

Document No.: 222-UM-003

Document Type: User Manual

Security Level: Limited

S911 Enforcer Operation Manual

Version 1.1

January 03, 2023



Copyright Laipac Technology Inc.

Release History

Revision	Date	Content
1.00	2018/05/14	It is initial release
1.0.1	2019/02/28	Update
1.1	2023/01/03	Update about USB Charger Adaptor

1	Configuring the Enforcer	5
1.1	LocationNow Suite.....	5
1.2	A first Look at the LocationNow Suite User Interface	7
1.2.1	Operations menus	7
1.2.2	Device ID and Password	8
1.2.3	Retrieving and Saving the Configuration Data	9
1.3	Operation menu - File.....	9
1.3.1	Import Default File	9
1.3.2	Import file	10
1.3.3	Save file	11
1.3.4	Change password (Reserved)	12
1.3.5	Logout	13
1.4	Operation menu - Network	13
1.4.1	Wireless Service Setup	13
1.4.2	Communication Mode Setup	15
1.4.3	Web Service Setup	16
1.4.4	Emergency Call Set up	17
1.5	Operation menu - Functions.....	19
1.5.1	Report Interval	19
1.5.2	Time Zone	20
1.5.3	G-Sensor Alert	20
1.5.4	Geo-fence	21
1.6	Operation menu – Advance.....	23
1.6.1	Server Query	23
1.6.2	Special Functions	24
1.6.3	Audio	25
1.6.4	Voice on Demand Feature	25
2	Firmware Update.....	26
3	Using your Enforcer	28
3.1	Checklist for getting an Enforcer ready for use.....	28
3.2	Charging.....	28
3.3	Power On and Off.....	30
3.4	Introduction to the LCD Display Icons	32
3.5	Checking the Enforcer’s Operating Status.....	34

4	Enforcer Alert Functions.....	35
4.1	Tamper Alert.....	35
4.1.1	The Security-lock and its' open/close operation	35
4.1.2	Voice Reminder and Display Associated with the Tamper Alert	36
4.2	SOS Alert.....	36
4.2.1	A Unique Property of the SOS Alert	36
4.2.2	Voice Reminder of SOS Alert and False Alarm Cancellation	36
4.3	G-sensor Alert.....	37
4.3.1	G-sensor Alert Action Sequence.....	37
4.3.2	Cancelling False Alarm G-sensor Alerts.....	37
4.4	Geo-fence Alert	37
4.4.1	Home Geo-fence	38
4.4.2	Voice Reminder and LCD display coming with Geo-fence Alert.....	38
4.5	Wrong Pin Alert	38
5	Warning Statement	39
5.1	FCC.....	39
5.2	ISED.....	40
5.3	CE RED	41

1 Configuring the Enforcer

In order to use an Enforcer with a tracking service such as LocationNow.com, the Enforcer must be configured to communicate with the service. The LocationNow Suite utility software is used to configure the Enforcer.

For information on downloading and installing the LocationNow Suite software, please refer to the **S911 Enforcer Quick Start** document.

LocationNow Suite should have access to the internet, as the program will check for updates to the Enforcer's firmware when the program starts.

1.1 LocationNow Suite

(1) Click on the LocationNow Suite icon on your computer's desktop to run the utility; the screen shown in Figure 1-1 will be displayed.

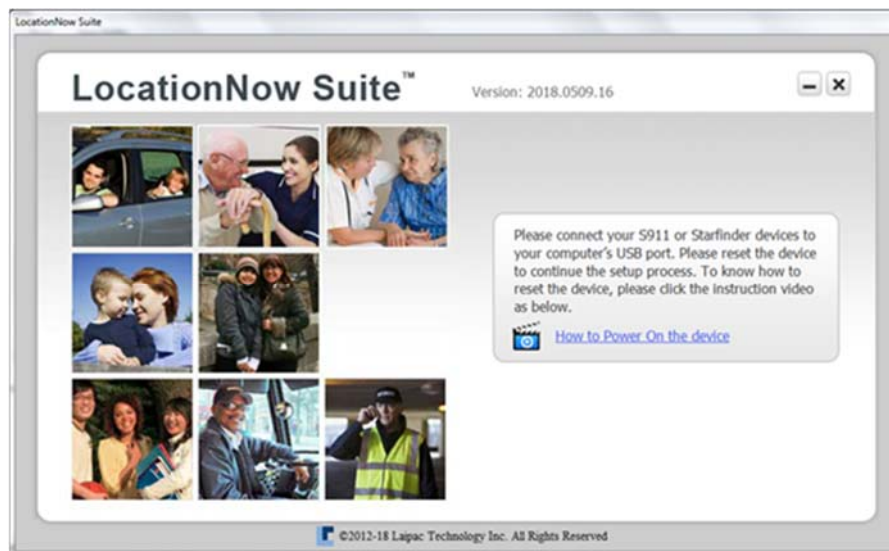


Figure 1-1: LocationNow Suite Start Up Screen

(2) Connect the Enforcer with the computer running the LocationNow Suite software using the supplied USB cable.

(3) If the Enforcer is on, power it off. Press the power on/off button for 3 seconds; the display will show TURNING OFF, and then go blank.


(4) Turn the Enforcer on; the Enforcer's LCD display will display USB CONFIGURATION and the  icon. On the computer side, the image in Figure 1-2 will be displayed.



Figure 1-2: Screen Confirming that Communication has been Established

(5) Click button Proceed to set up

If the screen shown in Figure 1-3 is displayed instead of the screen in Figure 1-2, it means that the utility has determined that there is a new firmware available for your Enforcer. For information on the firmware upgrade process, refer to chapter 2.

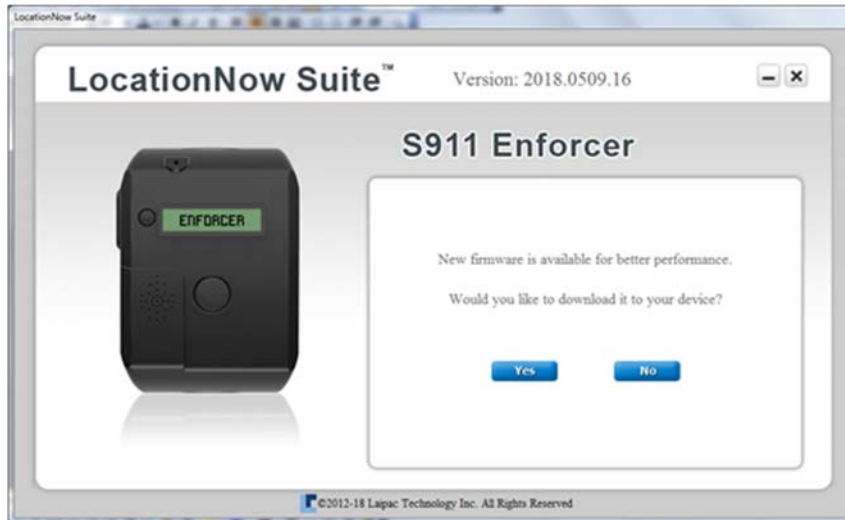


Figure 1-3: Firmware Update Screen

1.2 A first Look at the LocationNow Suite User Interface



Figure 1-4: The Network Setup Screen

When the LocationNow utility starts up, it reads the current configuration from the Enforcer. A popup at the bottom right of the LocationNow Suite window will report the success or failure of this operation.

