Encryption Administration Guide

Document Version	2.2
Date	10/28/14
Author	Keith Gray
Status	Draft

Revision History:

Version	Date	Author	Description
1.0	4/25	kg	Initial Draft
1.1	4/30	es	Edits
1.2	5/1	kg	Added SOS Assignment
2.0	9/15/2014	KG	Updated Gateway installation
2.1	10/21/2014	MDG et al.	Updates for new Encryption Gateway and inReach Encryption
2.2	10/28/2014	KG	Updated overview and Encryption Scheme Sections

1 Contents

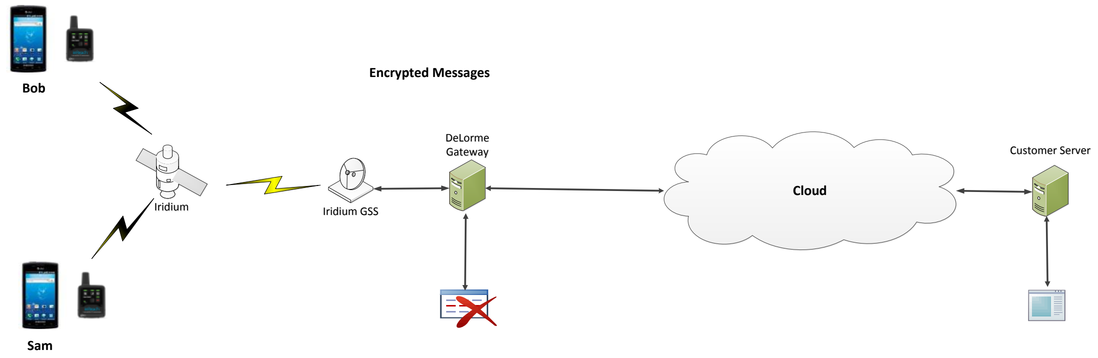
2 Overview

Enterprise customers have the option to enable encryption on the inReach system. One option, Earthmate Encryption, sends and receives encrypted text messages from the Earthmate application installed on mobile devices. The other option, inReach Encryption, encrypts all outgoing transmission from the inReach device.. The data flow of an encrypted message goes as follows - encrypted message is created on the mobile device, sent to the Iridium satellite via inReach, forward to the DeLorme Gateway and passed onto a customer specified server. The DeLorme Gateway recognizes that the messages are encrypted and records the bytes sent for billing purposes. The encrypted messages are deleted from the Gateway after it is forwarded onto the designated party. If the customer does not have their own gateway to manage the encrypted messages DeLorme can provide one to install on their server.

The first part of this guide explains how to setup the mobile devices for encryption. The second part describes how to setup the DeLorme's Gateway Server application on your server if desired. Call DeLorme to get the download link for the Gateway.

3 Setting up System for Encryption

3.1 System Architecture



- **Earthmate Application** – iOS/Android application that sends and receives encrypted text messages. The application also has the capability of displaying the text message location on a map. Encryption functionality is enabled via the DeLorme Gateway.
- **inReach** – Iridium based two way communication devices. The firmware supports the sending and receiving encrypted message packets. If encryption is turned on the inReach device all messages are encrypted before transmission.
- **DeLorme Gateway** – The Gateway processes incoming and outgoing message. In the case of encrypted messages the administrator of the customer devices enables encryption for their iOS/Android devices. The users have to sync with the server to enable the encrypted message

capability on their devices. The administrator also tells the Gateway where to send their traffic. The encrypted message is deleted from the DeLorme Gateway as soon as they have been sent and the size of the message is recorded for billing purposes.

- **Customer Server** – Customer messages are managed on the customer's server. The customer has the option to incorporate the encryption code into an already existing server or they can use the Encryption Server application supplied by DeLorme.
- **Encryption Option**

Enterprise customers have two encryption options to consider, Earthmate Encryption or inReach Encryption. They both have their use cases but DeLorme does not recommend using both at the same time. The user installed gateway has no way of know which encryption scheme is assigned to each device so keep it simple and chose one or the other for all of the devices in the system.

- **Earthmate Encryption:** Encrypted text is sent to/from the Earthmate iOS/Android application, is not visible on the inReach device, and is visible in the Customer Server.
- **inReach Encryption:** All messages sent to/from the inReach device are encrypted during transmission. These messages are stored in plaintext on the inReach device, are visible in the iOS/Android Earthmate application, and are visible on the Customer Server.

