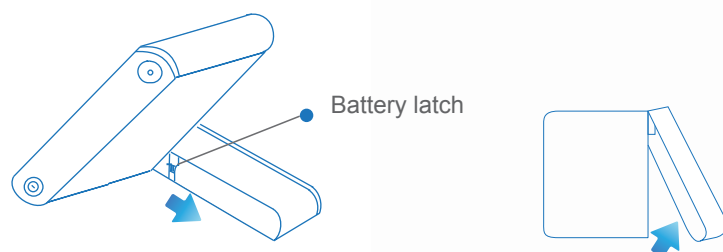


STEP 2

The powering down process takes about 20 seconds.
Wait until all the LEDs are off.

STEP 3

Pull down the battery latch in the direction as shown.



STEP 4

Remove the battery pack gently.

Note: Ensure your iSavi™ is off before removing the battery pack.

The battery pack can be charged separately without attached to your iSavi™.

03 NAVIGATING THE WEB CONSOLE

To control iSavi™ from a web browser, open a web browser after connected the Wi-Fi and enter **http://iSavi** or **http://192.168.1.35** on the address bar.

MENU OVERVIEW

HOME	DATA ▼	TELEPHONY ▼	SMS ▼	SETTINGS ▼	LOGOUT
DATA	TELEPHONY	SMS	SETTINGS		
Data Profile - Primary Profiles - Secondary Profiles (only for BGAN SIM)	SIP Settings	Compose	Account		
Firewall - Setup - Filters - Backup/Restore		Inbox	Wi-Fi - System Info - Wireless Setting - Security Setting		
Device Management		Sent	Security - SIM PIN - Terminal PIN		
Data Settings - VPN Passthrough - ALG		Drafts	Terminal Settings - Reboot Terminal - Factory Reset - Firmware Upgrade - Antenna Pointing Configuration		
			Terminal Info - Information - Logs - Call Log		
			Language		
			Support		

TERMINAL STATUS


The Home page provides the status information of the terminal, pointing information and allows a data connection to be established.

Navigate to Home page for terminal status checking. You can check for the service plan (Example: IsatHub or BGAN) through the area indicated in red box below:

HOME DATA ▼ TELEPHONY ▼ SMS ▼ SETTINGS ▼
iSavi™ LOGOUT

Home IsatHub

Status:
Registered to network - **Yes**
Data connection active - **No**

Signal:
61 dB


GPS:
Last acquired: Tue May 03 2016, 18:54:39 UTC+0800
Lat: 40° 31' 58.72" N
Long: 3° 39' 21.41" W
Type: 3D (NEW)

Battery: 92%
Temperature: Normal

Registered to Network but no active data connection exists. You are now able to make phone calls and send SMSs. Please activate a data connection before doing any data transfer.

Status	Indicates registration and data connection status.
Signal	Indicates terminal received signal strength.
GPS	Indicates GPS information.
Battery	Indicates available capacity of the battery.
Temperature	Indicates current operating temperature status.

Click “**Activate Data Connection**” or “**Deactivate Data Connection**” in order to activate or deactivate data connection.

Note:

Signal strength must be 42dB or above for the iSavi™ terminal to successfully connect or register to the network. Signal strength can be improved by pointing more accurately.

If the signal strength level indicated in the web console is low under registered condition, you can slowly adjust the terminal’s elevation and azimuth angles and monitor the signal strength displayed in web console.

DATA

DATA PROFILE SETTINGS

Navigate to **Data > Data Profile** in order to modify the connection type.

Connection profile defines the connection type.

You can select from a list of profiles to be the default primary profile and connection type.

Data Profile

IsatHub

Profiles

default ★

Edit

Add

★ - Default Profile

📶 - Activated

Click “Edit” to modify the data profile.

Note:

From a smart phone or tablet, the Control app will always use the connection profile defined as default.

You can create your customized primary profile.

Data Profile iSavi™

☒ Set as default

Profile Name:

'Static IP Address APN

Access Point Name (APN):

☐ SIM

☒ User Defined

Static IP
Address APN Username:

Static IP
Address APN Password:

Please note that the 'username' and 'password' stated above are not those used to login to the WebConsole. They are those provided by your Service Provider for a static IP address subscription. If you do not have any such a subscription or if you are not sure, please leave them blank.

Limited Connection:

Traffic Volume: MB (1 ~ 1024)

Usage Warning: %

Note:

Please note that the 'Static IP Address APN Username' and 'Static IP Address APN password' stated are not WebConsole login purpose.

These are provided by your Service Provider under a static IP address subscription. Leave it blank if you do not have such subscription.

Profile Name

Change the profile name as desired.

Access Point Name (APN)

By default, the APN from your SIM card is selected.

Follow these steps to change the Access Point Name (APN):

1. Select User Defined.
2. Enter the new APN in the field space provided (e.g. STRATOS.BGAN.INMARSAT.COM).
3. Enter the username and password if required (these details have been supplied by your service provider) if required.

Static IP Address APN

By default, a Dynamic IP Address is selected.

To use a Static IP Address:

1. Select Static IP Address and enter the APN address and password in the space provided.

Limited Connection (available only for iSatHub Control app)

By using this feature, the Administrator can configure and control the data usage of the user using limited volume options. Usage warning percentage is used to remind the user when their usage exceeds the specified percentage of the data limit.

Note:

The data connection will be automatically deactivated when the volume used has reached the defined limit. The usage warning will prompt in the Control app and the Web Console.

BGAN STREAMING

BGAN Streaming is an Inmarsat service which provides “guarantee” bandwidth to the users. It is charged by “per minute” connection. For iSavi, this feature is available only with BGAN SIM.

Note:

Select **Connection Type: Standard** if port configuration is required. Configure the desired rate and minimum rate under secondary profiles.

Streaming without port configuration:

1. Navigate to **Data > Data Profile> Primary Profile**.
2. Select **Connection Type: Streaming**.
3. Select Desired Rate and Minimum Rate of the Parameters (32k or 64k).
4. Click **Update Settings**.

The screenshot shows the 'Primary Profiles' configuration page. At the top, there's a 'Set as default' checkbox. Below it, the 'Profile Name' is set to 'default'. The 'Connection Type' is set to 'Streaming' (radio button selected). A warning message states: 'Using this connection type you will be charged **PER MINUTE** of time used. Use this connection type for UDP applications, data exchange and transfer such as Streaming Audio and Video application ONLY. DO NOT LEAVE STREAMING IP CONNECTED WHEN NOT BEING USED!'. The 'Access Point Name (APN)' section has 'SIM' selected with the value 'bgan.inmarsat.com'. There are fields for 'Static IP Address APN Username' and 'Static IP Address APN Password'. A note explains that these are not login credentials but for static IP subscriptions. The 'Streaming Parameters' section shows 'Desired Rate' and 'Minimum Rate' both set to '32k'. The 'Limited Connection' section has 'Traffic Volume' set to '1 ~ 1024 MB' and 'Usage Warning' set to '%'. At the bottom are 'Update Settings', 'Delete', and 'Cancel' buttons.

5. Navigate to **Home** page to activate data connection. Primary profiles is activated now.

Streaming with port configuration:

1. Navigate to **Data > Data Profile> Primary Profile**.
2. Select **Connection Type: Standard**.
3. Click **Update Settings** at the bottom for this settings to take effect.
4. Navigate to **Data > Data Profile> Secondary Profile**.
5. Select Desired Rate and Minimum Rate of the Parameters (32k or 64k).
6. Select '+' sign to add Destination Port ranges and Protocol type.
7. Click **Update Profile** at the bottom for this settings to take effect.

The screenshot shows the 'Secondary Profiles' configuration page. It has a 'Profile Name' field. The 'Streaming Parameters' section shows 'Desired Rate' and 'Minimum Rate' both set to '32k'. Below this is a table for 'Destination Port Ranges' with columns 'From', 'To', 'Protocol', and 'Delete All'. The first row has 'From' and 'To' fields, 'Protocol' set to 'TCP', and a 'Delete All' link. At the bottom are 'Add Profile' and 'Cancel' buttons.

8. Navigate to **Home** page to activate data connection. The settings are activated.

FIREWALL PROTECTION SETTINGS

Firewall is a built-in network security feature in the iSavi™ to monitor and control the incoming and outgoing network traffic by analysing the data packets based on predetermined security rules. It is highly secure and reliable that uses packet inspections to prevent hacker's attack.

With Firewall feature, you can:

- Block the unwanted traffic from the Internet network to your terminal.
- Block access from your terminal to Internet network locations.
- Filter the host names.
- Control the internet network access by using the keywords on the web addresses.

You can define up to 10 rules to allow or reject incoming IP packets from the public network. The filtering rules are based on the protocols, IP addresses (source/destination) and port numbers (source/destination). Firewall function is disabled by default. Navigate to the firewall setup page to enable it.

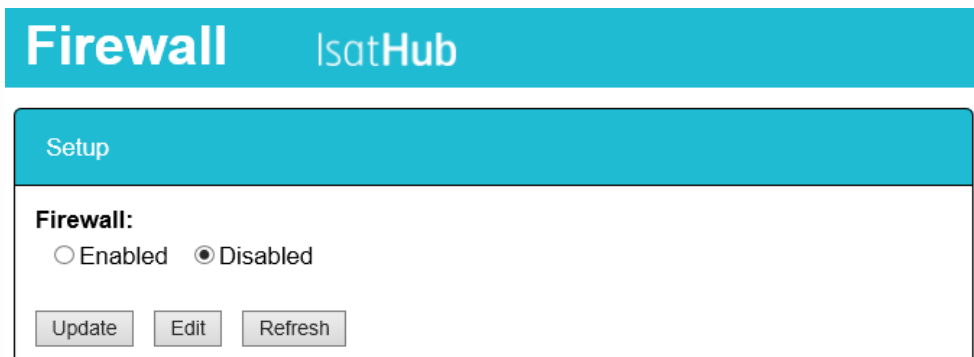
Scenario: Allow only internet browsing but block all other traffics on any connected devices

To block all other traffics on any PCs but only allow Internet Browsing, we have to reject all incoming packets and allow only two ports under both incoming and outgoing rules.

Port 80: Internet Browsing

Port 53: DNS lookup

Navigate to **Data > Firewall > Setup**, select Edit to modify the Firewall protection profile setup.

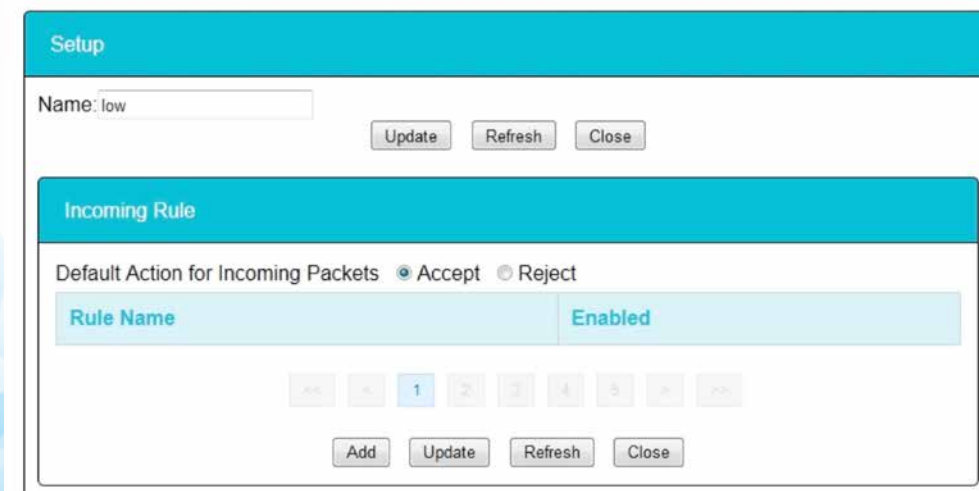


Note:

By default, Custom 1 and Custom 2 block everything from the internet.

Follow these steps to change the profile setting.

1. Select profile name.
2. Click **Edit** to modify the predefined profile settings.
You can edit the profile name and predefined rules to allow or reject incoming packets.



Incoming Rule

Rule Name:

Protocol: ☒ TCP ☐ UDP ☐ ICMP ☐ ANY

Source IP Address: . . . /

Source Port: -

Destination IP Address: . . . /

Destination Port: -

Action: ☒ Allow ☐ Reject

Note: IP Addresses, Ports with value 0 means ANY.
 eg. IP (0.0.0.0 / 0) means ANY IP, Port (0 - 0) means ANY Port.

Incoming Rule

1. Set the default action of Incoming Rule as **Reject** and click **Update**.
2. Under Incoming Rule tab, click **Add** to add new rules.
3. Enter your desired rule name and fill in the necessary information.

Rule Name: Allow internet browsing

Source IP Address: 0.0.0.0-0.0.0.0 (Note: to accept all IP address for range 0.0.0.0-0.0.0.0)

Protocol: TCP

Source Port: 80-80

Action: Allow

4. Select **Action: Allow** to allow port 80 only.
5. Click **Apply** to save the new incoming rules.
6. Click **Update** for this rules to take effects.
7. Click **Add** on the second row for the second incoming rule.
8. Repeat similar steps again to add new rule for port 53 to allow DNS lookup.
9. Click **Apply** to the save the new incoming rules.

Note: The firewall settings allow internet browsing only and block all other traffics on all the connected devices to the range 0.0.0.0-0.0.0.0 in the source IP address. To specify which device to be accessed to the terminal, check the device IP address under "Source IP Address" for both the incoming and outgoing rules.

Outgoing Rule

1. Set the default action of Outgoing Rule as **Reject** and click **Update**.
2. Under Outgoing Rule tab, click the '+' symbol besides the rule name to edit the existing rules. or click **Add** to add new rules.