1.2.1 Operations menus

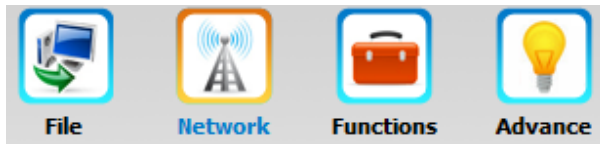


Figure 1-5: Setup Functions Selection Icons

The four operations menu pages in this utility:

- File
- Network
- Functions
- Advance

For details on each page, refer to sections 1.3 through 1.6.

1.2.2 Device ID and Password

A blue rectangular form with white text and input fields. It contains: 'Locator ID (IMEI): 351580050354816', 'Alternative Locator ID:' with an unchecked checkbox and a question mark icon, 'Password: 00000000', and 'Firmware version: 01.10.06'.

Figure 1-6: Using the devices 15 digit IMEI No. as the Device ID

A blue rectangular form with white text and input fields. It contains: 'Locator ID (IMEI): 351580050354816', 'Alternative Locator ID:' with a checked checkbox and an input field containing '12345678' and a question mark icon, 'Password: 00000000', and 'Firmware version: 01.10.06'.

Figure 1-7: Using an assigned 8 digit number as the Device ID

Device ID

Every locator requires a unique Device ID to be used when communicating with the monitoring server. The Enforcer can use either its' 15 digit IMEI number, or an 8 digit number assigned by the monitoring service. The IMEI number is used by default; to use the 8 digit ID, the Alternative Locator ID checkbox must be checked and the Device ID entered and saved to the Enforcer unit.

Password

The password is an eight digit number used to secure the data communication between the enforcer and the server. It will be assigned by the monitoring service. If the password is not the same between the device and server, some of the functions of the monitoring service may not work.

1.2.3 Retrieving and Saving the Configuration Data

On the bottom of the LocationNow Suite window, there are 2 buttons:



Click this button to retrieve the existing configuration from the device to the utility.



Click this button to save the current configuration in the utility to the device

1.3 Operation menu - File

Click the file icon to access the File Menu, which consists of the drop down menu shown in Figure 1-8.

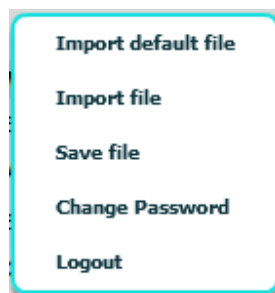


Figure 1-8: The File Options Menu

1.3.1 Import Default File

The Import default file option provides a minimal set of operational parameters, mainly for the Functions and Advance menus. Users will need to provide additional information such as the

specifics of the SIM card provider's APN gateway, and the Domain names of the monitoring server before the Enforcer can communicate with LocationNow or other monitoring servers.

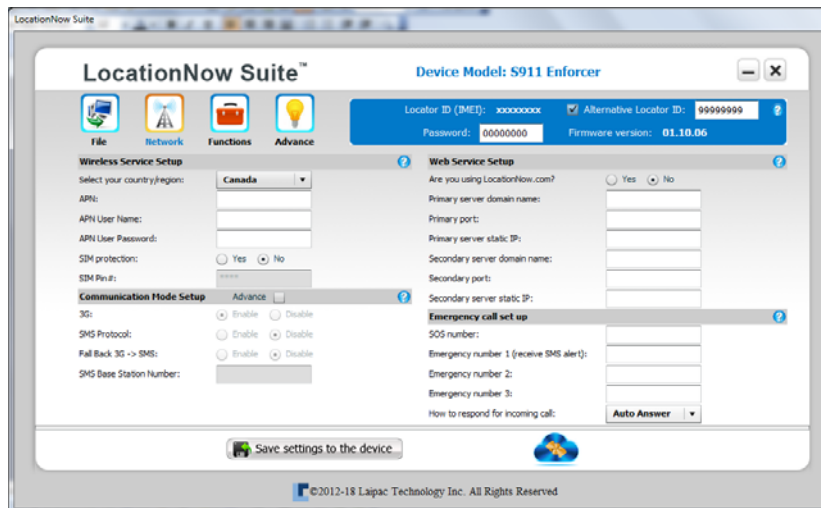


Figure 1-9: The Network Page

1.3.2 Import file

An Enforcer's configuration can be saved to a file for use at a later date; see section 1.3.3 for how to save a configuration. The Import file option loads a previously saved configuration file into the programs memory where it can be customized before it is saved to the Enforcer's onboard memory.

- (1) Select Import file
- (2) Using the Windows file browser, locate the desired file.

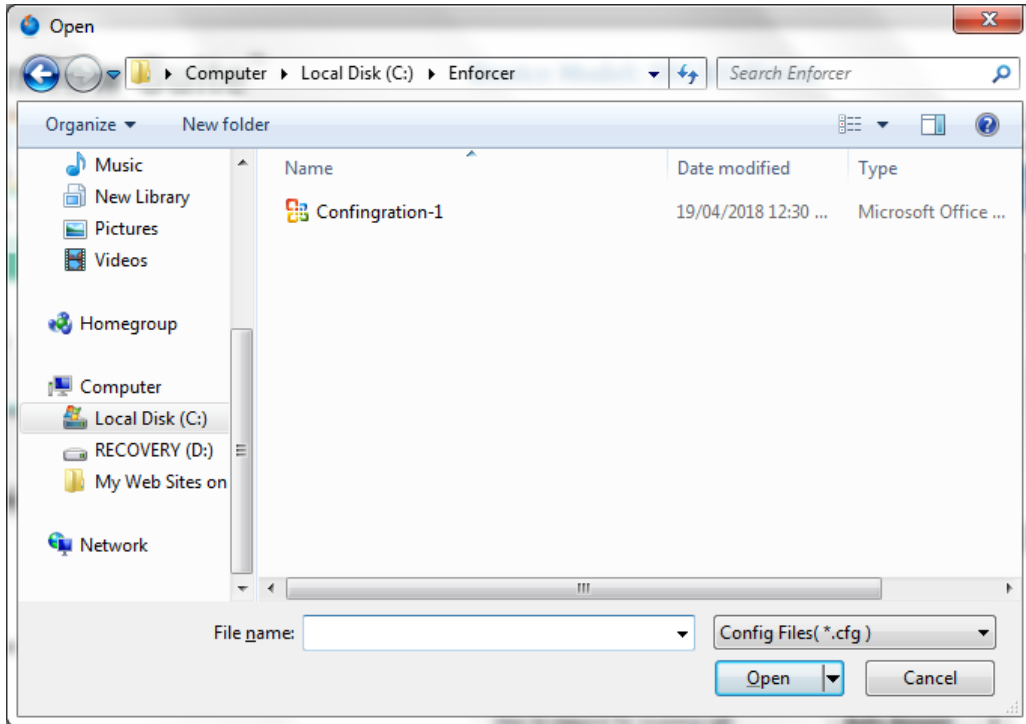


Figure 1-10: Selecting a Configuration File

(3) Click Open; the configuration, included in this file, will be imported.

Note:

The Save file and Import file functions provide an efficient way for a user to configure multiple Enforcers with similar configurations.

1.3.3 Save file

The Save file function is used to save a configuration to a file.