3.2 Encryption Scheme

3.2.1 Earthmate Encryption

For Earthmate Encryption DeLorme uses AES-256 encryption with two options of how to store/generate the keys on the mobile device. One option is to use password based key generator (PBKDF2). The other option is to store the 64 character key on the device. The key has to be exactly 64 characters and the characters have to either be numbers (0-9) or letters (A-F). The first option is the most secure but it is vulnerable to encrypting a message with an unknown password. The originator of the message can easily modify their password without the receiving party knowing, blocking them from reading the message. The second option avoids this problem since the key is stored, encrypted, on the device. The user has to go to great lengths to change the key on the device.

The administrator of the devices controls which key storage scheme to use. The one fact to remember is that each device can be given their own key and/or password but all devices within an account have to use the same key storage method. Switching storage methods will remove any key stored on the mobile device the next time the user sync their device to the DeLorme Gateway.

For Earthmate Encryption only the text messages are encrypted and they are stored encrypted on the mobile device. A password is need to send or read encrypted message on the mobile device. All other message types are not encrypted. Earthmate Encrypted messages cannot be read directly on the inReach device.

3.2.2 inReach Encryption

For inReach Encryption DeLorme uses AES-256 encryption with a key stored on the inReach device. The key has to be exactly 64 characters and the characters have to either be numbers (0-9) or letters (A-F). The user can change the key or the key can be set with the use of a configuration tool supplied by DeLorme.

All message types are encrypted during transmission and are stored on the inReach unencrypted so pairing a mobile device to the inReach allows the Earthmate application to view all messages on the inReach device. The inReach does have a pin code to stop unwanted access to the device but Earthmate running on a paired mobile device does not have a pin code protection. The administrator can remove Bluetooth pairing from the inReach device for a more secured system.

3.2.3 SOS

For devices using inReach Encryption, customers should be aware of the following:

- You *must* sign an SOS waiver with DeLorme, because inReach Encryption bypasses SOS processing in the DeLorme Gateway.
- Currently, there is no user interface (Emergency Call Center: ECC) for managing emergencies built into the DeLorme Encryption Gateway Server.
- SOS messages from the inReach are automatically acknowledged by the Hub Service.

3.2.4 Message Handling

- Using inReach encryption, the following inReach messages are handled:
  - TrackingPositionReport
  - LocateResponse
  - ConfirmEmergency
- The following inReach messages are partially handled:
  - FreeTextMessage, HeavyWeight, SharedMap (limited routing described in this document)
  - DeclareEmergency, DeclareEmergencyPuck, CancelEmergency (all are automatically acknowledged)
  - TrackStart, TrackIntervalChange, TrackStop (position is recorded only)
  - PuckMsg1,2,3 (text contents are not processed and is not routed to a destination)
  - Quick Text (text contents are not processed)
- The following inReach messages are not handled:
  - ReferencePoint
  - Binary
  - MailCheck
  - AmIAlive
  - WptNav

3.3 Check List

Below is a check list for setting up encryption on the DeLorme Gateway so that all traffic is sent to your server. For the list below the assumption is that the devices have already been purchased and the IMEI number for each device is known.

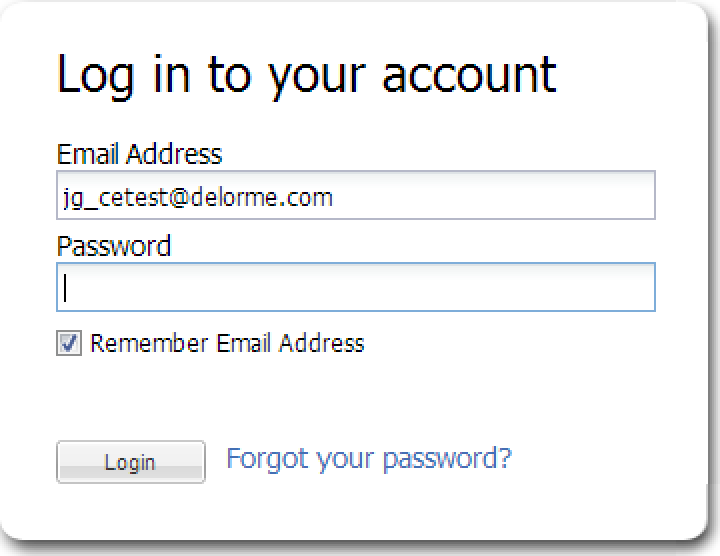
1. Call Delorme to setup your devices on an Enterprise Account
2. Log into enterprise.delorme.com to build user accounts and assign device IMEI number *(Only applicable to Earthmate Encryption)*
3. Enable Encryption and set the key storage method
4. Set the Outbound url to which all inReach traffic will be sent to
5. Set the Inbound account information. You server will need to use this to send messages back to the DeLorme Gateway
6. Set the SOS Assignment for all devices
7. Set Keep Alive Timer durations *(Only applicable to Earthmate Encryption)*
8. Make sure the most recent Earthmate application is installed on the mobile devices
9. Make sure the most recent inReach firmware is installed on the devices
10. Have each user sync their mobile device to the enterprise.delorme.com server (see user guide on how to sync devices) *(Only applicable to Earthmate Encryption)*
11. Setup key and or password on each mobile device (see user guide on how to setup key/password)
12. Test sending an encrypted message to your server