The screenshot shows the 'Outgoing Rule' configuration window. At the top, there's a title bar 'Outgoing Rule'. Below it, a section 'Default Action for Outgoing Packets' has two radio buttons: 'Accept' and 'Reject', with 'Reject' selected. Below this is a table with two columns: 'Rule Name' and 'Enabled'. The table lists several rules: FTP Data, FTP Ctrl, SSH, Telnet, SMTP, DNS, HTTP, POP3, and Ping. Each rule has a '+' icon to its left and a checkmark in the 'Enabled' column. At the bottom of the window, there are buttons for 'Add', 'Update', 'Refresh', and 'Close', along with a pagination control showing '1' of 10 items.

Rule Name	Enabled
+ FTP Data	<input checked="" type="checkbox"/>
+ FTP Ctrl	<input checked="" type="checkbox"/>
+ SSH	<input checked="" type="checkbox"/>
+ Telnet	<input checked="" type="checkbox"/>
+ SMTP	<input checked="" type="checkbox"/>
+ DNS	<input checked="" type="checkbox"/>
+ HTTP	<input checked="" type="checkbox"/>
+ POP3	<input checked="" type="checkbox"/>
+ Ping	<input checked="" type="checkbox"/>

3. You can create your desired rule name and fill in the necessary information.

The screenshot shows the 'Outgoing Rule' configuration window with the 'Add' rule form. The form has the following fields: 'Rule Name' (text box with 'Rule3'), 'Protocol' (radio buttons for TCP, UDP, ICMP, ANY, with TCP selected), 'Source IP Address' (text box with four empty boxes and a slash), 'Source Port' (text box with two empty boxes and a dash), 'Destination IP Address' (text box with four empty boxes and a slash), 'Destination Port' (text box with two empty boxes and a dash), and 'Action' (radio buttons for Allow, Reject, with Allow selected). Below the form are buttons for 'Apply', 'Clear', and 'Cancel'. At the bottom, there is a note: 'Note: IP Addresses, Ports with value 0 means ANY. eg, IP (0.0.0.0 / 0) means ANY IP, Port (0 - 0) means ANY Port.'

Rule Name: Rule3

Protocol: ☒ TCP ☐ UDP ☐ ICMP ☐ ANY

Source IP Address: [] . [] . [] . [] / []

Source Port: [] - []

Destination IP Address: [] . [] . [] . [] / []

Destination Port: [] - []

Action: ☒ Allow ☐ Reject

Apply Clear Cancel

Note: IP Addresses, Ports with value 0 means ANY.
eg, IP (0.0.0.0 / 0) means ANY IP, Port (0 - 0) means ANY Port.

Rule Name: Allow internet browsing
Source IP Address: 0.0.0.0-0.0.0.0 (Note: to accept all IP address for range 0.0.0.0-0.0.0.0)
Protocol: TCP
Source Port: 80-80
Action: Allow

4. Click **Apply** to save the new incoming rules.

5. Click **Update** for this rules to take effects.
6. Click **Add** on the second row for the second incoming rule.
7. Repeat similar steps again to add new rule for port 53 to allow DNS lookup.
8. Click **Apply** to the save the new incoming rules.

Note:

STMP,IMAP, POP3 are for Email purpose. HTTP is for browsing protocol purpose. You can add new rule to the list.

Re-activate your data connection for the new firewall setting to take effect.

Hostname Filtering

To stop the users from accessing certain websites through the internet, you can configure the filtering settings in your iSavi™.

Navigate to **Data > Firewall > Filters** to enable the filtering based on the hostname or the keywords.

Follow these steps to apply hostname filtering:

1. Select Enabled.
2. Click Update to modify the settings.
3. Click Add to add new keywords (eg. facebook).
4. You can modify existing keywords by selecting the Text from the list.
5. Click Edit to modify or Delete to delete the selected keywords.

Note:

Hostname filters will only take effect when HTTP/HTTPS rules are enabled under Data> Firewall> Setup.
Re-activate your data connection for the new settings to take effect.

Filters

Hostname Filters:

☐ Enabled ☒ Disabled

Note: Hostname filters will only take effect when HTTP/HTTPS rules are enabled (allowed)

Hostname/Keywords

Text

<< < 1 > >>

Backup/ Restore the Firewall Settings

Firewall settings can be saved and kept as a reference for the future reference.

Navigate to **Data > Firewall > Backup** to save or restore the firewall settings.

Backup firewall settings:

1. Click Backup.
2. The firewall settings will be saved as a document.
(eg. iSavi_FirewallBackup_20141218170807.bin)

Restore firewall settings:

1. Browse the file location of previous backup file.
2. Click Restore.
3. Navigate to **Settings > Terminal Settings > Reboot Terminal** for the new settings to take effect.

Backup/Restore

Backup:

Restore:

Backup package: No file selected.

ACCESS RIGHTS SETTING ACCORDING TO MAC ADDRESS

Navigate to **Data > Device Management** to set the allowed MAC address and the access rights.

The MAC address is a number that uniquely identifies any device connected to a network. Once the device is connected to the terminal, the MAC address will be shown on the page.

From this page, you can also check the number of connected devices, their MAC addresses and the data usage of the terminal.

Name	MAC Address	Admin
Default Rule		
C0F8DA223F34★	C0:F8:DA:22:3F:34	



Add Edit Delete Refresh

★ - Device connected

Device connected: 1/128
Upload: 1.66 MB
Download: 0 byte

You can add a new MAC address by clicking Add or create a nickname for an existing MAC address by clicking on the Edit button. Data usage of the device is available at the bottom of the page.

Note:

The actual value of the data usage might be slightly different from the readings in Control app and Web Console.

☒ Temporary Entry

Name:

MAC Address:

Access Level: ☐ Admin

Permissions:
☒ Incoming Call
☒ Outgoing Call
☒ Data

Update Cancel

★ - Devices connected

IP Address: 192.168.1.40
Upload: 214.72 KB
Download: 0 byte

1. Define a nickname for the device.
2. Check if the MAC address belongs to the smart phone or tablet used to host the Control app. Only one device is allowed to use the Control app at a time.
3. You can define access rights selecting the relevant permission options.
4. The settings are stored temporarily and are not retained after terminal is rebooted. If you plan to keep the same access rights settings, deselect **Temporary entry** so that the access rights are stored even after the terminal is rebooted.

DATA SETTING

A Virtual Private Network (VPN), is a network technology that constructs a secure network connection over a public network (usually the internet) or a private network owned by a service provider. It enables remote users to securely connect to a private network.

VPN tunnel is the link between the two locations.

Note: The VPN Passthrough is disabled by default and users need to navigate to the Data Setting page to enable it.

Navigate to **Data > Data Settings > VPN Passthrough** to change the VPN Passthrough setup.

PPTP Passthrough:

Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network.

IPSec Passthrough:

Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks by using the cryptographic security services.

To enable VPN Passthrough

1. Click **Enabled**.
2. Click **Update** for the new configuration to take effect.

Data Settings IsatHub

VPN Passthrough

	State
+ PPTP Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
+ IPSec Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Update Refresh

Application Layer Gateways (ALGs) manage specific protocols by intercepting traffic as it passes through the security device. After analyzing the traffic, the ALG allocates resources to permit the traffic to pass securely Application Layer Gateway (ALG). It allows customized Network Address Translation (NAT) traversal filters to be attached into your iSavi™ and support address and port translation for certain application layer protocols (control/data).

To allow the data transmission across NAT

1. Click **Enabled**.
2. Click **Update** for the new configuration to take effect.

Data Settings IsatHub

VPN Passthrough

ALG

	State	Protocol
+ FTP ALG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	TCP ▼
+ H.323 ALG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	TCP ▼

Update Refresh

TELEPHONY

SIP SETTINGS

Navigate to **Telephony > SIP setting > SIP Server** to change the RTP Codec. The RTP codec is an audio encoding. The quality of the voice depends on your smart devices. You may change the RTP codec for better voice quality.



Note:

SIP calls with the iSavi™ terminal require a special SIP client application on your smart phone or tablet. The Isathub Voice app is available from the App Store or Google Play.

SIP calls from a Windows or Macintosh PC are not supported. For best results, please use the Isathub Voice App, other SIP clients may work but are not recommended and will need configuration.

SMS

COMPOSE NEW SMS

Navigate to **SMS > Compose** to enter compose page.



1. Enter the recipient's phone number in the Phone no. box. Type the message in the text editor box.
2. Click **Send** to send the SMS.
3. To save an unsent SMS, click **Save** and the unsent SMS will be saved in **Drafts**.
4. Check the box ☒ if you wish to store a sent SMS on to the SIM card.
5. Click **Append GPS** to include your GPS location in the SMS.

Note:

When sending an SMS with your iSavi™ terminal you should always enter the full international phone number format for your recipient. This is true even if you are located in the same country as the recipient when sending the message. Larger SMS content with more than 160 characters are supported as multi-segmented SMS.

VIEW RECEIVED SMS

Navigate to **SMS > Inbox** to view Received SMSs.

Reply to an SMS from Inbox:

1. Select the SMS you plan to reply to by selecting the particular SMSs.
2. Click **Reply**.
The inbox console is switched to Compose mode.
3. Enter your reply in the text box.
4. Click **Send**.

Forward an SMS from the Inbox:

1. Select the SMS you plan to forward and click **Forward**.
The inbox console is switched to Compose mode.
2. Enter your reply in text box.
3. Click **Send**.

Delete an SMS from the Inbox:

1. Select the SMS you plan to delete and click **Delete**.
A single SMS or multiple SMSs can be deleted based on the selection.
2. Click **OK** to confirm the deletion, or **Cancel** to abort.

To Refresh the Inbox list:

1. Click **Refresh**.

VIEW SENT SMS

Navigate to **SMS > Sent** to view Sent SMS.

Resend a sent SMS:

1. Select the SMS you plan to resend and click **Resend**.
The SMS is sent to the recipient.

Forward a sent SMS:

1. Select the SMS you plan to forward and click **Forward**.
The Sent console is switched to the Compose mode.
2. Enter the recipient's number in the Phone No. field.
3. Click **Send**.
4. The SMS is sent to the recipient.

Delete a sent SMS:

1. Select the SMS you plan to delete.
2. Click **Delete**.
3. Click **OK** to confirm the deletion, or **Cancel** to abort.

Note:

Sending or receiving SMSs through the Voice app do not leave a copy in the SIM card for privacy reason.
User have to open Control app in parallel for any SMS sending through Voice app.
SMS sending can be done once your iSavi™ terminal is registered to the network. Data connection is not required for voice call and SMSs

VIEW DRAFT SMS

Stored SMSs are saved inside the draft folder.
Navigate to **SMS > Draft** to view Draft SMSs.

Send a draft SMS:

1. Select the draft SMS you plan to send.
2. Click **Send**.
The SMS is sent to the recipient.

Forward a draft SMS to other recipient:

1. Select the draft SMS you plan to send and click **Send**.
2. Click **Forward**.
3. The draft console is switched to the Compose console.
4. Enter the recipient's number in the Phone No. field.
5. Click **Send**.
The SMS is sent to the recipient.

Delete a draft:

1. Select the draft SMS you plan to send.
2. Click **Delete**.
3. Click **OK** to confirm the deletion, or **Cancel** to abort.

SETTINGS

CREATE ACCOUNT FOR WEB CONSOLE ACCESS

Navigate to **Settings > Account** to create or edit an account for Web Console and Control app access.
By default, the password for admin is **1234**. You are recommended to change the admin password for security reasons.

Only one User and one Admin account are allowed for iSavi™.

Most of the configuration changes are done by admin account.
User account are basically for the user to change APN settings, extract terminal information such as serial numbers and logs.

Differences of access right for user account (Web Console and Control app Interface):

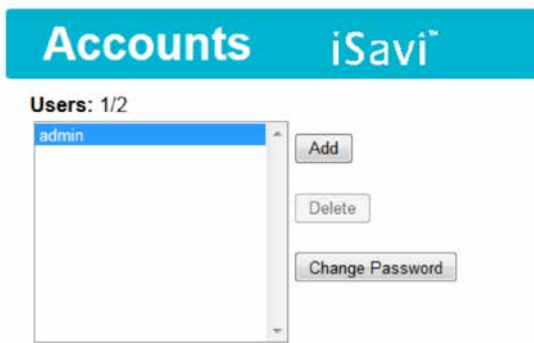
Web Console- User Account

- Data-> Data Profile for SIM card APN settings
- SMS features
- Terminal info such as Information of terminal, Logs
- Language of the Web Console
- Support team contact
- Device Management are not accessible.

Control App- User Account

- Firewall and Wi-Fi password are not accessible.
- Others tab can be accessed as normal in the Control app.
- Device Management can be done through Control app (access right based on devices).

Navigate to **Settings > Account** to create or edit an account for Web Console and Control app access. By default, the password for admin is **1234**. You are recommended to change the admin password for security reasons.



Add a new account:

1. Click **Add**.

This screenshot shows the 'Add' form in the iSavi Accounts section. The header is the same as the previous image. Below the header, there are three input fields: 'Username:' with the value 'user', 'New Password:', and 'Re-type Password:'. At the bottom of the form are two buttons: 'Add' and 'Cancel'.

2. Type New Password and Re-type Password.
3. Click **Add**.
The new account is added into the account list.

Delete an account:

1. Select the account which you want to delete.
2. Click **Delete**.
Account name is deleted successfully.

Change account password:

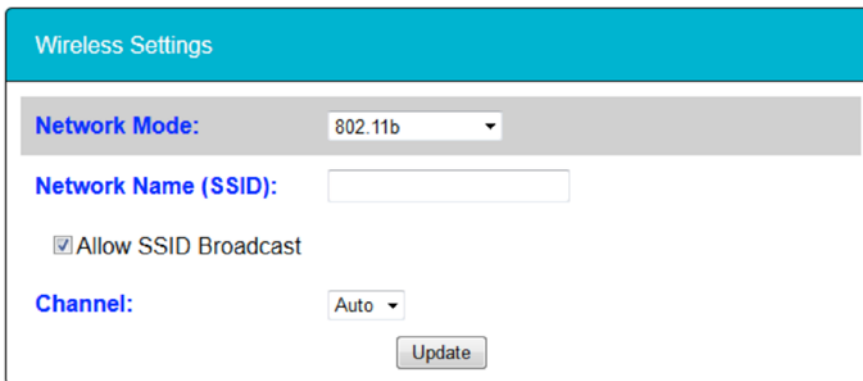
1. Select the account which you want to change the password (example: admin).