(1) Select Save file and use the Windows' file browser to select the desired folder; in this example **C:\Enforcer**

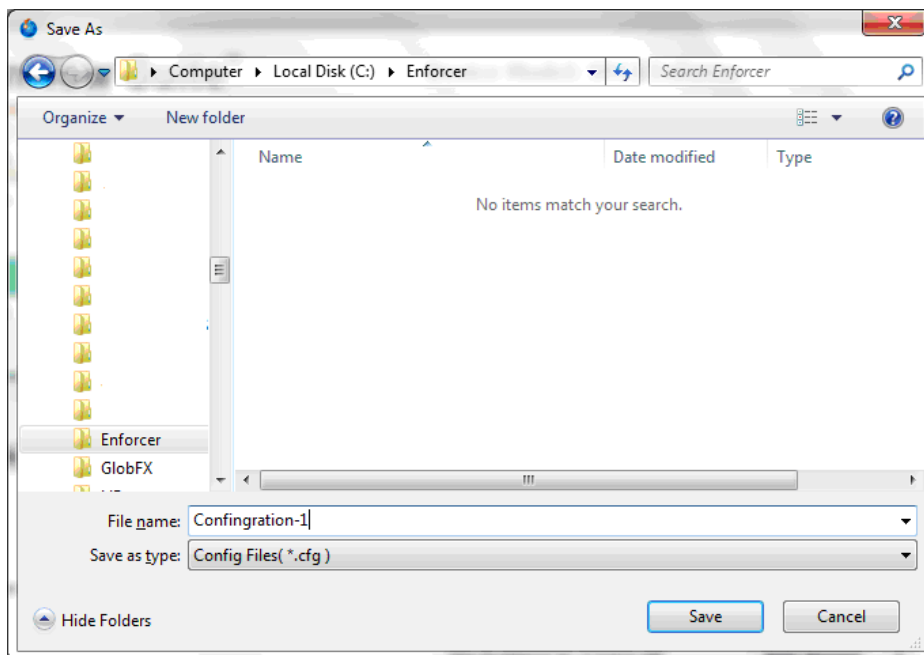


Figure 1-11: Saving a Configuration File

- (2) Enter a file name such as, **Configuration-1**, in the File name block and click Save
- (3) A file with the name Configuration-1.cfg will have been created in the **C:\Enforcer** folder.

1.3.4 Change password (Reserved)

Certain applications have a requirement that the configuration of an Enforcer must not be changed without authorization

When set, the password option in this menu prevents changes to the configuration of an Enforcer without the user providing the password. The password in the File menu is separate from the Password shown on all pages of LocationNow Suite which controls access between the Enforcer and the LocationNow Monitoring Service.


To use the password control function with the Enforcer, please contact Laipac.

1.3.5 Logout

Logout will return the utility to the start up menu.

1.4 Operation menu - Network



Click the  icon to access the Network menu.

1.4.1 Wireless Service Setup

A screenshot of a web form titled "Wireless Service Setup". The form has a light gray background and a white border. It contains the following fields:

- "Select your country/region:" with a dropdown menu showing "Canada" and a downward arrow.
- "APN:" with a text input field containing "internet.fido.ca".
- "APN User Name:" with a text input field containing "fido".
- "APN User Password:" with a text input field containing "fido".
- "SIM protection:" with two radio buttons: "Yes" (unselected) and "No" (selected).
- "SIM Pin#:" with a text input field containing "****".

Figure 1-12: Wireless Service Setup

Select your country/region:

Use the drop-down menu in Figure 1-13 to select the country where the Enforcer unit will be used.

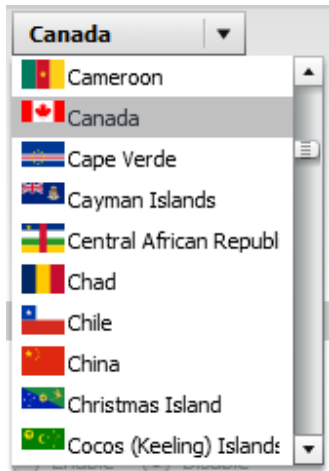


Figure 1-13: Country Selection Drop Down Menu

APN: Enter the Access Point Name for the SIM card that you will be using. This is set by the cellular service provider who's SIM is used.

APN User Name: The user name for accessing the APN; set by the cellular service provider, in many cases will be blank.

APN Password: The password for accessing the APN; set by the cellular service provider, in many cases will be blank.

SIM protection: If the SIM card has a PIN code, check the box; otherwise leave unchecked.

SIM Pin #: When SIM card has a PIN code assigned, enter the code here.

Note:

To make full use of all of the Enforcer's capabilities, the SIM card must be associated with an account that has voice, SMS (text) and data services enabled.

The APN settings and the SIM card's PIN should be obtained from the service provider.

1.4.2 Communication Mode Setup

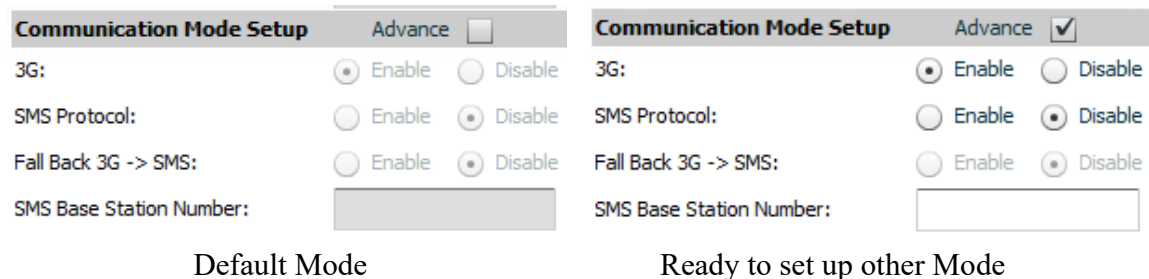
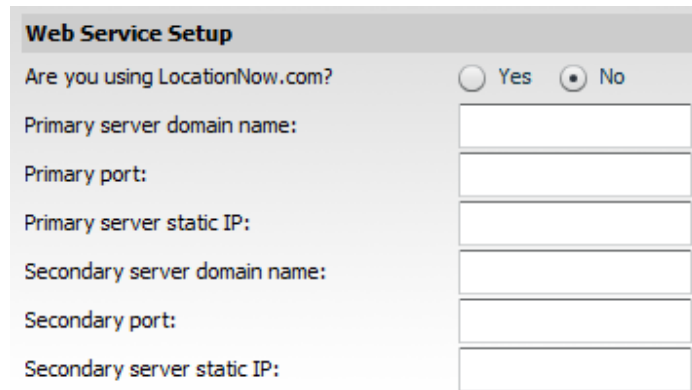


Figure 1-14: The Communication Mode Setup Section

- Advance:** Check this box to access the options available in this section
- 3G:** The default mode, TCP/IP over the 3G network with the monitoring platform, such as, Laipac's LocationNow.com.
- SMS protocol:** Legacy communication method, data and commands can be passed between the Enforcer and the Monitoring Server using SMS (text) messages. Not recommended for new installations.
- Fall Back 3G→SMS:** When enabled with the SMS protocol also active, an Enforcer can use the SMS protocol for communication if a data connection is not available. Legacy communication method, not recommended for new installations.
- SMS Base Station No.:** If a telephone number is provided here, only SMS messages originating from this number will be processed. Please. check with Laipac's technical support for information on how this process works. Legacy communication method, not recommended for new installations.