3.3.1 Step 1 – Setup Enterprise Account

- Call DeLorme Customer Service to setup your devices on an Enterprise account. The order number will be needed and what type of monthly billing plan will be used. They can answer any question you might have. At the end of the conversation they will email the account information to the local administrator who can log into the DeLorme Gateway – enterprise.delorme.com to continue the rest of the following steps.

3.3.2 Step 2 – Build User Accounts *(Optional if using inReach Encryption)*

- From you browser type in https://enterprise.delorme.com
- Enter account information from the first step



Log in to your account

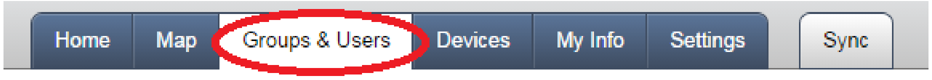
Email Address

jg_cetest@delorme.com

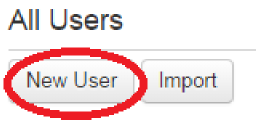
Password

☑ Remember Email Address

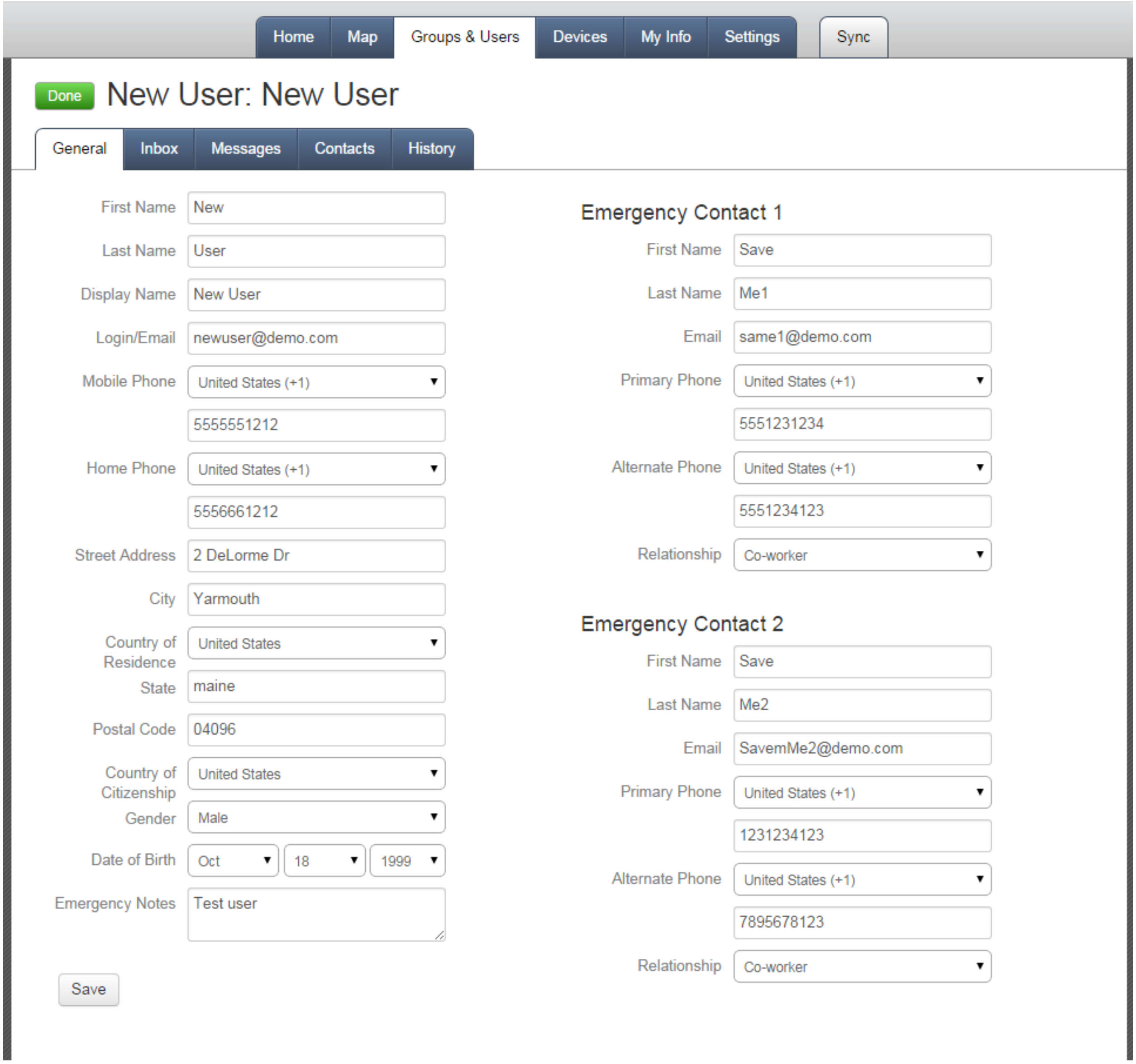
- Go to the Groups & Users tab



- Select New User



- Complete required fields and select IMEI assigned to that account. The user information can be fictitious since the encrypted messages will be sent to your server and deleted from the DeLorme Gateway. The fictitious users on this page will be displayed on the map if they are turn on tracking or if unencrypted messages are sent through the DeLorme Gateway.