This screenshot shows the 'Change Password' form for the 'admin' user. The 'Username:' field is pre-filled with 'admin'. Below it are three input fields: 'Old Password:', 'New Password:', and 'Re-enter New Password:'. At the bottom are two buttons: 'Update' and 'Cancel'.

2. Type the old password, the new password, and then re-enter the new password.
3. Click **Update** for the new password to take effect.

CHANGE SSID AND WI-FI PASSWORD

Navigate to **Settings > Wi-Fi> Wireless Settings** to change network mode and network name.

A screenshot of the 'Wireless Settings' interface. It features a blue header bar with the title 'Wireless Settings'. Below the header, there are four main sections: 'Network Mode:' with a dropdown menu showing '802.11b'; 'Network Name (SSID):' with an empty text input field; a checkbox labeled 'Allow SSID Broadcast' which is checked; and 'Channel:' with a dropdown menu showing 'Auto'. At the bottom right of the settings area is an 'Update' button.

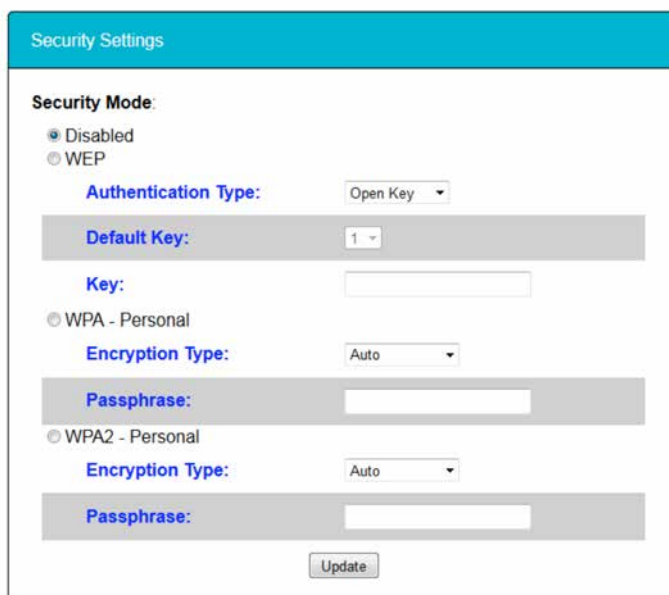
Note:

SSID network name is the Wi-Fi network name that other users will see on their smart phone, tablets or personal computers when they view a list of available networks.

You can get the default SSID of your iSavi™ from the product label.

After changing the Wi-Fi setting, the Wi-Fi connection will be disconnected.
Please wait for about 30 seconds and establish the Wi-Fi connection again.

Navigate to **Settings > Wi-Fi> Security Settings** to set password of your Wi-Fi network.

A screenshot of the 'Security Settings' interface. It has a blue header bar with the title 'Security Settings'. The main content area is divided into sections for different security modes. The 'Security Mode:' section has three radio buttons: 'Disabled' (selected), 'WEP', and 'WPA - Personal'. Under 'WEP', there is an 'Authentication Type:' dropdown set to 'Open Key', a 'Default Key:' dropdown set to '1', and a 'Key:' text input field. Under 'WPA - Personal', there is an 'Encryption Type:' dropdown set to 'Auto' and a 'Passphrase:' text input field. Below these, there is another section for 'WPA2 - Personal' which also has an 'Encryption Type:' dropdown set to 'Auto' and a 'Passphrase:' text input field. An 'Update' button is located at the bottom right of the settings area.

Security Mode: Disabled or select the security mode for the wireless local area network.

Three different security modes are available:

- Wired Equivalent Privacy (WEP)
For 64-bit encryption - You can enter either 5 ASCII characters or 10 hexadecimal digits (any combination of 0-9, a-f, A-F, empty string is not permitted).

For 128-bit encryption - You can enter either 13 ASCII characters or 26 hexadecimal digits (any combination of 0-9, a-f, A-F, empty string is not permitted)

- Wi-Fi Protected Access® Personal (WPA)
You can enter 8-63 characters of keys for the password.
- Wi-Fi Protected Access® 2 Personal (WPA2)
You can enter 8-63 characters of keys for the password.

Note: WPA2 is highly recommended over WEP for a higher level of security.

Note:

The default SSID password of iSavi™ is configured under WPA2 mode.

To help safeguard your data connection and the associated bill, please change the default SSID password printed on the product label of iSavi™ to your preferred password as soon as possible.

After changing the Wi-Fi setting, the Wi-Fi connection will be disconnected. Please wait for about 30 seconds and establish the Wi-Fi connection again.

To reset SSID and Wi-Fi password, follow these steps:

1. With the terminal off, remove the SIM card.
2. Press and hold the 'Power' button for 5 seconds to turn on iSavi™.
3. Once the 'Power' button LED is steady red, press and release the 'Exit Pointing Mode' button for 3 times continuously.
4. Press and hold the 'Exit Pointing Mode' button for 5 seconds before releasing the button .
5. All the LEDs will flash in red once the reset is triggered.
6. iSavi™ will reboot automatically once the reset is completed.
7. Once the 'Power' button LED is steady red, press and hold the 'Power' button for 5 seconds to turn off iSavi™.
8. Insert the SIM card.
9. Press and hold the 'Power' button for 5 seconds to turn on iSavi™.
10. Re-establish again the Wi-Fi connection about 1 minute after the terminal is power on.

CONFIGURE SECURITY SETTING

SIM PIN

If the security feature is enabled, a prompt requests you to enter the SIM PIN each time you power up your iSavi™. This helps to prevent unauthorised use of your SIM. Disable this feature to skip the PIN entry process.

Navigate to **Settings > Security> SIM PIN** to enable SIM PIN.

1. Select **Enabled** to set the SIM PIN.
2. Select **Disabled** if you do not need to set the SIM PIN.
3. Enter the PIN number in the space provided and click **Apply**.

Note:

The SIM PIN depends on the SIM card. Consult your service provider if necessary.

[HOME](#) [DATA ▾](#) [TELEPHONY ▾](#) [SMS ▾](#) [SETTINGS ▾](#) [LOGOUT](#)

Security

iSavi™

SIM PIN

PIN

☐ Enabled ☒ Disabled

Enter PIN:

TERMINAL PIN

Once Terminal PIN is activated, your iSavi™ will prompt for the password everytime when you reboot the terminal. The same password is used for the Factory Reset PIN.

Navigate to **Settings > Security> Terminal PIN** to enable Terminal PIN.

1. Select **Enabled** to enable Terminal PIN.
2. Select **Disabled** if you do not need to enable Terminal to SIM.
3. Enter the PIN number in the space provided and click **Update PIN**.

Terminal PIN

PIN

☐ Enabled ☒ Disabled

Enter PIN:

Note:

With SIM PIN or Terminal PIN enabled, the Power Button of your iSavi™ LED is solid red after powering up process. Login to Web Console to enter the PIN number.

TERMINAL SETTINGS

Navigate to **Settings > Terminal Settings> Reboot Terminal** to reboot the terminal.

Reboot Terminal

Click on the button to reboot the Terminal:

Reboot

Navigate to **Settings > Terminal Settings > Factory Reset** to factory reset the terminal.

Enter security code for factory reset (Default:0000).

Factory Reset

Security code:

Factory Reset

NOTE:
Executing "Factory Reset" will reset all of the system configuration settings to default values and clear all user data from the non-volatile memory.

Note:

By default, the security code is 0000. Once you change the Terminal PIN, the Factory Reset password is changed to match the Terminal PIN.

From firmware R02.0.0 onwards, after factory reset, Web Console will remind you to change a password with higher security requirement. The password should be minimum 6 characters long with a combination of uppercase and lowercase letters, numbers and symbols.

HOME DATA TELEPHONY SMS SETTINGS

iSavi™ LOGOUT

Change Password IsatHub

Username:	admin
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Re-enter New Password:	<input type="password"/>

Update

Note:
For maximum security, password should be min 6 characters long and a combination of uppercase and lowercase letters, numbers and symbols.

UPGRADE FIRMWARE

Firmware upgrade allows you to update your iSavi™ with the latest operating software. Your iSavi™ has to be in Safe Mode for firmware upgrading.

Navigate to **Settings > Terminal Settings> Firmware Upgrade** to perform a firmware upgrade. Your iSavi™ will reboot in Safe Mode once you click the Firmware Upgrade button. Refer to page 34, Web Console in Safe Mode for details.

Note:

It takes about 90 seconds for your terminal to reboot into safe mode. Please establish the Wi-Fi connection again.

Firmware Upgrade

Need to reboot in the Firmware Upgrade Mode (Safe Mode). Please do it manually if reboot failed.

Firmware Upgrade

Disclaimer

Please be informed that firmware upgrading is done at your own risk and the equipment manufacturer will not be held responsible for any possible malfunction or damage to the system due to upgrading the firmware.

If you encounter any problems or have any questions, please contact the equipment distributor for technical support.

CONFIGURE ANTENNA POINTING LED

By default, all the Antenna Pointing LEDs would be switched off when the LED status is ready for service or Data is activated.

Navigate to **Setting > Terminal Settings> Antenna Pointing LED Configuration** to change the setting. You can select **Always On (Antenna Pointing LED)** and click **Update** for the new settings to take effect.

Antenna Pointing LED Configuration

Antenna Pointing LED: ☒ Off
☐ Always On (Antenna Pointing LED)

Update Refresh

TERMINAL INFORMATION AND LOG FILES

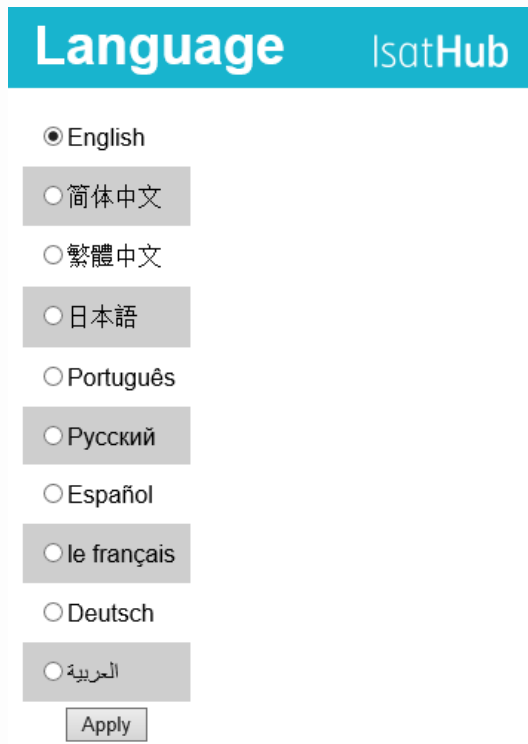
Navigate to **Setting > Terminal Info> Information** in order to check for the detail of the terminal. You may need to supply this information when contacting your service provider.

Event Logs and Error Logs

Navigate to **Setting > Terminal Info> Logs** to view the Event Log or Error Log of the terminal. Click **Export all Logs** in order to export the logs.

SELECT LANGUAGE

Navigate to **Setting > Terminal Info> Language** to select the desired language for the Web Console. The default language is English. English, Chinese Simplified, Chinese Traditional, Japanese, Portuguese, Russian, Spanish, French, German and Arabic are available for your selection.



Language IsatHub

- ☒ English
- ☐ 简体中文
- ☐ 繁體中文
- ☐ 日本語
- ☐ Português
- ☐ Русский
- ☐ Español
- ☐ le français
- ☐ Deutsch
- ☐ العربية

Apply

TECHNICAL SUPPORT

Navigate to **Settings > Support** to get the contact information of your service provider's support team.

04 WEB CONSOLE IN SAFE MODE

Safe Mode is a simple version of the normal Web Console with some basic settings. If you could not access the Web Console in normal way, you can try to access the Web Console in the Safe Mode.

ENABLE SAFE MODE

There are two methods of enabling Safe Mode.

Method 1: Enter Safe Mode by Web Console (Normal Mode)

1. With the terminal on, connect your smart devices or personal computer to the Wi-Fi of iSavi™.
2. Login to Web Console by typing **http://iSavi** or **http://192.168.1.35** into the address bar of any web browser.
3. Navigate to **Settings > Terminal Settings> Firmware Upgrade** to perform firmware upgrade. iSavi™ will be rebooted in the safe mode once you click the Firmware Upgrade button.
4. If Safe Mode is enabled successfully, all of the four Antenna Pointing LEDs are amber, refer to page 56, Appendix A: Antenna Pointing LED Status Table.
5. Connect the computer to the Wi-Fi of your iSavi™.
6. Login to the Web Console in safe mode by typing **http://iSavi** or **http://192.168.1.35** into the address bar of any web browser.

Method 2: Enter Safe Mode by using physical buttons.

1. With the terminal off, press and hold 'Exit Pointing Mode' button.
2. Press the 'Power' button for 5 seconds.
3. Release both 'Exit Pointing Mode' button and 'Power' button.
4. If Safe Mode is enabled successfully, all the four Antenna Pointing LEDs will turn to Amber colour, refer to page 56, Appendix A: Antenna Pointing LED Status Table.
5. Connect the computer to the Wi-Fi of your iSavi™.
6. Log in to the Web Console by typing **http://iSavi** or **http://192.168.1.35** into the address bar of any web browser.

Note:

The username and password of the Web Console are the same for Normal Mode and Safe Mode.