1.4.3 Web Service Setup



Web Service Setup

Are you using LocationNow.com? Yes No

Primary server domain name:

Primary port:

Primary server static IP:

Secondary server domain name:

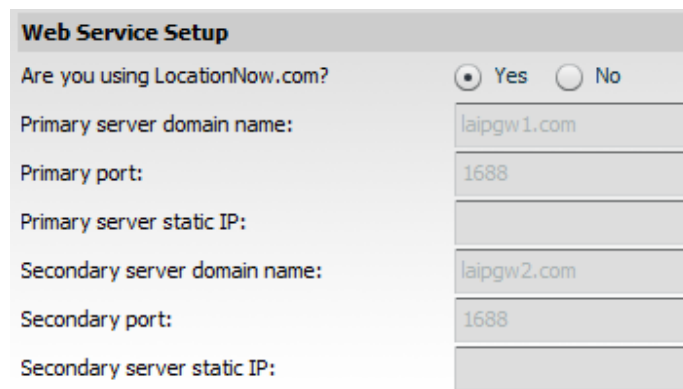
Secondary port:

Secondary server static IP:

Figure 1-15: The Web Service Setup Section

Are you using LocationNow.com

Select “Yes” and the utility will complete the Web Service Setup section automatically as shown in Figure 14.



Web Service Setup

Are you using LocationNow.com? Yes No

Primary server domain name: laipgw1.com

Primary port: 1688

Primary server static IP:

Secondary server domain name: laipgw2.com

Secondary port: 1688

Secondary server static IP:

Figure 1-16: The Web Service Setup (Auto filled when using LocationNow.com)

If the monitoring server is not LocationNow.com, select No, and enter the address information of the server the Enforcer is to send data to.

Primary server domain name: The domain name of the primary server. For www.LocationNow.com, it is **laipgw1.com**.

Primary port: The port used by the primary server. For www.LocationNow.com, it is **1688**.

Primary server static IP: The primary server's static IP address if known. The primary server domain name will generally point to this address. This parameter will be used if both the Primary server domain name and the Primary server static IP values are entered in this section.

Secondary server domain name: The domain name of the secondary server.

Secondary port: The port used by the secondary server.

Secondary server static IP: The secondary server's static IP address

When the Enforcer develops a TCP/IP connection with a remote monitoring service platform, it will try the Primary server static IP first, the Primary server domain name second, the Secondary server static IP third, and finally the Secondary server domain name. If no connection is established, the Enforcer will re-attempt this connection sequence repeatedly.

1.4.4 Emergency Call Set up

Emergency call set up	
SOS number:	<input type="text"/>
Emergency number 1 (receive SMS alert):	<input type="text"/>
Emergency number 2:	<input type="text"/>
Emergency number 3:	<input type="text"/>
How to respond for incoming call:	<input type="button" value="Auto Answer"/> ▼

Figure 1-17: The Emergency Call Setup Section

Phone No.	Emergency event and its available phone No.			
	SOS Alert	G-sensor Alert	Geo-fence Alert	Tamper Alert
SOS No.	Call	Call	Call	Call
Emergency No. 1	SMS	SMS	SMS	SMS
Emergency No. 2	Call	Not Used	Not Used	Not Used
Emergency No. 3	Call	Not Used	Not Used	Not Used

Table 1-18: Emergency Alert's Action Sequences

Activation of an SOS alert and its' action sequence:

- 1) When the SOS button is pressed, the following actions are initiated:
 - a. An SOS alert is sent to the monitoring server.
 - b. An SMS (text) message is sent to the number in the Emergency Number 1 field.
 - c. Voice calls are made in sequence to the SOS Number, Emergency Number 2 and Emergency Number 3 if present.
- 2) If the SOS number is not set, or there is no answer, a call will be placed to Emergency Number 2. If Emergency Number 2 is not set, or there is no answer, a call will be placed to Emergency Number 3. The Enforcer will allow approximately 12 seconds for the phone to be picked up before moving on to the next number. If none of the calls above is picked up, the same calling cycle will repeat until a call is picked up.
- 3) An auto answer on the called number such as a voice mail pickup, or a voice prompt from the carrier will be treated as a successful call and the dialing sequence will stop at that point.
- 4) The SOS number and Emergency number 1 can be set to the same number; as can Emergency numbers 2 and 3, though setting these numbers the same provides no additional functionality.

How the Enforcer responds to an incoming call:

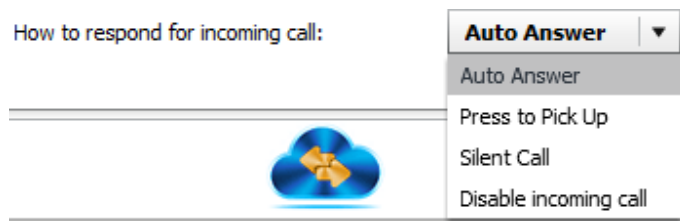


Figure 1-18: Options for Handling Incoming Phone Calls

The Enforcer has four options for responding to an incoming call. Select the desired option from the drop down menu.

- Auto Answer:** The Enforcer answers the phone call without any action from the user
- Press to Pick Up:** The user presses the “SOS” button to answer the incoming call
- Silent Call:** The Enforcer answers the call. The speaker is disabled so the calling party can listen, but no sound from the calling party or their surroundings will be heard by the called party.
- Disable incoming call** The Enforcer will not answer any incoming calls.

1.5 Operation menu - Functions

Click the Functions icon, to access the Functions menu.

1.5.1 Report Interval

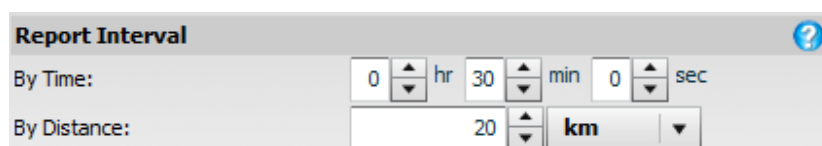


Figure 1-19: Setting the Reporting Intervals

- By Time:** User defined value, sets the time interval on which the Enforcer will report its' position.
Setting the value to 0 hours, 0 minutes and 0 seconds will disable time based reporting. The minimum interval is 15 seconds.
- By Distance:** User defined value, sets the distance interval the Enforcer will use when reporting based on distance. The units of measure for distance supported are: Kilometers, Meters, Miles, or Yards.

1.5.2 Time Zone



Figure 1-20: Setting the Local Time Zone

Time Zone: Select the time zone the Enforcer will use from the drop down menu.

Day Time Saving: When enabled, the Enforcer will automatically switch between standard time and daylight savings time on the appropriate dates during the year.

1.5.3 G-Sensor Alert

Using an accelerometer (G-sensor), the Enforcer is able to sense a change in acceleration such as a fall; on detection of an acceleration above a user defined threshold, a message can be sent to the monitoring server and an SMS device.