New User: New User

First Name	New
Last Name	User
Display Name	New User
Login/Email	newuser@demo.com
Mobile Phone	United States (+1) 5555551212
Home Phone	United States (+1) 5556661212
Street Address	2 DeLorme Dr
City	Yarmouth
Country of Residence	United States
State	maine
Postal Code	04096
Country of Citizenship	United States
Gender	Male
Date of Birth	Oct 18 1999
Emergency Notes	Test user

Emergency Contact 1

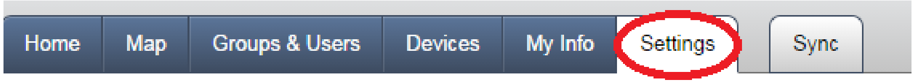
First Name	Save
Last Name	Me1
Email	same1@demo.com
Primary Phone	United States (+1) 5551231234
Alternate Phone	United States (+1) 5551234123
Relationship	Co-worker

Emergency Contact 2

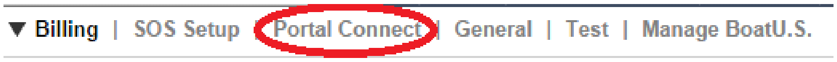
First Name	Save
Last Name	Me2
Email	SavemMe2@demo.com
Primary Phone	United States (+1) 1231234123
Alternate Phone	United States (+1) 7895678123
Relationship	Co-worker

3.3.3 Step 3 – Enable Encryption and Set Key Storage

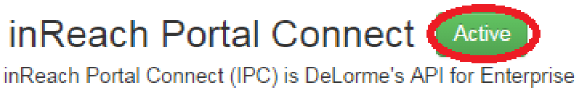
- Select the Settings tab



- Select Portal Connect


▼ Billing | SOS Setup | Portal Connect | General | Test | Manage BoatU.S.