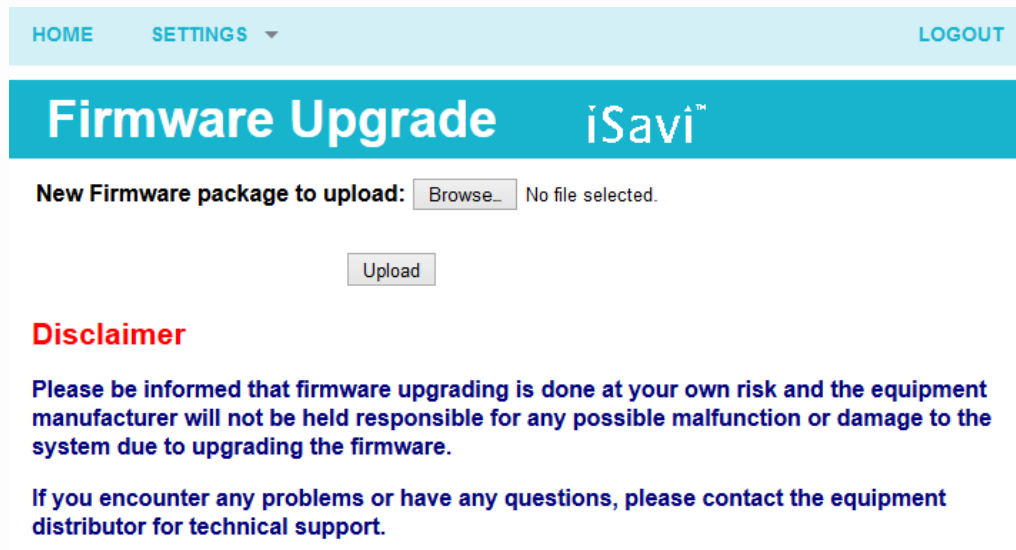
MENU OVERVIEW

HOME	SETTINGS ▼	LOGOUT
SETTINGS		
Factory reset		
Terminal Info		
Logs		
Calibration		

UPGRADE FIRMWARE

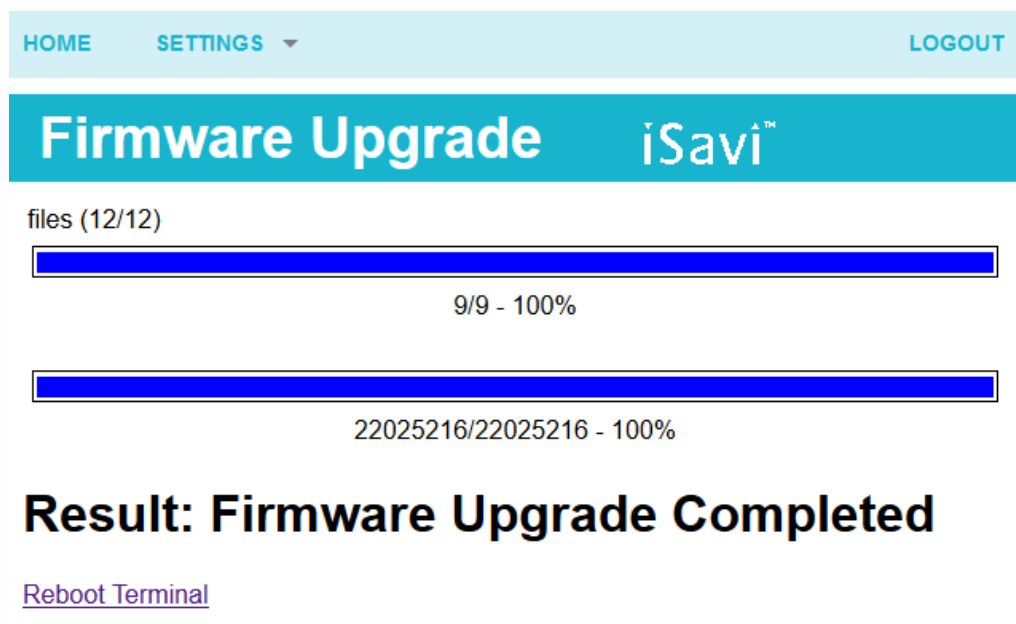
The Home page of Safe Mode is for the firmware upgrade purpose.
Navigate to Home page in order to perform a firmware upgrade.
Plug in the power adapter to iSavi™ before the firmware upgrades.

1. Browse to the file location of the new firmware, select and click **Upload**.



The screenshot shows the 'Firmware Upgrade' page for iSavi™. At the top, there is a navigation bar with 'HOME', 'SETTINGS' (with a dropdown arrow), and 'LOGOUT'. Below this is a teal header with 'Firmware Upgrade' and the iSavi™ logo. The main content area has a label 'New Firmware package to upload:' followed by a 'Browse...' button and the text 'No file selected.' Below this is an 'Upload' button. A red 'Disclaimer' section follows, containing two paragraphs of text in blue. The first paragraph states that firmware upgrading is done at the user's own risk and the manufacturer is not responsible for malfunctions or damage. The second paragraph advises contacting the equipment distributor for technical support if problems arise.

2. Firmware upgrade will take less than 10 minutes to complete.
You will be prompted with the Result: **Firmware Upgrade Completed message**.



This screenshot shows the 'Firmware Upgrade' page after the upgrade is complete. The navigation bar and header are the same. The main content area now displays two progress bars, both at 100%. The first bar is labeled 'files (12/12)' and '9/9 - 100%'. The second bar is labeled '22025216/22025216 - 100%'. Below the progress bars, the text 'Result: Firmware Upgrade Completed' is displayed in a large, bold, black font. At the bottom, there is a link labeled 'Reboot Terminal' in purple.

3. Click **Reboot Terminal** for the new firmware to take effect.

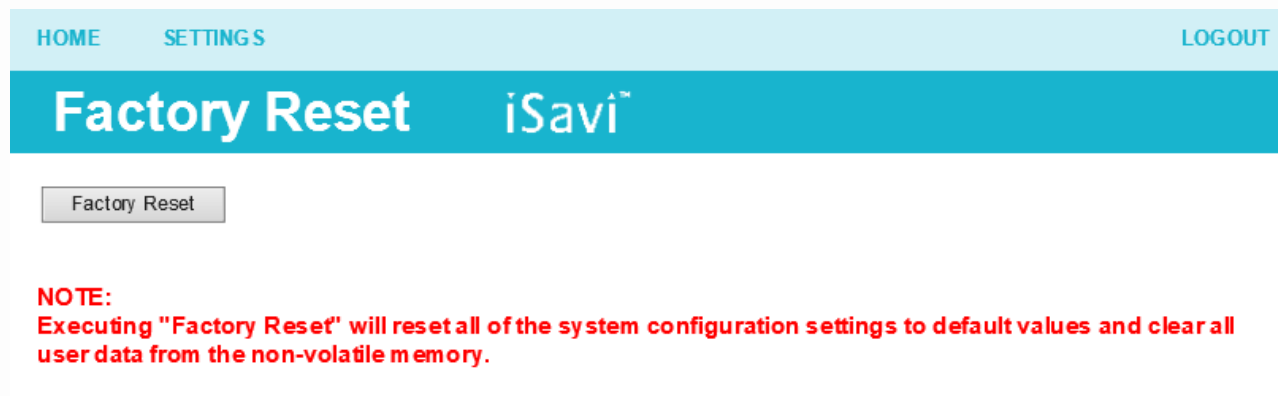
Note:

Ensure the battery level is at least 75% before performing the firmware upgrade or have the terminal on charge.

FACTORY RESET OF SAFE MODE

To reset the terminal, navigate to **Settings >Factory Reset**.

1. Click **Factory Reset**.
2. Enter security code for factory reset (Default: 0000).
iSavi™ will be rebooted within 90 seconds.



3. Re-establish the Wi-Fi connection again.

Note:

By default, the security code is 0000. Once you change Terminal PIN, the Factory Reset password is depends on the Terminal PIN.

All the system configuration settings are set to default value after factory reset is completed. You are recommended to backup the firewall settings before triggering the factory reset.

TERMINAL INFORMATION AND LOG FILES

Navigate to **Setting > Terminal Info** in order to check for the details of the terminal's operation. You may need to supply this information when contacting your service provider.

Event Logs and Error Logs

Navigate to **Setting > Logs** to view the Event Log or Error Log of the terminal. Click **Export All Logs** in order to export the logs.

CALIBRATE THE MAGNETOMETER

Your iSavi™ contains a magnetometer (digital compass) which the accuracy can be affected by magnetic or other environmental interference.

A magnetometer is a type of sensor that measures the strength and direction of the local magnetic field. Occasionally, if iSavi™ is in close proximity to ferrous objects, the sensors will have difficulty determining its correct orientation. When this happens, the LEDs will flash in the Magnetic Inteferece status while the magnetic interference message will be appeared on the IsatHub Control app.

The compass may need to be calibrated from time to time, it is called magnetometer calibration.

Navigate to **Settings >Calibration** to perform magnetometer calibration to your iSavi™.

1. Click on the **Start** button and check the 'left' and 'right' of the Antenna Pointing LEDs are flashing in green.

Calibration iSavi™

Magnetometer Calibration

Start

1. Turn your device at least one round in the left/right direction (Y-axis).
2. Hold your device upright and turn it at least one round in the left/right direction (X-axis).
3. Verify calibration data.
4. Calibration completed.

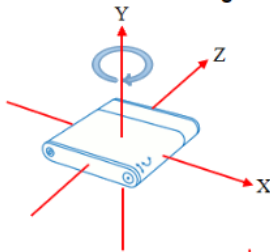
2. Rotate your terminal in a clockwise direction around the Y-axis.

Calibration iSavi™

Magnetometer Calibration

Recalibrate **Stop**

➡ 1. Turn your device at least one round in the left/right direction (Y-axis).



2. Hold your device upright and turn it at least one round in the left/right direction (X-axis).
3. Verify calibration data.
4. Calibration completed.

15%

Note:

The number of rotation is depending on the strength of the magnetic interference.

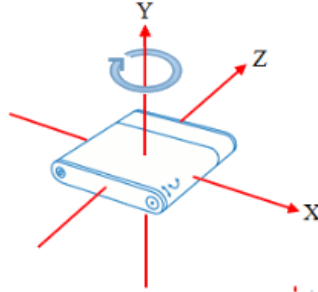
Calibration iSavi™

Magnetometer Calibration

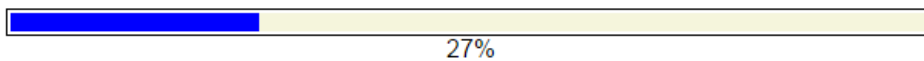
Recalibrate

Stop

1. Turn your device at least one round in the left/right direction (Y-axis).



2. Hold your device upright and turn it at least one round in the left/right direction (X-axis).
3. Verify calibration data.
4. Calibration completed.



3. Once the Y-axis calibration has been completed, check that the 'left' and 'right' LEDs remain steady green and the 'up' and 'down' LEDs are flashing green.
4. Rotate the terminal in a clockwise direction around the X-axis.

Note:

The number of rotation is depending on the strength of the magnetic interference.

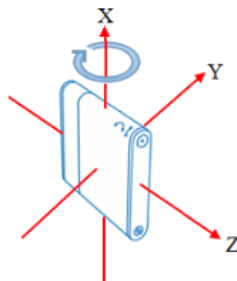
Calibration iSavi™

Magnetometer Calibration

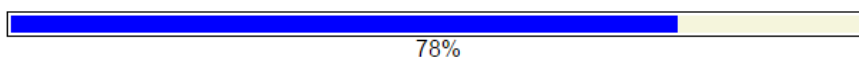
Recalibrate

Stop

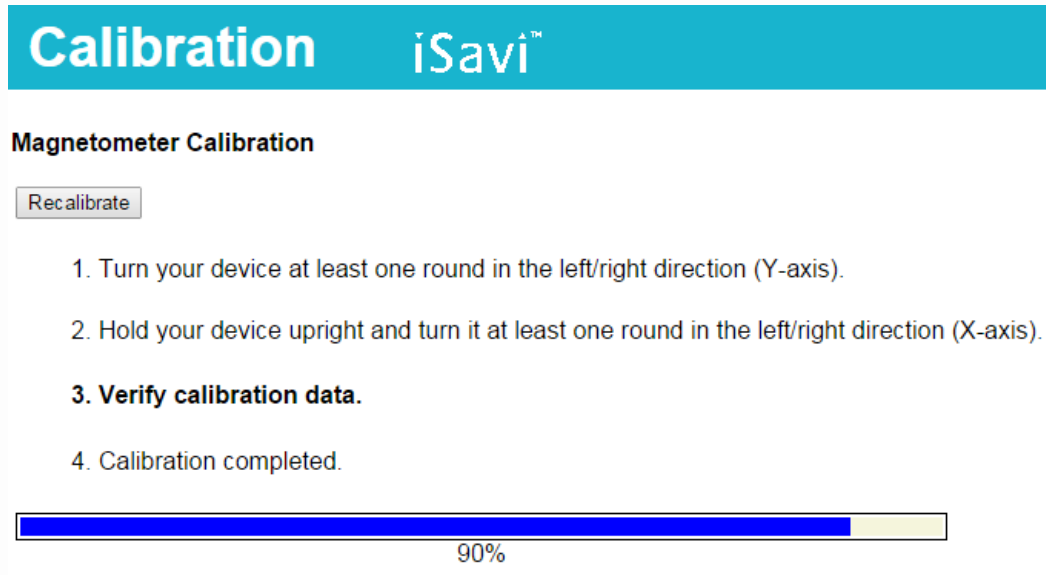
1. Turn your device at least one round in the left/right direction (Y-axis).
2. Hold your device upright and turn it at least one round in the left/right direction (X-axis).