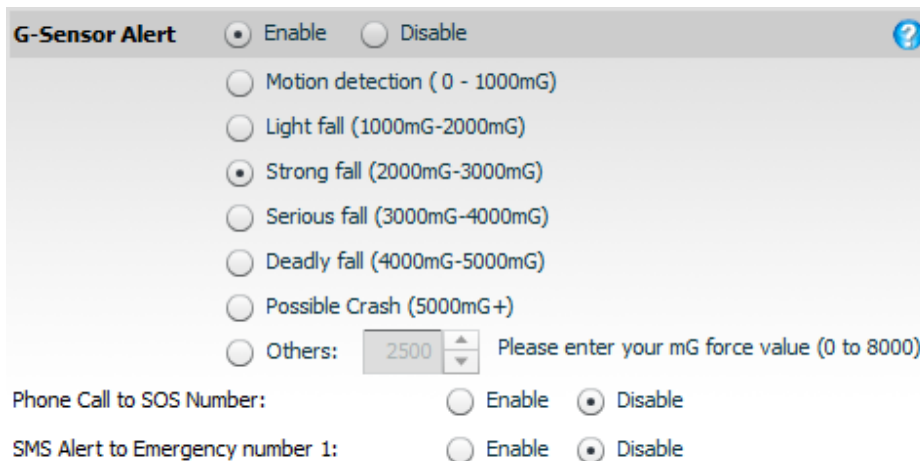


Figure 1-21: Setting the G-Sensor Alert Response

G-sensor Alert: Enables or disables the G-Sensor alert function.

G-sensor Alert Trigger Value: Sets the threshold value for the motion sensor to trigger an alert. The range available is 0 to 8000 micro gravities (mG), the default value is 2500 mG.

Phone Call to SOS Number If this option is enabled, when a G-sensor alert is triggered, Enforcer will make an emergency phone call to the SOS number.

SMS Alert to Emergency No.1

If this option is enabled, when a G-sensor alert is triggered, an SMS message will be sent to the Emergency No.1 number.

If the **G-sensor Alert** function is enabled, when a G-sensor alert is triggered, the Enforcer will complete the following tasks:

An alert message will be sent to the monitoring server,

A text message will be sent to the SMS device set in the Emergency No.1 field,

A phone call will be made to the phone number set in SOS number field.

See section 4.2, for additional information.

1.5.4 Geo-fence

A Geo-fence is a virtual fence that generates alerts should a person wearing an Enforcer enter or exit from a geo-fenced area.

The Geo-fence Alert is a very useful function provided by Enforcer. Using a remote server platform, such as locationnow.com, a user can set up a fenced area on an electronic map. When a user, wearing an Enforcer, enters or exits this specified area, the Enforcer will send a Geo-fence alert message to the remote server and an SMS device.

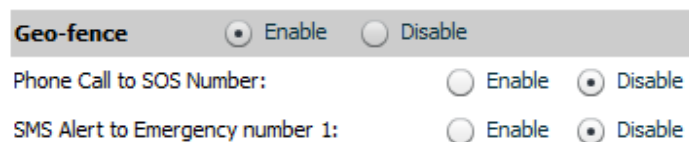


Figure 1-22: Setting the Geofence Alert Response

Geo-fence Alert:

Enables or disables the Geo-fence alert function.

Phone Call to SOS Number

If this option is enabled, when a Geo-fence alert is triggered, Enforcer will make an emergency phone call to the SOS number.

Send Alert to Emergency #1:

If this option is enabled, when a Geo-fence alert is triggered, an SMS message will be sent to the Emergency No.1 number.

Geo-fence Alert Action Sequence and Voice Reminder

If the Geo-fence Alert function is enabled, when a Geo-fence Alert is triggered, the Enforcer will complete the following tasks:

An alert message will be sent to the monitoring server.

A text message will be sent to the SMS device set in the Emergency No.1 field.

A phone call will be made to the phone number set in the SOS number field.

The Geo-fence Alert function's text message and phone call can be disabled using the setup software.

If the Voice on Demand Feature is enabled, when a geo-fence alert is triggered; the Enforcer will play an audio prompt.

See section 1.6.4 for additional information.

1.6 Operation menu – Advance

Click the Advance icon to access the Advance operations menu.

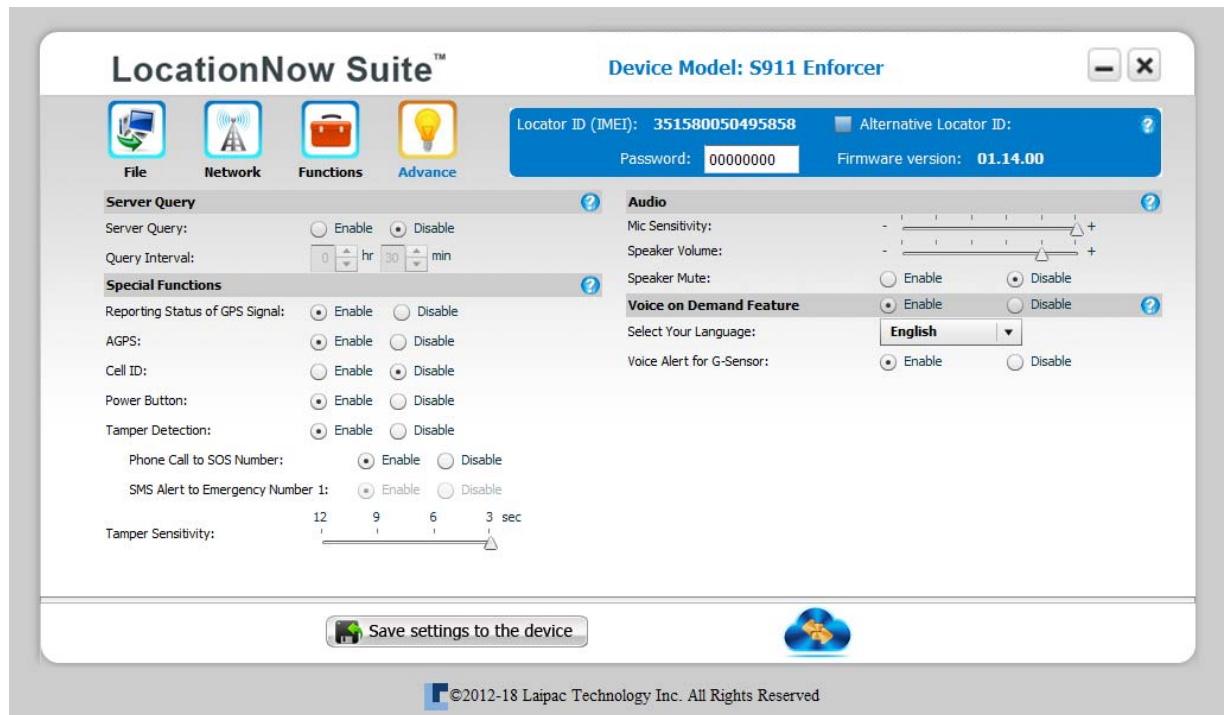


Figure 1-23: The Advanced Functions Page

1.6.1 Server Query

Server Query: Enable or disable this function

Query Interval: This parameter specifies how often the Enforcer will communicate with the monitoring server to keep the communication channel open. Service providers may shut down communication channels that are not actively sending data. This function can be set to make sure that there is communication between the Enforcer and Bracelet frequently enough that this doesn't happen.

1.6.2 Special Functions

Reporting Status of GPS signal: enable or disable this function

When this function is enabled, the Enforcer reports data on the strength of the signals used for cellular communications. This information is for diagnostic purposes; the function is off by default.

AGPS: enable or disable this function

Assisted GPS is a technique for improving the Time to First Fix (TTFF) when bringing the Enforcer on after being off for an extended period of time. This function is on by default.