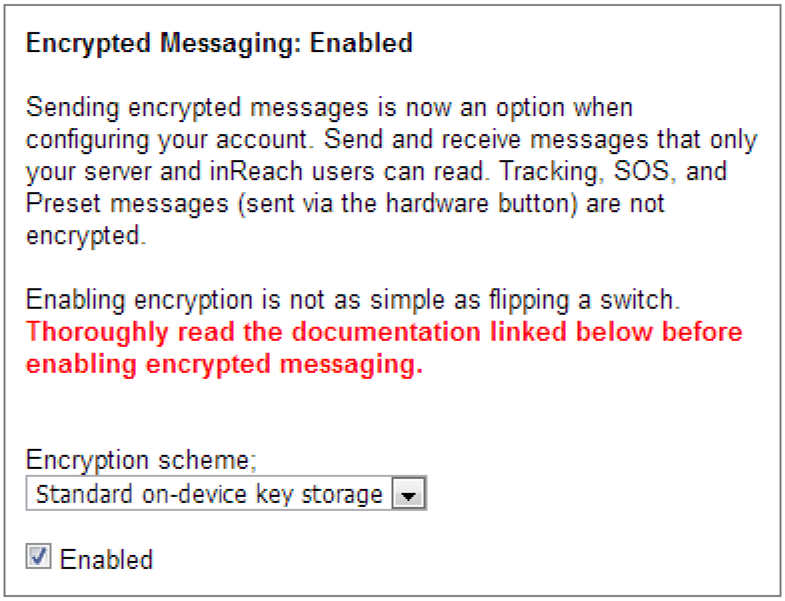
- Activate inReach Portal Connect



inReach Portal Connect Active

inReach Portal Connect (IPC) is DeLorme's API for Enterprise

- *(Optional if using inReach Encryption)* Enable encryption for the devices in your group and also set the key storage method for all devices



Encrypted Messaging: Enabled

Sending encrypted messages is now an option when configuring your account. Send and receive messages that only your server and inReach users can read. Tracking, SOS, and Preset messages (sent via the hardware button) are not encrypted.

Enabling encryption is not as simple as flipping a switch. **Thoroughly read the documentation linked below before enabling encrypted messaging.**

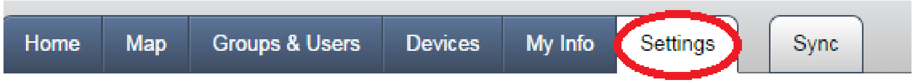
Encryption scheme;

Standard on-device key storage ▾

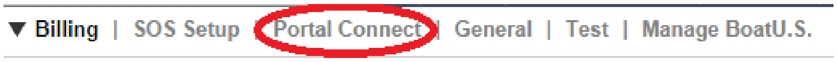
☑ Enabled

3.3.4 Step 4 – Outbound Connection

- Select the Settings tab

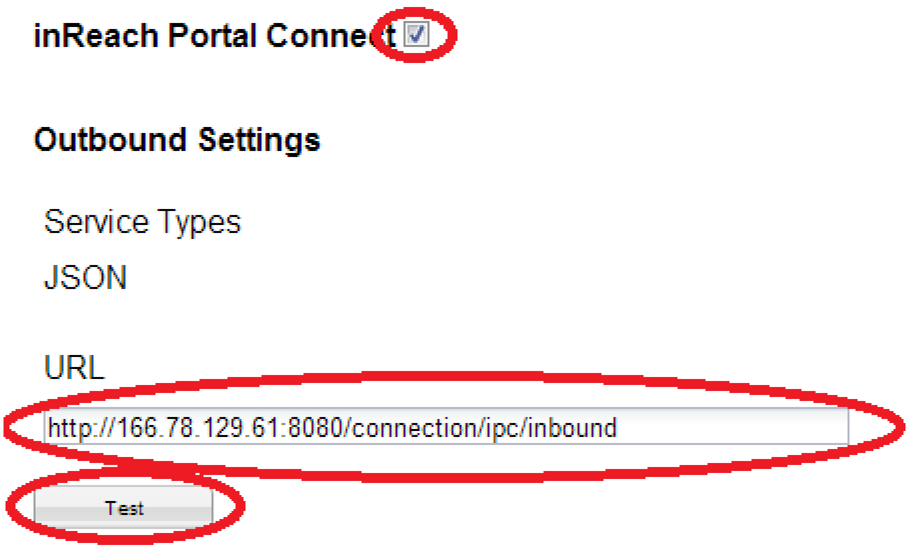


- Select Portal Connect



▼ Billing | SOS Setup | Portal Connect | General | Test | Manage BoatU.S.