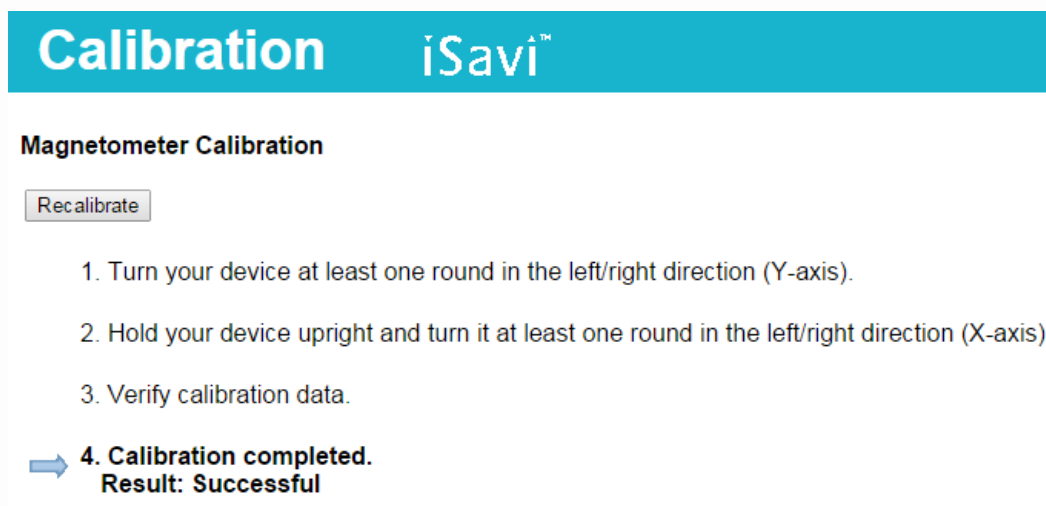
3. Verify calibration data.
4. Calibration completed.



5. Once the X-axis calibration has been completed, check that all the four Antenna Pointing LEDs display in steady green.
6. Once the calibration is completed, check that Verify Calibration Data is displayed. All the four Antenna Pointing LEDs are flashing green.



7. Once the verification is completed, check that the message "Calibration completed. Result: Successful" is displayed.



- 8 . If the message “Calibration completed. Calibration failed! Please change your existing location and recalibrate again” displays, repeat the procedure. Click **Recalibrate**.

Note:

Failure of the calibration can be caused by magnetometer interference from the surrounding area. You need to change to a new location for recalibration process.

Calibration iSavi™

Magnetometer Calibration

Recalibrate

1. Turn your device at least one round in the left/right direction (Y-axis).
2. Hold your device upright and turn it at least one round in the left/right direction (X-axis).
3. Verify calibration data.
- ➡ **4. Calibration completed.**
Calibration failed! Please change your existing location and recalibrate again.
Error: 3

ACCESS SAFE MODE THROUGH MICRO USB CONNECTION

The Micro USB connection is designed as a secondary method to access the Safe Mode. It provides a physical connection from our computer to iSavi™.

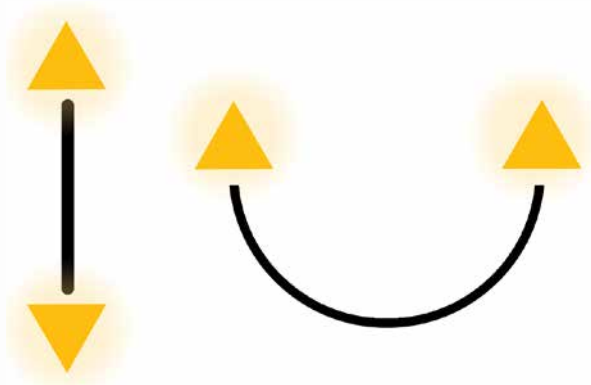
To establish the Micro USB connection, driver installation is required to the PC for the first time set-up.

Note:

Micro USB connection is only design for Safe Mode purpose.

Install Micro USB driver for Windows XP and Windows 7

1. Ensure the Safe Mode is enabled successfully, with all the four Antenna Pointing LEDs in Amber colour, refer to page 63, Appendix A: Antenna Pointing LED Status Table.



2. RNDIS USB driver file is available on the USB drive which is included in the iSavi™ packaging box. You are required to copy the file into your personal computer (Windows XP or Windows 7).
3. Unzip the attached file and select the .inf as the driver file
4. Connect the Micro USB cable to your personal computer.
5. The USB installation should complete with a new network adapter created as USB Remote NDIS device.
6. Disconnect or remove any physical Ethernet/ Wi-Fi connections of your personal PC and leave only the Micro USB cable which is connected between your personal computer and your iSavi™.
7. Log in to Web Console by typing <http://iSavi> or <http://192.168.1.35> into the address bar of any web browser. Proceed the firmware upgrade steps as normal (refer to page 39).

Note:

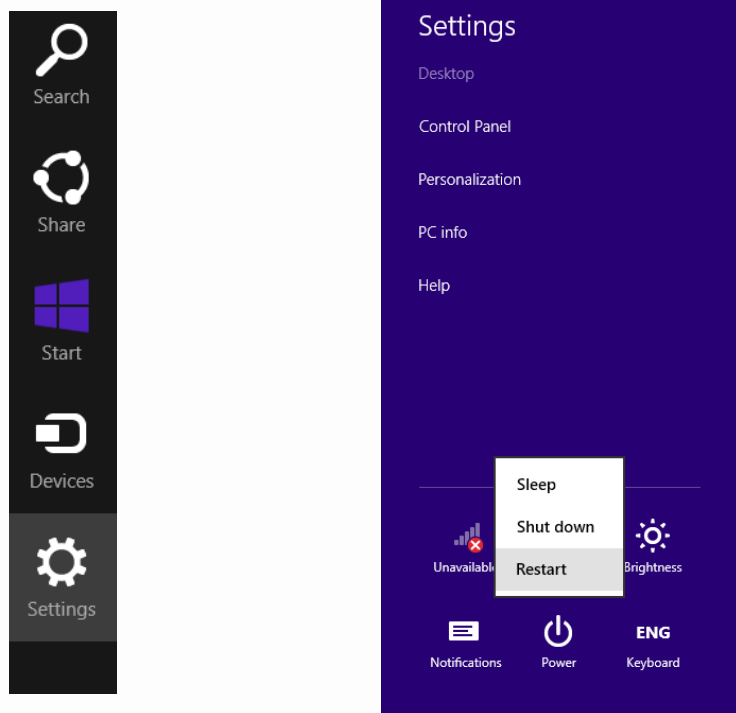
Ensure the battery level is at least 75% before performing the firmware upgrade or have the terminal on charge.

You are recommended to perform the firmware upgrade through Wi-Fi connection. Firmware upgrade through Micro USB is only required when the firmware is corrupted.

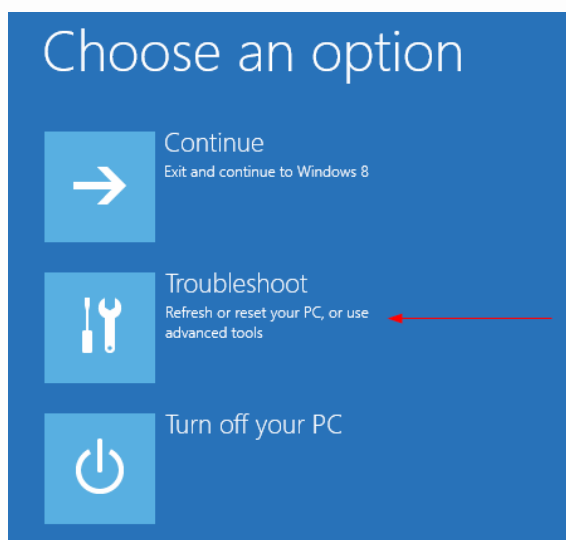
Install Micro USB Driver for Windows 8

How to Install an Un-Signed 3rd Party Driver for Windows 8

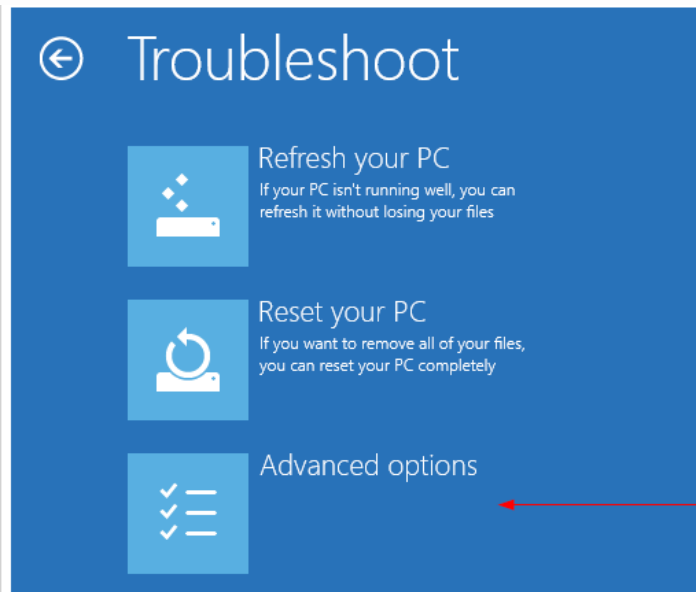
1. Navigate to **Settings**.
2. Press and hold the SHIFT key on the keyboard and click **Restart**. The PC reboots to the Advanced Startup menu.



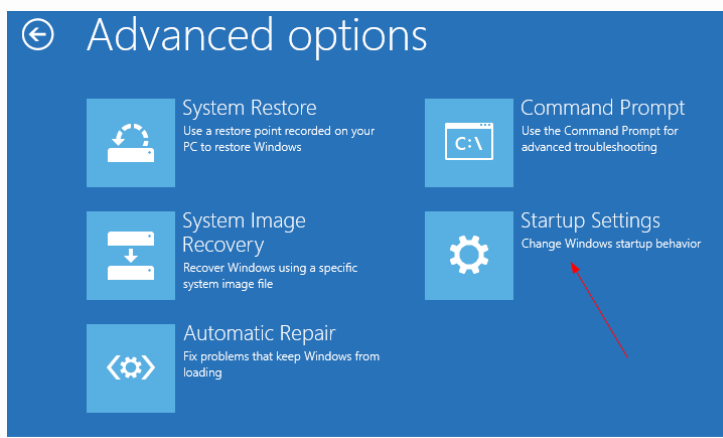
3. Your computer will restart. Select **Troubleshoot** from the list.



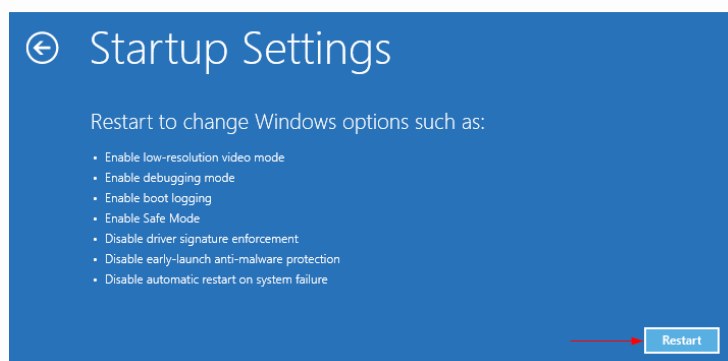
4. Select **Advanced Options** from the next screen.



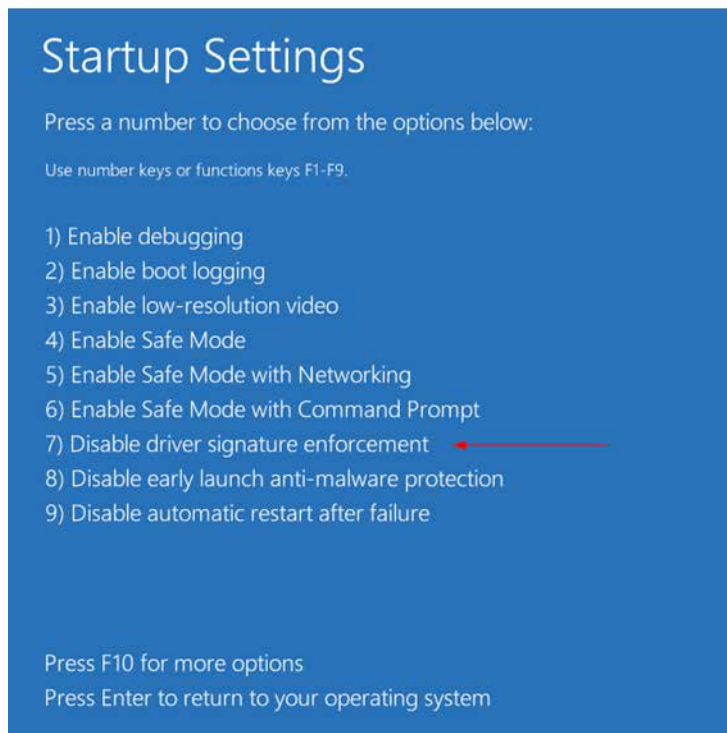
5. Select **Startup Settings**.



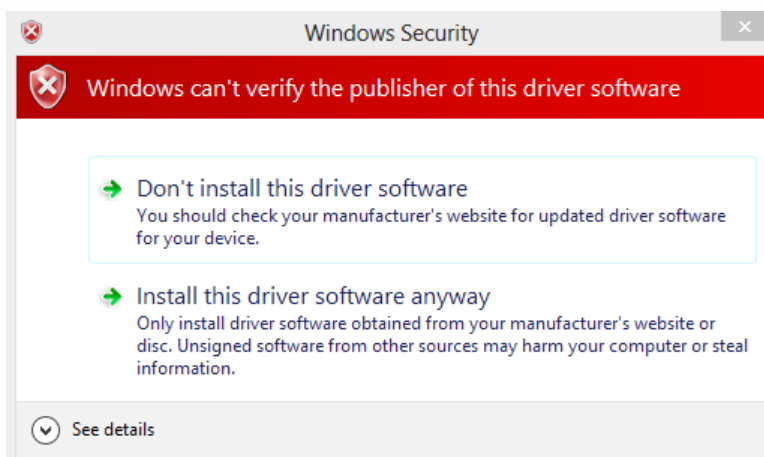
6. Select **Restart** button.