Cell ID: enable or disable this function

The Cell ID is the identification codes for the cellular tower that the Enforcer is communicating with. This function is off by default, it can be useful when communicating with systems that use the cellular network to enhance the data supplied by the GPS system.

Power Button: enable or disable this function

Used to enable or disable the power button.

Tamper Detection: enable or disable this function

When enabled, the Enforcer will send alerts if it detects that the wrist strap has been tampered with. Enabled by default.

Tamper Sensitivity: Reserved by Laipac

Tamper Alert Action Sequence and Voice Reminder

If Tamper Detection is enabled, when a Tamper Alert is triggered, the Enforcer will complete the following tasks:

An alert message will be sent to the monitoring server,

A text message will be sent to the SMS device set in the Emergency No.1 field,

A phone call will be made to the phone number set in SOS number field.

The Tamper Detection function's text message and phone call can be disabled using the setup software.

If the Voice on Demand Feature is enabled, when a Tamper Alert is triggered; the Enforcer will play an audio prompt indicating if the wrist strap is open or closed.

1.6.3 Audio

Mic Sensitivity: Set the sensitivity of the Enforcer's microphone. The slider can be set to one of six positions.

Speaker Volume: Set the speaker volume of the Enforcer. The slider can be set to one of six positions.

Speaker Mute: enable or disable this function.

Off by default, when enabled, the Enforcer's speaker is muted allowing the Enforcer to send audio to the other party on the call, but will not hear anything from the other party.

1.6.4 Voice on Demand Feature

Voice on Demand Feature Enable or disable the voice reminder functions requested by the SOS, G-sensor, Geo-fence, and Tamper Alerts.

Select Your Language: Select the language to be used for voice reminder prompts and SMS text messages.

Voice Alert for G-sensor: Enable or disable the Voice Reminder for a G-sensor Alert.

2 Firmware Update

This chapter covers how to update the Enforcer's firmware using the LocationNow Suite utility software. The computer running this application needs internet access to function properly.

Here is the procedure:

- (1) Start the LocationNow Suite utility.
- (2) With the Enforcer powered off, connect the Enforcer to a USB port on your computer using a USB cable; a USB cable with the appropriate connectors is shipped with the Enforcer.
- (4) The Enforcer's LCD screen will show USB CONFIGURATION; on the computer's side, the utility will check the firmware version currently installed on the Enforcer. If the current firmware is older than the one currently issued by Laipac for the Enforcer, the utility will display the window below and ask the user to update the firmware.

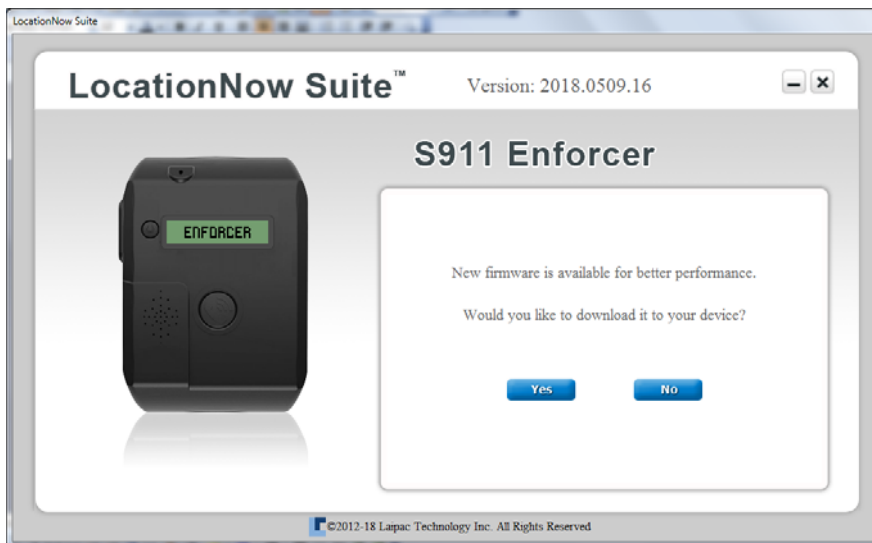


Figure 2-1: The Firmware Update Options Screen

- (5) Click the Yes button, to update the firmware, press no to abort the update and move to the utility.
- (6) When the update process is completed, the screen below is shown.

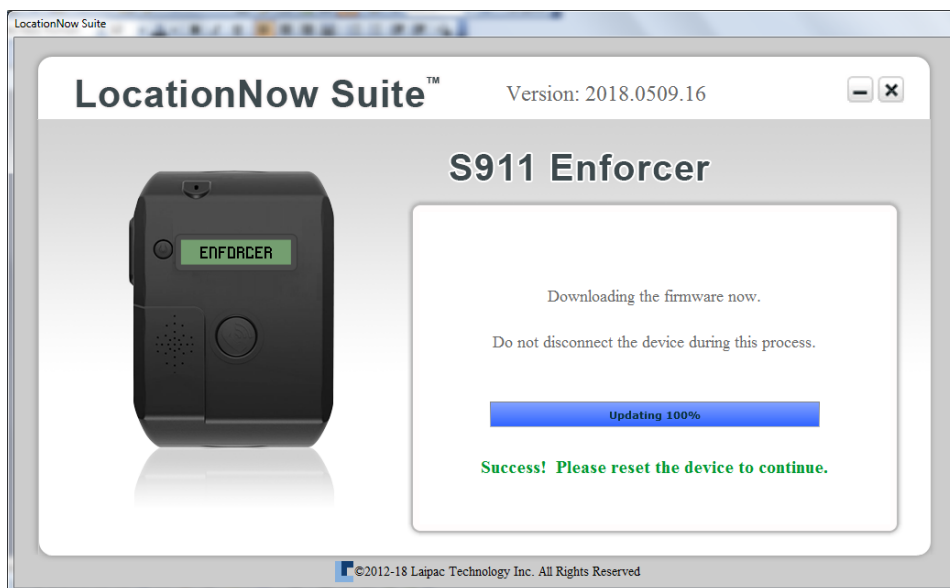


Figure 2-Firmware Update Reporting Screen



Figure 2-3: Screen Confirming that Communication has been Established

After clicking on the Proceed to set up button, make sure that the configuration settings have been read successfully. Save the settings back to the Enforcer.

This is a critical step after a firmware update!