- Enable the inReach Portal Connect which tells the DeLorme Gateway to send all traffic to your server.
- Set the url for your server location
- Select the Test button to test the connection to your server. You might need to open a port (8080) on your firewall to allow the DeLorme Gateway to communicate with your server.



inReach Portal Connect ☑

Outbound Settings

Service Types

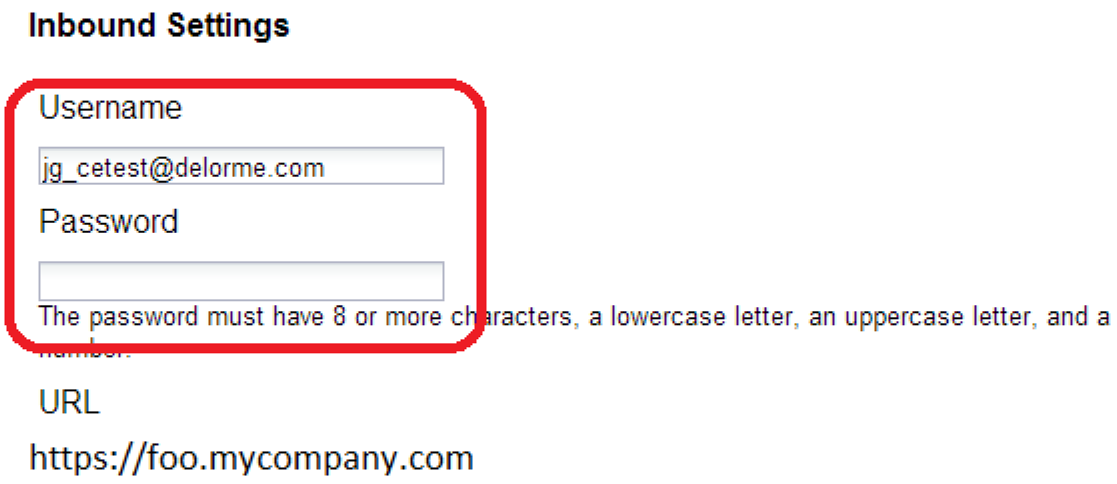
JSON

URL

http://166.78.129.61:8080/connection/ipc/inbound

3.3.5 Step 5 – Inbound Connection

- Set the account information to allow your server to send message back to the DeLorme Gateway



Inbound Settings

Username

jg_cetest@delorme.com

Password

The password must have 8 or more characters, a lowercase letter, an uppercase letter, and a number.

URL

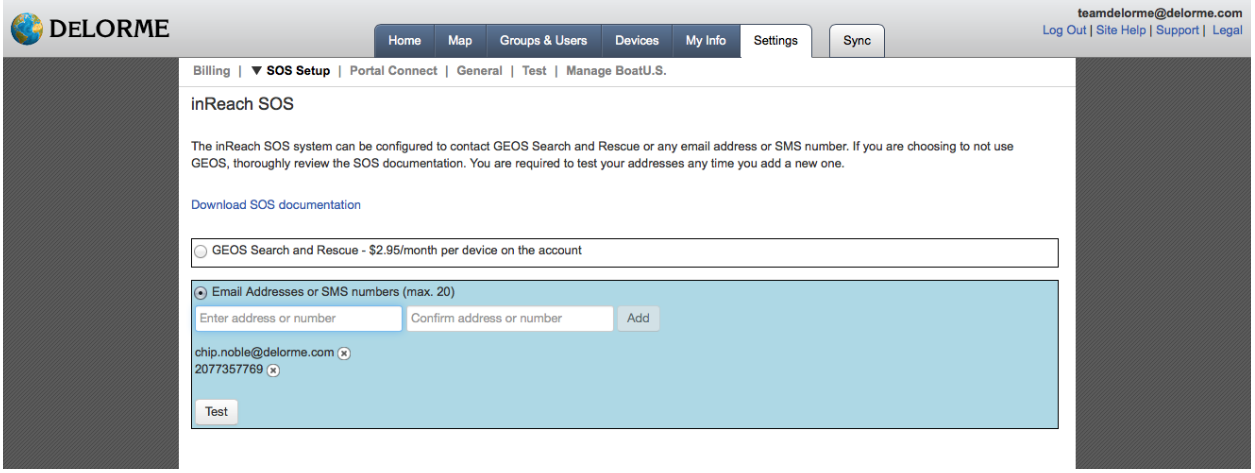
https://foo.mycompany.com

3.3.6 Step 6 – Set SOS Assignment

This section only applies to devices which are using Earthmate Encryption, but not using inReach encryption. By default all SOS alerts are set to a 3rd party called GEOS. This can be reassigned to another email address. Check with your DeLorme account representative to enable the controls for assigning your own email contact. You must sign a waiver in order for you to handle SOS messages privately. At that point, you will be able to make such an assignment by logging into enterprise.delorme.com, selecting the Settings tab, and then selecting the SOS Assignment tab.