7. Your computer reboots and the Startup Settings menu is displayed for selection.
Press number **7** or **F7** to continue booting to Windows 8 with the digital sign enforcement disabled.



8. Windows Security dialog box is displayed. Select **Install this driver software anyway**.



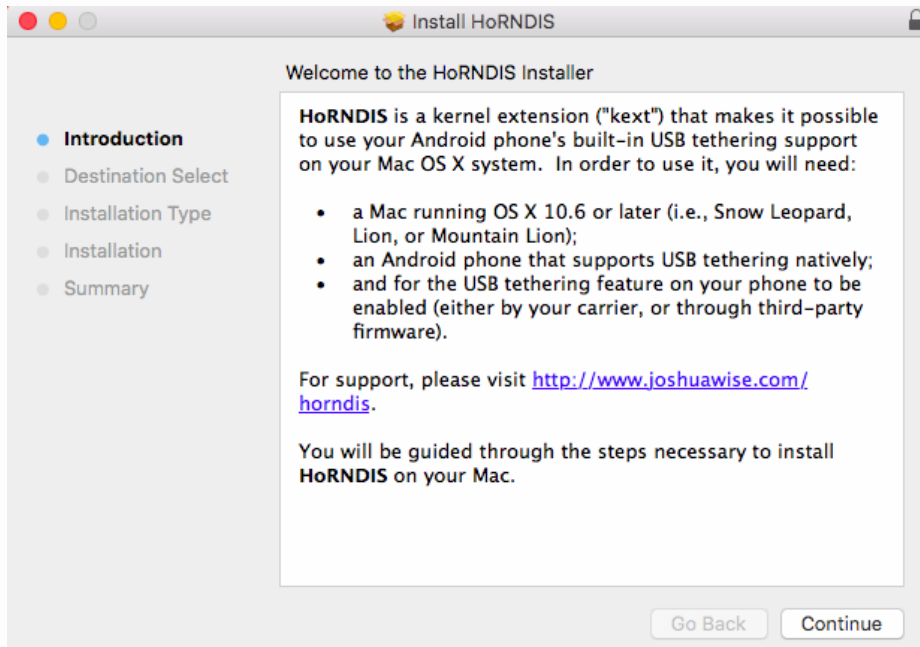
The driver is installed successfully now.

IMPORTANT:

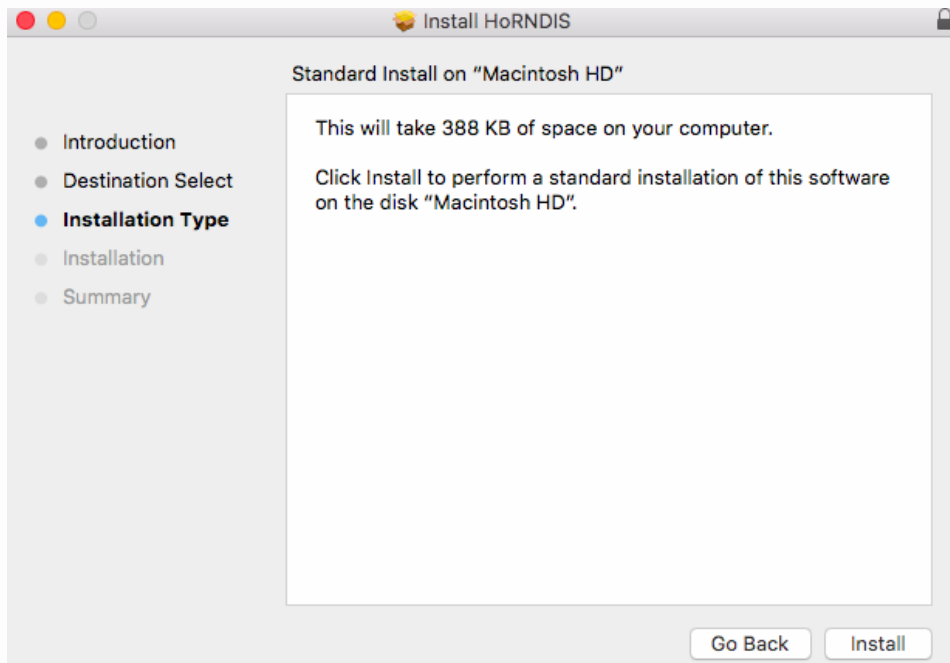
Once the driver is installed, restart your computer once again and go through the steps to re-enable the digital sign enforcement.

Install Micro USB Drive for Mac OS X

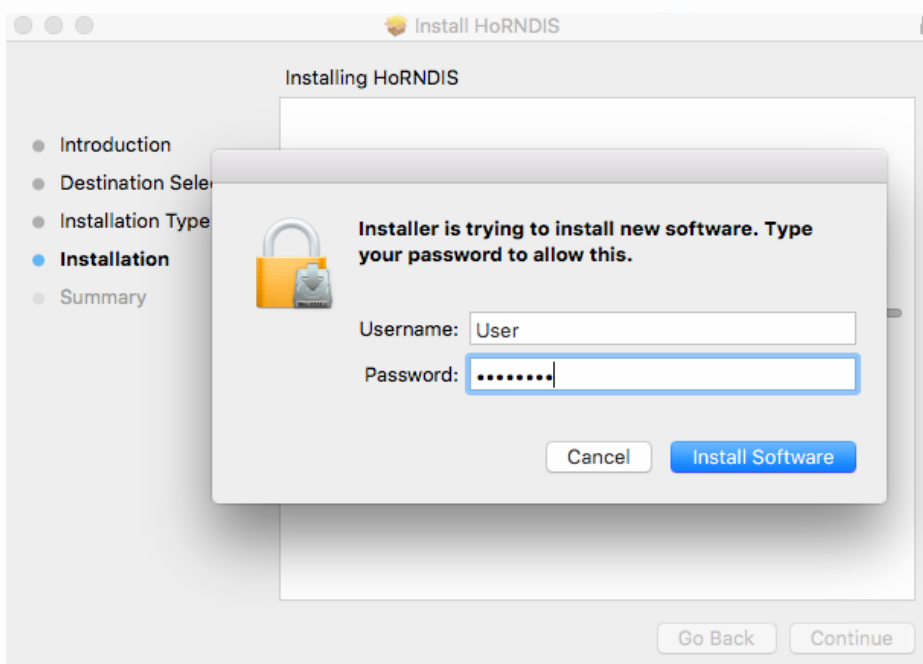
1. Download the latest HoRNDIS driver from the internet.
2. Launch the HoRNDIS driver. An Introduction window will be displayed. Select **Continue**.



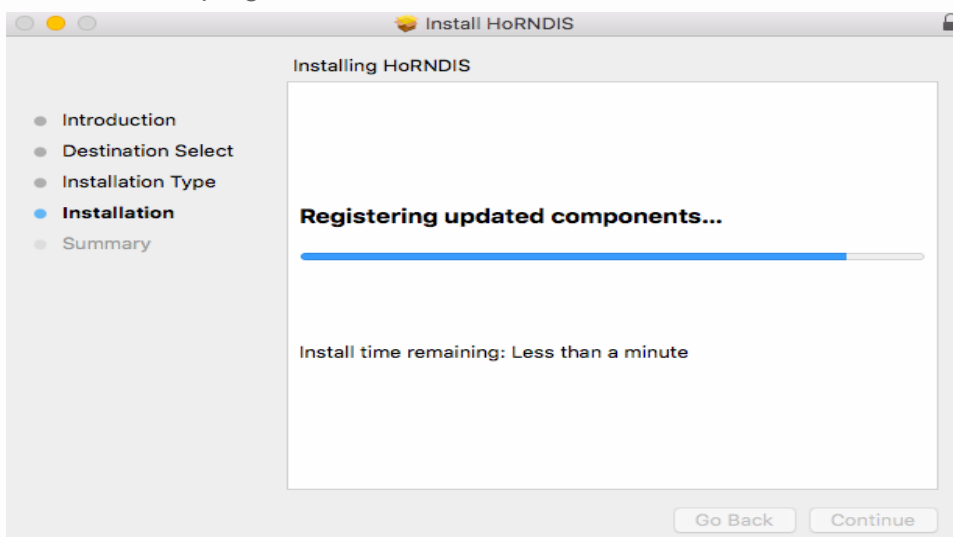
3. Select **Install**.



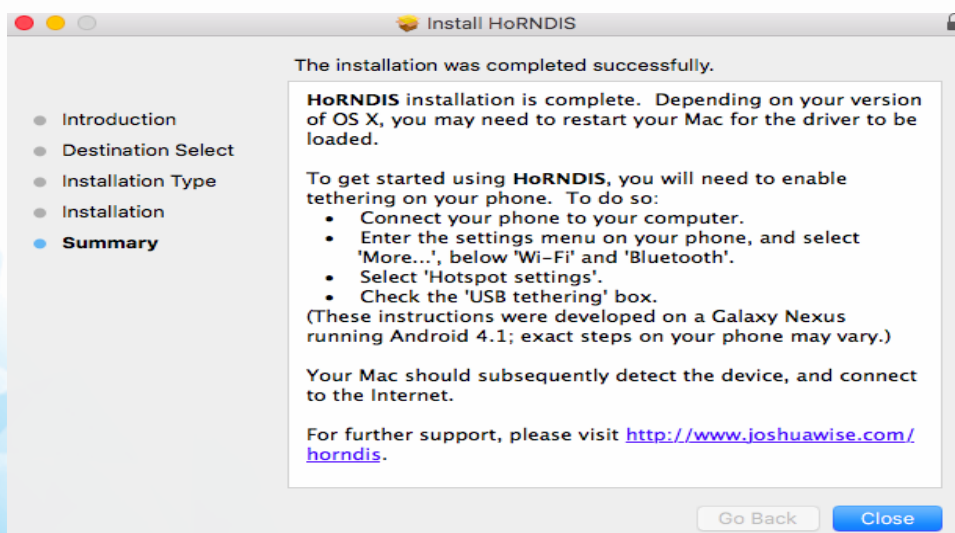
4. Type your Mac PC password to allow the installation.



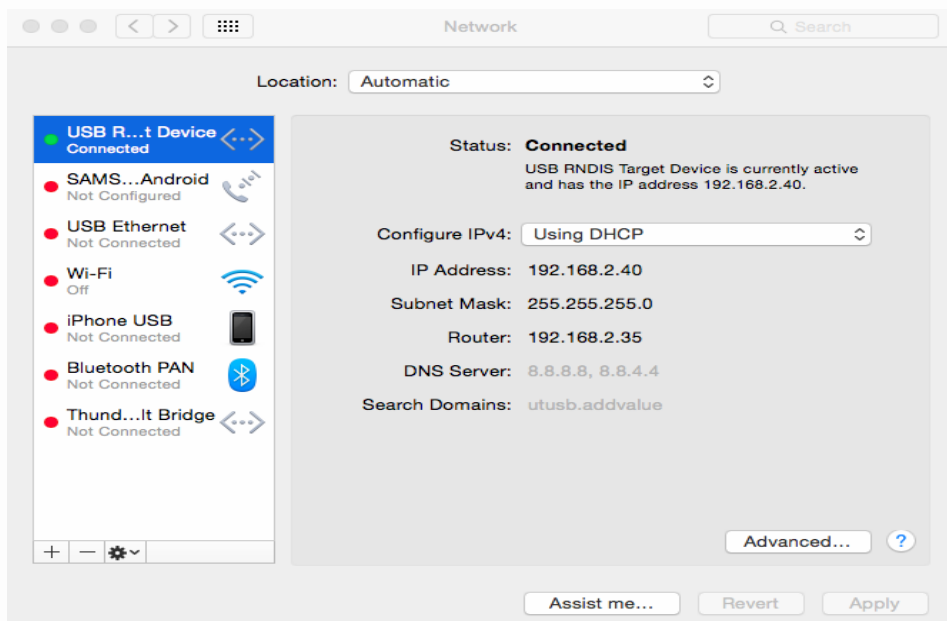
Installation in progress.



Installation is completed successfully.



5. Disconnect or remove any physical Ethernet or Wi-Fi connections of your Mac computer.
6. Ensure the safe mode is enabled successfully for iSavi™. Connect the Micro USB cable from iSavi™ to the Mac computer.



7. Refer to page 38, Web Console in Safe Mode to have more information.

DATA ACCESS AND COST MANAGEMENT

There are five methods to optimize the data usage.

User are highly recommended to read through all the methods and apply them to minimize the data usage.

Method 1: IsatHub Control app

STEP 1

Download the IsatHub Control app from the iOS App Store or Google Play on your smart devices.

STEP 2

Open the IsatHub Control app on the smart phone or tablet.

STEP 3

Access Right Management

Manage the data access right, incoming and outgoing call access right by device basis.

TIP 1: IsatHub Control app has a built-in data counters which can monitor how much data is used by each connected devices. The value of the data usage is indicative, there might be slightly different in the IsatHub Control app and the Web Console. The real data usage should not exceed those indicative values.

STEP 4

Data Counters and Alert Messages

You can set a predetermined threshold to limit the overall usage of the terminal. An alert message can be set to notify you when data usage is reaching the data limit

TIP 2: There is a Service Control SMS features that allows the Inmarsat Distributor Partners to send a free format message directly to the iSatHub users for the information of data usage, billings or other customer care related notification.

TIP 3:

After registered successfully to the network, you can make calls or send text message through the Voice app. Data connection do not need to be activated. This can save the data usage and improve the battery standby time.

Method 2: iSavi™ Firewall

Your iSavi™ has a built-in firewall feature which allows you to select the firewall profiles.

The access right given to an Admin or a User might be different for firewall configuration. These firewall settings apply to all the connected devices.

There are four firewall profiles available: Email only, All Internet, Custom 1, and Custom 2.

Custom 1 and Custom 2 are meant for customization purpose.

The customization can only be done by the Admin through the Web Console.

By default, it blocks everything from the internet for Custom 1 and Custom 2.

Below are the details of the default settings.