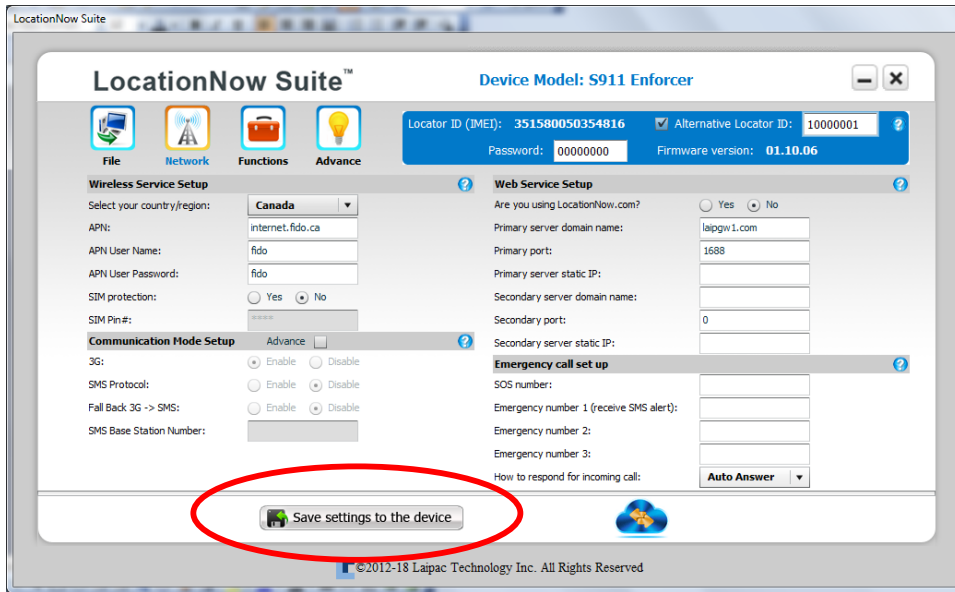


Figure 2-4: Save the Current Settings to the Enforcer after the Upgrade

3 Using your Enforcer

3.1 Checklist for getting an Enforcer ready for use

1. Install the SIM card (open case and install Nano-SIM card); make sure that the SIM has been activated and has voice, SMS and data services enabled.



2. Charge the Enforcer's battery.
3. Use LocationNow Suite to configure the Enforcer; detailed configuration information can be found in section 2.

3.2 Charging

As shown in figure 3-1 below, use the supplied USB cable and charger to charge the battery.



Figure 3-1: Charging the Enforcer.

Note:

The electrical characteristics of the charger:

Input: AC 100 to 240V /100mA
Output: DC 5V/1A
Frequency: 50-60Hz

Turning the Enforcer off while charging will reduce the time required to charge the unit. With the Enforcer powered off, and charging, the LCD will display Charging; see Figure 3-2.

Fully charging the Enforcer can take up to 4 hours, depending on how low the battery has discharged at the beginning of the charging cycle.



Figure 3-2: LCD Display while charging with the Enforcer off.

3.3 Power On and Off

Power on

Press the Power on/off button for about 3 seconds; the Enforcer's LCD backlight will start flashing, and a vibration will be felt. The LCD display will show ENFORCER for several of seconds, then



A set of indicators will appear on screen. These indicators reflect the operating status of the Enforcer.



The indicators from left to right:

















- Status of cellular connections
- Local time
- Status of Bluetooth connections
- GPS signal status
- Battery consumption status

















Power off

Press the Power on/off button for about 3 seconds,

- the Enforcer's LCD screen's backlight will be on, and the unit will vibrate
- the display will show TURNING OFF for several seconds, before turning off and leaving the display blank.






















3.4 Introduction to the LCD Display Icons

Icon	Description
	Device is operating under a configuration or firmware update process
	No SIM card installed
	Device is searching for a cellular network or trying to connect with one.
	Device is not connected to a cellular network
	Device connected to cellular network, signal level is very low
	Device connected to cellular network, signal level is low
	Device connected to cellular network, signal level is good
	Device connected to cellular network, signal level is very good
	Device connected to monitoring platform, signal level is very low
	Device connected to monitoring platform, signal level is low
	Device connected to monitoring platform, signal level is good
	Device connected to monitoring platform, signal level is very good
	AM and PM, used with the clock's 12 hour mode
	A Bluetooth beacon has been detected
	A Bluetooth beacon has not been detected
	When flashing, the device's GPS position is unknown When solid, the device's GPS position has been determined

Indicator	Description	
	Security band is closed; used with the tamper-close-alert	
	Security band is open; used with the tamper-open-alert	
	The Enforcer has entered into a Geo-fenced area, used with the Geo-fence in/out alert	
	The Enforcer has exited a Geo-fenced area, used with the Geo-fence in/out alert	
	Battery Empty	
	Battery Very Low	
	Battery Low	
	Battery Middle	
	Battery High	
	Battery Full	
	Proximity Alert, used with the Restraining Order Application	
	Restriction Alert, used with the Restraining Order Application	
	Fall Detection 1	<p data-bbox="644 1630 1315 1704">These 4 icons are used to create an animation, which indicates a fall down accident.</p> <p data-bbox="644 1738 1066 1771">It is used with the G-sensor Alert</p>
	Fall Detection 2	
	Fall Detection 3	
	Fall Detection 4	

3.5 Checking the Enforcer's Operating Status

The table below lists those statuses, of those major function parts of an Enforcer, to be checked

Status	Description	The suggested action
Battery	 or  If  or  appear the battery is low and needs to be charged.	Charge the battery as soon as possible.
SIM card	 If  appears, the SIM card can not be found.	Check the SIM card installation and reinstall if necessary.
3G network Searching	 If  appears, it means the device is searching for a 3G network.	Keep waiting.
Failed to access 3G network	 If  appear, it means device has failed to access a 3G network.	Check 3G network service provider for 3G signal coverage in the area where the device is operating. Also, check if the SIM card has been activated
Connected to 3G network	 If any one of  appear, it means the device has connected to a 3G network.	Keep waiting for device to develop connection with the Location Based Server platform.
Connect to Location Based Server platform	After waiting for a while, if any one of:  appears, it means the device has connected to a Location Based Server platform successfully. If none of these icons appear, the device cannot connect to the expected Location Based Server platform even though it is able to connect to the 3G network.	To check why the device has failed to connect to the Location Based Server Platform: <ul style="list-style-type: none"> - does the SIM card has a valid data plan. - are the APN settings correct. - are the Gateway's domain Name, IP address and port number correct.
Detection of Bluetooth Beacon	Since detection of a Bluetooth beacon is still a reserved function, only  appears	At present, this check can be skipped
GPS	 If  is flashing, it means the GPS signal is being used for positioning  If  stop flashing, the device's position has been located Note: When the device enters into its power saving mode,  also stops flashing.	 If  continues flashing for 5 minutes or more. Reposition the Enforcer for a better view of the sky.

Note:

If the Enforcer passes all status checks listed above, the user should check their monitoring platform to confirm that the Enforcer is reporting to the platform.

4 Enforcer Alert Functions

4.1 Tamper Alert

4.1.1 The Security-lock and its' open/close operation

The pictures below show:

- 1) The security-lock and the tool to open or close this lock (Figure 4-1)
- 2) How to open or close the lock when the user is wearing their Enforcer (Figure 4-2)



Figure 4-1: Enforcers Lockable Wrist Strap

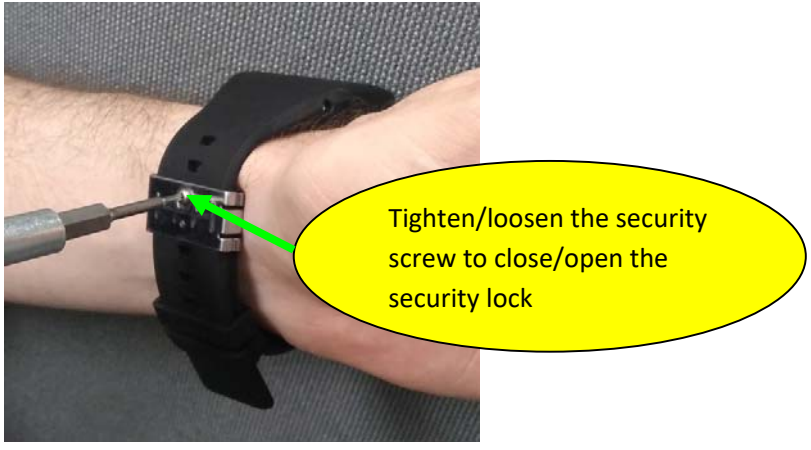


Figure 4-2: Locking and Unlocking the Wrist Strap

4.1.2 Voice Reminder and Display Associated with the Tamper Alert

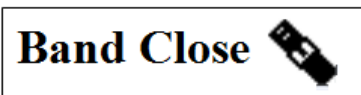
If the Voice on Demand Feature is enabled, whenever a Tamper Alert is triggered, the Enforcer will play an audible prompt.

Tamper alert triggered by	The content of voice reminder
Security-lock is open	Wrist band is open
Security-lock is closed	Wrist band is closed

The LCD display, will show:



with the icon flashing when the security-lock is open



when the security-lock is closed

4.2 SOS Alert

4.2.1 A Unique Property of the SOS Alert

Unlike other Enforcer alerts, the SOS alert cannot be disabled using the LocationNow Suite utility.

4.2.2 Voice Reminder of SOS Alert and False Alarm Cancellation

When a user presses the SOS button for 3 seconds, it will trigger an SOS alert.

If the Voice on Demand option is enabled, after an SOS alert is triggered, the Enforcer will cause the light for the LCD screen too flash, generate a vibration and play the audio prompt shown below five times.

SOS activated, if false alarm, press SOS button to cancel it

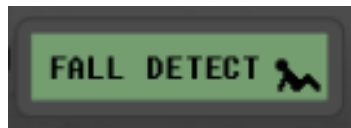
If the SOS button is presses a second time during the confirmation process provided by the Voice on Demand function; the SOS Alert will be cancelled, and no record will be made.

If the SOS Alert is not cancelled, then the Alert will proceed as described in section 1.4.4.

4.3 G-sensor Alert

4.3.1 G-sensor Alert Action Sequence

If the G-sensor Alert function is enabled, whenever the G-sensor detects an event that meets the configured levels, a G-sensor Alert will be triggered. On the LCD display, a scrolling alert message FALL DETECTED with an animated icon will be displayed on the screen. An Alert will be processed as described in Section 1.5.3.



4.3.2 Cancelling False Alarm G-sensor Alerts

If the Voice on Demand option is enabled, after a G-sensor alert is triggered, the Enforcer will cause the light for the LCD screen too flash, generate a vibration and play the audio prompt shown below five times.

Fall Alert, if you are OK, press SOS button to cancel it.

During this period, if the user wants to cancel this alert, they can press the SOS button in order to terminate the G-sensor Alert. The G-sensor Alert will be cancelled, and no record will be made.

4.4 Geo-fence Alert

The Enforcer provides a Geo-fencing function with support for up to 20 geo-fenced areas. If the Enforcer crosses the boundary of a geo-fenced area an alert can be raised based on the configuration of the individual Geo-fence. While the geo-fences definition parameters are stored in the Enforcer's memory, the creation and maintenance of the geo-fence is done using the

LocationNow website. Information on creating and maintaining a geo-fence can be found in the LocationNow User's Manual.

4.4.1 Home Geo-fence

The 20 geo-fences are by default named GF00 through GF19; the names can be changed to better associate them with the end user's application.

Geo-fence GF00 has an additional function as the Home Geo-fence. When an Enforcer powers on, it will check if GF00 has been configured, and if it has, check if it is inside or outside of the defined area.

4.4.2 Voice Reminder and LCD display coming with Geo-fence Alert

If the Voice on Demand Feature is enabled, whenever a Geo-fence Alert is triggered, the Enforcer will play a Voice Reminder. The content of this Voice Reminder depends on the type of Geo-fence Alert.

Type of Geo-fence Alert	The content of Voice Reminder
Geo-fence in alert	Geo-fence Alert, you have entered the Geo-fence
Geo-fence out alert	Geo-fence Alert, you have left the Geo-fence

Also, on the LCD display, a scrolling alert message will be shown:



ENTER GEO-FENCE when it is a geo-fence in alert

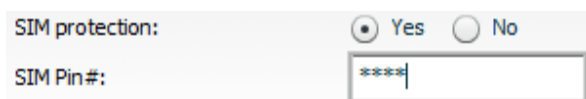


EXIT GEO-FENCE when it is a geo-fence out alert

4.5 Wrong Pin Alert

If the SIM card is configured with pin protection, when configuring an Enforcer, the user must ensure that this pin is entered into the Enforcer using the LocationNow Suite utility software.

Steps for entering a pin number:

A screenshot of a software interface for SIM protection configuration. It shows a label "SIM protection:" followed by two radio buttons: "Yes" (which is selected) and "No". Below this, there is a label "SIM Pin#:" followed by a text input field containing four asterisks "****".

- 1) Select Yes on the SIM Protection radio button
- 2) Input the Pin number in the SIM Pin# field. This is usually a 4 digit number, and is provided by the SIM card provider
- 3) When entering the pin, the entered digits are not displayed on screen and are replaced with asterisks.

This pin, together with the other settings, must be saved into the Enforcer's memory.

When the Enforcer starts running; it will check the validity of the PIN. If the PIN is incorrect, it will show the alert message below on the LCD display and cease further operation.



If a user sees this alert message, they should power off the Enforcer, and use the LocationNow Suite utility software to enter the correct PIN.

5 Warning Statement

5.1 FCC

Federal Communications Commission (FCC) Statement

15.19

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- 1) this device may not cause harmful interference and
- 2) this device must accept any interference received, including interference that may cause undesired operation.

15.105(b)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the

equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

15.21

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. During testing, EN105 is set to their highest transmission levels and placed in positions that simulate use against the head, with 10mm separation, and on the wrist, with no separation. When placing EN105 near your face, keep at least 10mm of separation to ensure exposure levels remain at or below the as-tested levels.

5.2 ISED

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique 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.

Caution: Exposure to Radio Frequency Radiation

1. To comply with the Canadian RF exposure compliance requirements, this device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.
2. During testing, EN105 is set to their highest transmission levels and placed in positions that simulate use against the head, with 10mm separation, and on the wrist, with no separation. When placing EN105 near your face, keep at least 10mm of separation to ensure exposure levels remain at or below the as-tested levels.

Attention: exposition au rayonnement radiofréquence

1. Pour se conformer aux exigences de conformité RF canadienne l'exposition, cet appareil et son antenne ne doivent pas être co-localisés ou fonctionnant en conjonction avec une autre antenne ou transmetteur.

2. Durant les tests, les radios de l'EN105 est réglé sur le niveau de transmission maximal et sont placées dans des positions simulant une utilisation contre la tête, avec une séparation de 10 mm, et au poignet, sans séparation. Lorsque vous approchez votre EN105 du visage, gardez une séparation d'au moins 10 mm pour veiller à ce que les niveaux d'exposition ne dépassent pas les niveaux testés.

5.3 CE RED

During testing, EN105 is set to their highest transmission levels and placed in positions that simulate use against the head, with 10mm separation, and on the wrist, with no separation. When placing EN105 near your face, keep at least 10mm of separation to ensure exposure levels remain at or below the as-tested levels.

Wireless	Frequency Band	Max. Rated Power (dBm)
Bluetooth Low Energy	2402MHz-2480MHz	-0.5 ± 2
WCDMA, 3G	Band 1	22 ± 2
	Band 8	22 ± 2