Firewall	Email Only (SMTP, IMAP, POP3)	All Internet	Custom 1	Custom 2	Description
Mail					
SMTP	Yes	Yes	No	No	Send email, using Thunderbird, Outlook (not MS exchange) or encrypted connection.
IMAP	Yes	Yes	No	No	Receive Email using IMAP4.
POP3	Yes	Yes	No	No	Receive Email using POP3
Browsing					
HTTP	No	Yes	No	No	Basic Browsing protocol
HTTPS	No	Yes	No	No	Secure Browsing protocol
FTP					
FTP control	No	Yes	No	No	FTP control session
FTP Data	No	Yes	No	No	FTP Data session
ICMP	No	Yes	No	No	Ping, Tracers

TIP 1: As a part of out-of-box sequence, IsatHub Control app will requests the users to set up the firewall access level.

Note:

It is not technically possible for the firewall settings to differentiate and block certain data usage.

Example, application updates, OS backups, Cloud access, etc.

Therefore, users are recommended to change the settings of the smart devices and the computers.

Refer to next page for more details.

Method 3: Smart Devices Settings

Smartphones and tablets offer a rich experience with many applications and services that frequently connect to a cloud or the Internet. However, when users access data through a satellite connection, it is important that the most relevant applications are prioritised in order to avoid unwanted satellite cost. There are a number of things users can do to make the most efficient use of their data access.

Common steps for both iOS and Android devices:

1. Browse mobile sites instead of full desktop sites.
2. Disable all auto updates.
3. Disable push email.
4. Switch off push notifications and disable background application refresh through iOS setting (iOS) or device settings (Android).
5. Switch off iCloud backups (iOS) or Cloud backup (Android).
6. Switch off photo uploading to iCloud(iOS) or any cloud service.
7. Use powerful web browsers which have capability to resample images and make the size smaller.
8. Switch off browser image for downloading.
9. Install Ad blocking program to block advertisement for unnecessary data usage.

TIPS for iOS

- You can use iOS Restrictions settings for application specific access management.
Refer to <http://support.apple.com/kb/ht4213>
- You may also download the monitoring applications for iOS which can provide the information about Wi-Fi data usage

TIPS for Android

- You can download an application that helps to shut down unnecessary applications running at the background.
- You may also download the monitoring applications for Android which can provide the information about Wi-Fi data usage
- There are commercially available firewall applications for Android which can be used for detailed access control.

Method 4: Computer Settings

There are few options to minimize the data usage:

1. Disable automatic OS updates and auto downloads when possible.
2. Configure the email client setting to download only the E-mail headers (Example: Outlook).
3. Use the basic HTML web email (Example: Outlook Web mail).

Windows 10 does not give owner the option to disable all the Windows 10 updates. It is not advisable to connect a satellite terminal to a Windows 10 computer since any data transferred over the satellite network is billed.

TIP 1: Do not leave a connected device unattended.

Some web pages will be refreshed when unattended. It is better to disconnect the device from your iSavi™ terminal to ensure that no data is transferred over the satellite connection. You may also turn off your iSavi™ if you do not expect a phone call over it.

Method 5: Network Support

Inmarsat network support basic data compression.

- The communication going from a satellite to ground is called downlink, and when it is going from ground to a satellite it is called uplink. The TCP / PEP with a downlink to the terminal improve the performance of downloaded data. Through a PC client on the user's laptop, PEP can perform a compression and reduce over-the-air data. Currently, the client software is only available for Microsoft Windows and Apple OSX. It can be downloaded from the Inmarsat website.
- Inmarsat Distributor Partners (DP) might be able to provide further compression technology for the users. In addition, the DP might also provide tailored services for the users (Example: firewall service.)

06 TROUBLESHOOTING AND FAQ

1. iSavi™ does not turn on successfully.

- Check if the battery is attached correctly, and then press and hold the Power Button for 5 seconds.
- Check if the battery level is low. Supply power to the terminal using power adapter as needed.

2. How do I turn off iSavi™?

Press and hold the Power Button for 5 seconds.

Note: Do not remove the battery when power down iSavi™ otherwise the terminal logs will not be saved .

3. When can I turn off iSavi™?

You can turn off iSavi™ when the Power button LED turns solid green or solid red.

4. Where can I check the default SSID and password of the Wi-Fi connection?

The information is available on the product label below the serial number. The same label is available on the packaging box.

5. LED Status indicates SIM card is not detected.

Power button LED is red. Ensure that a correct SIM card is inserted before you turn on iSavi™. iSavi™ is compatible only with an Inmarsat IsatHub or the BGAN SIM card.

Connect to Web Console to check for the error statements. The error statement will show if the SIM card is not inserted, SIM PIN entry is required, or the terminal PIN entry is required.

Contact your service provider if you are unable to solve the problem.

6. Where can I check the IMSI (SIM card number) of iSavi™?

In the Control app, navigate to **Setting > About**.

Alternatively, in the Web Console, navigate to **Setting > Terminal Info > Information** to check the details of the terminal (Serial Number, IMEI, IMSI number). It is suggested you record the iSavi™ IMEI number and SIM card number when you first use the device.

7. My iSavi™ and/or SIM card have/has lost or stolen.

With the detailed information as written on FAQ 6, contact your service provider as soon as possible so that the iSavi™ and/or SIM can be barred.

8. I cannot connect to the Wi-Fi.

Ensure that both the Wi-Fi SSID and password are correct. Disable 3G or 4G service from your smart devices, and then try to connect to the Wi-Fi again. The password is case-sensitive. If your password has uppercase or lowercase letters, they must be entered in the appropriate case.

9. Where should I place the terminal for the best results?

Make sure iSavi™ is placed outdoor with a clear, unobstructed view of the sky. To acquire GPS, power on iSavi™ and place the terminal flat on the ground, facing the sky. Leave it for approximately one minute. Once the GPS coordinates have been acquired, iSavi™ will automatically trigger the LED Visual Pointing Mode for optimal signal strength (refer to LED Status Quick Reference Guide). The GPS fix status can now be found in the Web Console.

Refer to Appendix A: Antenna Pointing LED Status Table for the LED's displays.

10. GPS is not available after time-out.

Press and hold the Power Button for 5 seconds to turn off iSavi™. Repeat the procedure as describe on FAQ 9.

11. Magnetic interference detected.

There are 3 methods for antenna pointing. To continue using LED Visual Pointing Mode, move your iSavi™ to a new location. Ensure iSavi™ is placed outdoor and away from any electrical devices, metal objects, or appliances that generate RF noise, in the unobstructed view of the sky. Press the Exit Pointing Mode Button once to return back to LED Visual Pointing Mode, and then repeat the set up procedure.

Use the Audio Assisted Pointing Mode with its beeping frequency to indicate its signal strength. Refer FAQ 12 to learn how to switch to the Audio Assisted Pointing Mode.

You can also perform the antenna pointing method by using the Control app. Follow the on screen instructions and press 'Pointing assist' for its specific help. Adjust until you get the optimal signal strength and register to the network from the Control app.

12. How do I switch to Audio Assisted Pointing Mode?

By default, iSavi™ is in LED Visual Pointing Mode. To switch to the Audio Assisted Pointing Mode, press and hold the Exit Pointing Mode Button for 5 seconds.

Note: iSavi™ will automatically default to the LED Visual Pointing Mode whenever you reboot iSavi™.

13. Azimuth and elevation are correct, but global beam (satellite signal) is not available.

Ensure that there is no blockage between iSavi™ and the Inmarsat satellite. There must be a clear line of sight between the iSavi™ and the satellite. Shift the location of your terminal until the Exit Pointing Mode LED shows flashing green. This indicates that the global beam (satellite signal) has been detected.

Alternatively, you can switch to Audio Assisted Pointing Mode. Refer to FAQ 12. Beeping frequency is the indicator for the signal strength. The frequency of the beeping will become higher when the signal is stronger.

14. Network Registration failure.

Press and hold the Exit Pointing Mode Button for 3 seconds to repeat the LED Visual Pointing Mode procedure again to attempt the network registration. Contact your service provider if you are unable to solve the problem.

15. iSavi™ terminal is registered to the network but failed in data activation.

- iSavi™ needs a signal strength of at least 42dB to perform at an acceptable service level. Check the signal strength of your iSavi™ on the Control app or Web Console. If the signal strength is below 42dB, power down the terminal and repeat the set up procedure again.
Note: Make sure you have signal strength of at least 42dB during set up.
- If you have a prepaid subscription, check your balance to ensure you have sufficient credit to make a data connection. Check the APN settings on the Data Profile under Data via the Web Console. By default, the APN settings should be read from the SIM card unless you have specified to use another APN instead of the one defined on the SIM card.

16. No internet access even though data connection is activated.

- Make sure there is no problem with the Wi-Fi connectivity. Verify that the Wi-Fi signal of your smart devices or personal computer is good.
- Check the firewall settings to ensure that it does not block the required internet (IP) access.

17. All LEDs are off after the terminal registered to network. How do I check the terminal's status?

You can check the LED status by pressing the Exit Pointing Mode Button once. Please refer to LED Status Quick Reference Guide. Alternatively, you can check the status via the Web Console or Control app.

From the Web Console, navigate to **Setting > Terminal Settings > Antenna Pointing LED Configuration** in order to change the LEDs settings to Always On (Antenna Pointing LED). Click **Update** for the new settings to take effect,

18. Web console cannot receive a SMS.

Maximum SMS storage is dependent on the SIM card memory. If the memory is full, delete text messages to free up memory for new SMSs. Text messages cannot be sent to and from some service providers who do not have an interconnect agreement with Inmarsat. Please try another network or use the Inmarsat website tool to send the SMS.

Sending or receiving SMSs through the Voice app does not leave a copy in the SIM card for privacy reason. Disconnect the smart device with Voice app if you want to receive the SMS through Web Console. Web Console can receive the next SMS once the Voice app is disconnected to the terminal,

19. I am having a problem in accessing the Web Console.

Check that there is no problem with the Wi-Fi connectivity. Make sure that the hostname is entered correctly: **http://iSavi** or **http://192.168.1.35**.

20. I cannot enter "Safe Mode".

With the terminal powered off, first press and hold the Exit Pointing Mode Button, and then press and hold the Power Button. Release both Exit Pointing Mode button and the Power button after 5 seconds simultaneously.

21. Firmware upgrading failure.

A firmware upgrade failure is due to using an incorrect upgrade package file. Check that the correct firmware upgrade package has been selected. Unzip the firmware package file before you select the file for firmware upgrade.

You can refer to **www.wideye.com.sg**. The latest firmware is available under **Support > Downloads**. Failure can also be due to an interruption of the power supply during firmware upgrade. If the firmware upgrade is unsuccessful, repeat the procedure through Safe Mode using the Micro USB cable that bundled with iSavi™.

22. Problem with incoming / outgoing call.

Verify that the Wi-Fi signal of your smart devices or personal computer is good. You are recommended to stay within 5 metre to your iSavi™ during the calling session.

Check that the Voice app status shows "Phone Ready". If it shows "Registering..", check your Wi-Fi connection to ensure that your iSavi™ is connected to the smart phone or the tablet. Check that the number format you dialled includes the full international prefix. Verify whether the correct access right is given to the smart devices (incoming / outgoing call functionality).

If you have a prepaid subscription, check your prepaid balance to ensure you have sufficient credit to make a call.

23. How do improve the incoming / outgoing call quality?

Verify that the Wi-Fi signal of your smart devices or personal computer is good. You are recommended to stay within 5 meter to your iSavi™ during calling session.

Navigate to **Telephony > SIP setting > SIP Server** to change the RTP Codec.

The RTP codec is an audio encoding. The quality of the voice is dependent on your smart devices.

You may change the RTP codec for better voice quality.

24. Where do I download the Quick Start Guide, User Guide and LED Status Quick Reference Guide?

You can get these documents from **www.wideye.com.sg**. Navigate to **Support > Downloads > User Guides**.

25. What should I do if I have forgotten the admin password?

New temporary login password is required to unlock the iSavi™ terminal.

Contact your service provider.

With SIM Card inserted, power on the terminal with the AC adapter connected.

Open any web browser with **http://isavi** and log in with the following information.

Username: admin

Password: (leave it blank)

Click **Log in**.

A token pin code will be generated. Email the token pin code to your service provider within 24 hrs. As an anti-theft procedure, Wideye technical support team will only provide the temporary admin password to your service provider.

Log in web console using the given temporary admin password.

Initiate a factory reset through **Settings > Terminal Settings > Factory reset** (enter code 0000) to reset the admin password to a default value.

The token is valid for 24hrs for iSavi™. Customer is expected to perform a “Factory Reset” once they gain temporary access to the Web Console.

Note:

Check that iSavi™ is powered on the entire time until the temporary password is generated and entered, since a different token pin code is generated at every power cycle. The token pin code is valid for 24hrs for iSavi™. Customer is expected to perform a “Factory Reset” once they gain temporary access to the Web Console.

26. How do I send text messages using the Voice app?

Login to the Control app before using the Voice app to send or receive SMSs.

27. Control app or Web Console is disconnected during login session.

Control app or Web Console is the user interface for configuration settings of your iSavi™. It is designed to allow only one control device to login to the Control app and another control device to login to the Web Console at the same time.

When a first device is logged into the Control App or the Web Console, it will automatically be disconnected when you use a second device to login to the user interface.

Note: The Control app and the Web Console are limited to one control device to be connected at any one time. Multiple devices can simultaneously access all other functions of your iSavi™.

28. What is the safety distance to prevent radiation from the terminal?

For safety reason, never stand closer than one metre in front of your iSavi™ terminal's transceiver when it is connected to the network.

29. The LEDs status indicates the SIM is not detected.

If Terminal PIN and / or SIM PIN are/is enabled, the Power Button LED will turn red. Connect to the Wi-Fi connection as usual. You have to login to the Control App or Web Console to enter the PIN.

30. My iSavi™ is having some abnormalities. Can someone help to investigate my problem?

Save and send the "System Logs" to your service provider by following the steps below:

1. Click Settings at the top of the Web Console.
2. Click Terminal Info.
3. Scroll down after you select Logs, and then Click Export All Logs.
4. Save and send both the System Log files – (SystemLogs_2014120322xxxx.csv file) and (System Logs - SystemLogs_2014120322xxx.bin file) to your service provider.

31. How to install the micro USB drivers of iSavi™

Micro USB connection is designed only for the safe mode access purpose.

You install Micro USB driver in your computer only at the first time connection.
Method of installation is similar to any other driver files based on your computer OS.
You may contact your service provider if you cannot install the driver successfully

32. My iSavi™ is displaying “ +CME ERROR: 15 ”.

This error indicated that the SIM card used is wrong.
If you are using BGAN SIM, you can relate it with the firmware version of the terminal.
BGAN SIM card is only compatible to the firmware version R01.1.0 onwards.
You can verify the firmware version by using the Safe Mode option.

33. My iSavi™ is displaying “ +CME ERROR: 529 ”.

This error indicates the user authentication is failed.
The APN username and/or password are incorrect. Please check the APN settings on the Data Profile through Web Console. You obtain the APN username and password from your service provider. Contact your service provider if you are unable to solve the problem.

34. My iSavi™ is displaying “ +CME ERROR: 539 ”.

In general, this error shows because the signal is weak for the activation of a PDP context or due to the network congestion.
CME 539 can also denote that the Satellite connection was lost and a new connection needs to be established. It usually occurs when there is any partial blockage of the signal.
You are recommended to check whether there is blockage and shift the unit to a better line of sight location.

35. I could not find the magnetometer calibration option in Web Console.

This option is only available in "Safe Mode". Switch the terminal to Safe Mode.
Navigate to **Settings > Calibration** to perform magnetometer calibration to your iSavi™.

36. What is really the maximum power required if the battery is empty and my iSavi™ need to be operated and charged at the same time?

The input DC voltage of iSavi™ can be between 15VDC and 20VDC.

Depending on the input voltage you supply multiplied by the supplied current needs to be equal to or greater than 20 watts to run the iSavi unit and 50 watts to run the iSavi unit and also charge the battery.

Addvalue recommend that for a full load (transmitting at full capacity and charging the battery at the same time) the charger or panel should be capable of providing 65 watts

Note: Battery pack draws up 1.5A from 18V source when charging.

37. Can I use a smaller solar panel to charge iSavi™?

iSavi™ terminal can be charged with a Solar Panel delivering around 30 watts at 18 VDC, which means that the battery will take a bit longer to charge. The charging speed will be faster if you charge the battery alone without attaching to the transceiver.

38. Can I use iSavi™ in the rain?

iSavi™ is having the ingress protection rating of IP65, which means it is protected from dust ingress and low pressure water jets from any direction. However, under charging condition, you need to protect the terminal from the rain or water contact.

39. What is the recommended configuration for DTMF type (IsatHub Voice app)?

DTMF is sent when you press a number key with an auto attendant (such as “press 1 for customer service”). By default, the voice app is configured under Inband DTMF .

SIP INFO has lesser packet lost and you are recommended to Send DTMF using SIP INFO.

40. iSavi™ points me to APAC satellite but I want to point to MEAS satellite. Is there a method for this?

Control App and LED Visual Pointing Mode methods always point you to the recommended satellite.

You can manually point to the satellite that you want based on the reference Elevation and Azimuth angle displayed at the home page of the Web Console.

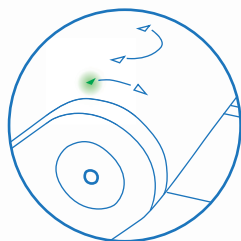
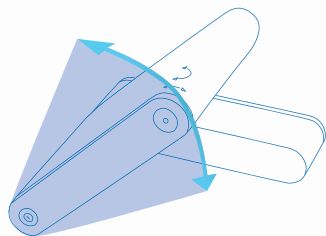
07 CARE AND MAINTENANCE

Caring for iSavi™

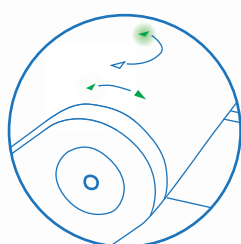
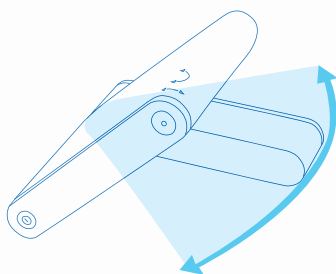
iSavi™ is a highly sophisticated electronic device. Complying with the following recommendations will help you to protect your warranty coverage and extend your terminal's life:

- Keep your terminal dry. Liquids or moisture can contain minerals that will damage electronic circuits. If iSavi™ does get wet, dry it with a soft absorbent cloth as soon as possible, remove the battery module and allow your transceiver and battery to dry completely before reassembling it.
- The connector covers are intended to protect your terminal. Keep these covers firmly closed at all times. Ensure that the connectors are free from dust or dirt before connecting any accessory. When closing the connector cover, ensure the area around the connectors, and the rubber sealing surfaces of the cover are clean and free from dirt. Ensure that the cover is fully closed to give maximum protection to your terminal.
- Do not store your terminal in dusty, dirty or damp areas as this may shorten its life.
- Do not store your transceiver and battery in extreme cold or hot areas exceeding a certain temperature range. Storage temperature range for the transceiver is -40°C to +80°C (-40°F to +176°F) whereas for the battery it is -20°C to +40°C (-4°F to +104°F). Extreme temperatures can shorten the life of your terminal and damage the battery.
- Your terminal's operating temperature range is -25°C to +55°C (-13°F to +131°F). The charging temperature range is 0°C to +40°C (+32°F to +104°F).
- Avoid regular use in high or low temperature environments. Lithium ion batteries have an optimal working and storage temperature. If they are continually used in an extreme temperature environment, it will negatively affect the battery's use time and useful number of recharging cycles.
- If you don't need to use iSavi™ for a long time where the lithium ion battery might be left unused for 3 months or more, partially recharge the lithium ion battery, then store the device (recharge the battery to around 30-70% of capacity) to prevent battery damage. You may need to take the device out of storage and charge again after a few months.

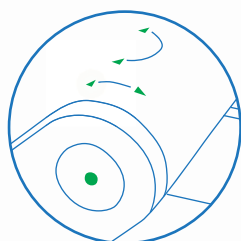
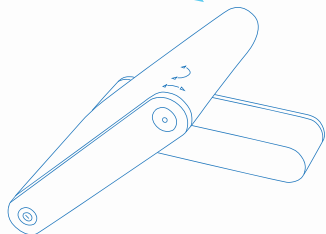
APPENDIX A: ANTENNA POINTING LED STATUS TABLE



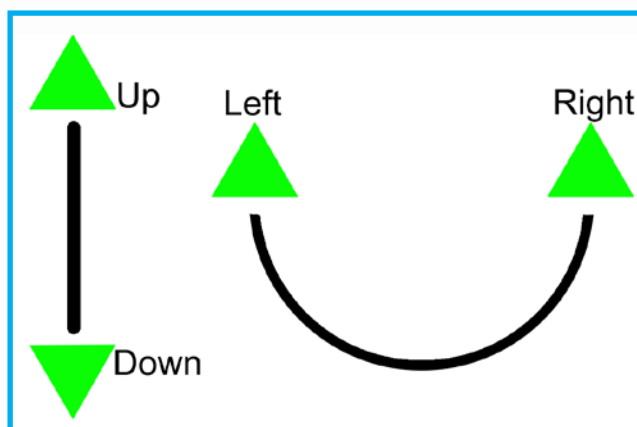
Tilt iSavi™ up or down in the direction of the flashing green light until both 'up' and 'down' LEDs are solid green.



Turn iSavi™ left or right in the direction of the flashing green light until both 'left' and 'right' LEDs are solid green.



When all four tilt & turn LEDs are solid green, press the flashing 'Exit Pointing Mode' Button. iSavi™ is now connected to the network.



LED Legend

* LED Flashing



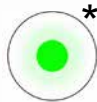


















† LED Flashing in sequence

State	Power Button	Antenna Pointing LEDs	Exit Pointing Mode Button	Actions / Status
OFF				Terminal is OFF.
Power On				Turn ON by pressing the Power Button for 5 seconds. The Antenna Pointing LEDs will turn on in Red / Amber for about 4 seconds, followed by all in Green for approximately 30 seconds before going into the next state.
Firmware Loading				Powering up in progress – this may last up to 30 seconds.
GPS Acquiring				This LED state (Antenna Pointing LEDs in Amber) is only applicable for first time fresh terminal setup. The GPS acquisition will take 30 seconds to 5 minutes depending on each setup location.
LED Visual Antenna Pointing				Tilt iSavi™ in upward direction (follow “Up” LED flashing green light). Stop when both “Up” and “Down” LEDs are solid green.
				Tilt iSavi™ in downward direction (follow “Down” LED flashing green light). Stop when both “Up” and “Down” LEDs are solid green.
				Turn iSavi™ in clockwise direction (follow “Left” LED flashing green light). Stop when both “Left” and “Right” LEDs are solid green.
				Turn iSavi™ in counterclockwise direction (follow “Right” LED flashing green light). Stop when both “Left” and “Right” LEDs are solid green.

LED Legend

* LED Flashing

† LED Flashing in sequence

Situation	Power Button	Antenna Pointing LEDs	Exit Pointing Mode Button	Actions / Status
Exit Pointing				All Antenna Pointing LEDs are solid green, Azimuth and Elevation are in correct positions. Press the flashing Exit Button once to exit Antenna Pointing mode and register to the network. Note: Pressing the Exit Button for 3 seconds will put iSavi™ into the alternative Audio Pointing mode.
Network Registering				Azimuth and Elevation are correct. Press Exit Button to exit Antenna Pointing and register to network.
Ready for Service				Network registration successful and ready for service. All LEDs will turn off after about 1 minute. Note: When all LEDs are off, you can always check the LED state by pressing the Exit Button once.
Data Activated				Data activated successfully through web console/ Control app. You can now connect your smart devices to iSavi™ terminal and start accessing the internet. Note: For LED status check, you can always press the Exit Button once.
Audio Pointing Mode ON-Global Beam available				Audio Pointing Mode is enabled. Satellite signal found.
Safe Mode				Safe Mode is enabled.
Powering Down				Pressing the Power Button for 5 seconds. The Antenna Pointing LEDs flashing red in sequence for approximately 30 seconds before turning off.






















LED Legend

* LED Flashing

† LED Flashing in sequence

Others LED Status

Refer to TROUBLESHOOTING AND FAQ on page 39.

Situation	Power Button	Antenna Pointing LEDs	Exit Pointing Mode Button	Actions / Status
SIM not detected				SIM card not recognized or SIM card not detected. Check whether correct SIM card is used. Enter SIM PIN / Terminal PIN in Web Console if the features is activated.
Audio Pointing Mode- Global Beam not available				Audio Pointing Mode ON- Global beam is not available
Network Registering failure				Network registering failure.
Global beam not available				Satellite signal is not detected. Ensure the antenna pointing direction is correct and no blockage in between the terminal and the satellite.
GPS not available				GPS not available (timeout). Ensure no blockage in between the terminal and GPS satellite.
Magnetic interference detected				Magnetic interference detected from the surrounding area. You need to change to a new location and press 'Exit Antenna Pointing' button once to exit from this status
Data activation failure				Data activation failure.

APPENDIX B: TECHNICAL SPECIFICATIONS

Operating Frequency

Satellite Transmit: 1626.5 – 1660.5 MHz and 1668 – 1675 MHz

Satellite Receive: 1518 – 1559 MHz

GPS Frequency: 1574.42 – 1576.42 MHz

Dimensions (L x W x H)	
Overall Terminal	
180 x 170 x 30 mm	7.09 x 6.69 x 1.18 in
Transceiver	
130 x 170 x 30 mm	5.12 x 6.69 x 1.18 in
Standard Battery Pack	
50 x 170 x 30 mm	1.97 x 6.69 x 1.18 in

Weight	
Overall Terminal	
880g	1.94lb
Transceiver	
620g	1.37lb
Standard Battery Pack	
260g	0.57lb

Environmental

Operating Temperature: -25°C to +55°C, -13°F to +131°F (with DC supply)
-20°C to +55°C, -4°F to +131°F (with battery)

Storage Temperature: -40°C to +80°C, -40°F to +176°F (Transceiver)
-20°C to +40°C, -4°F to +104°F (Battery)
-20°C to +40°C, -4°F to +104°F (Transceiver with battery)

Battery Charging Temperature: 0°C to +40°C, +32°F to +104°F

Storage Humidity: 95% RH (non-condensing at +40°C or +104°F)

Ingress Protection: IP65 Compliant

UV resistant

Services

Standard IP: Up to 240/384kbps (send & receive)
SMS: Using VoIP Apps or WebMMI; Standard 3G
(up to 160 characters, SMS larger than 160 characters are supported)
Voice Connectivity: SIP server using Apps on Smart Devices
Data Connectivity: Wi-Fi 802.11 b/g/n Access Point with internal Wi-Fi Antenna

Power Requirement

Power adaptor
input: 100 - 240 VAC
Output: +18VDC, 65 watt

Battery

Standard: 10.8V @ 3Ah Li-ion Battery Pack

ITEM	SPECIFICATION
Battery Type	Lithium ion, rechargeable
Nominal Voltage	10.8V
Standard Battery Capacity	3Ah
Charging temperature	0°C to +40°C
Operating temperature	-20 °C to +55 °C, -4°F to +131°F
Min. charge cycles	300
Storage Temperature	
1 month	-20 °C to +45 °C, -4°F to +113°F
6 months	-20 °C to +40 °C, -4°F to +104°F
1 year	-20 °C to +35 °C, -4°F to +95°F

APPENDIX C: INMARSAT COVERAGE MAP



I-4 and Alphasat coverage