- Select the Settings tab
- Select the SOS Assignment
- Select the Email Address or SMS number radio button

- Enter in the SOS email address or SMS number and hit Add
- Select the Test button to verify the connection


DELORME
teamdelorme@delorme.com
Log Out | Site Help | Support | Legal
Home
Map
Groups & Users
Devices
My Info
Settings
Sync
Billing | ▼ SOS Setup | Portal Connect | General | Test | Manage BoatU.S.

inReach SOS

The inReach SOS system can be configured to contact GEOS Search and Rescue or any email address or SMS number. If you are choosing to not use GEOS, thoroughly review the SOS documentation. You are required to test your addresses any time you add a new one.

Download SOS documentation

○ GEOS Search and Rescue - $2.95/month per device on the account

● Email Addresses or SMS numbers (max. 20)

chip.noble@delorme.com ⊗
2077357769 ⊗

3.3.7 Step 7 – Set Keep Alive Timer Durations *(Optional if using inReach Encryption, these settings are available on the device)*

When you first launch the app, all encrypted messages are “locked” and cannot be read. These messages can be unlocked by tapping on them in the “Messages” page and entering your password. The application is now “Unlocked” and all encrypted messages are decrypted and displayed as plain text.

There are two timers that are set the first time you go into unlocked mode and that tell the application how long to keep the system in the unlocked mode. The duration of these timers can be set by you in your enterprise.delorme.com account, and are set in the application when you sync.

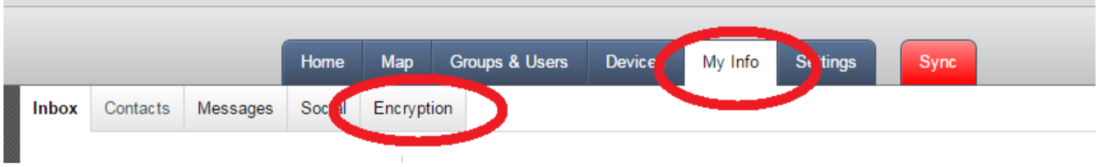
The Idle Keep Alive time is reset after each action (swiping, tapping, scrolling, etc.) in the application. If you have been idle for the designated time period the application will automatically lock encrypted messages.

The Absolute Keep Alive timer is started at the first time the application is set to unlock mode and does not get reset after any action in the application. One minute before the Absolute time expires you are asked if you want to reset the Absolute Keep Alive timer. If you decline or enter the password in incorrectly the application goes into locked mode.

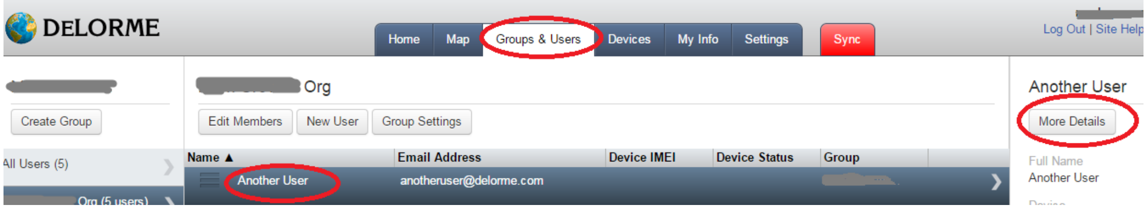
Both timers are there to protect the device from getting used by another user for a long period of time in the unlocked state. If the device is left unattended for a set period of time the idle timer will go off. If the device is stolen when in the unlock state the Absolute timer will go off and force the device into unlocked state.

The app will also lock if the mobile device is locked, either by the mobile devices lock timer or by user action. This is a quick and easy way to lock all messages and to prevent them from being read by unauthorized personnel. The settings for the Keep Alive Timers on the Enterprise Site -> https://enterprise.delorme.com/

- To edit your own settings, choose the My Info tab, then choose the Encryption tab. (If you do not see this tab, you have not enabled encryption yet.)

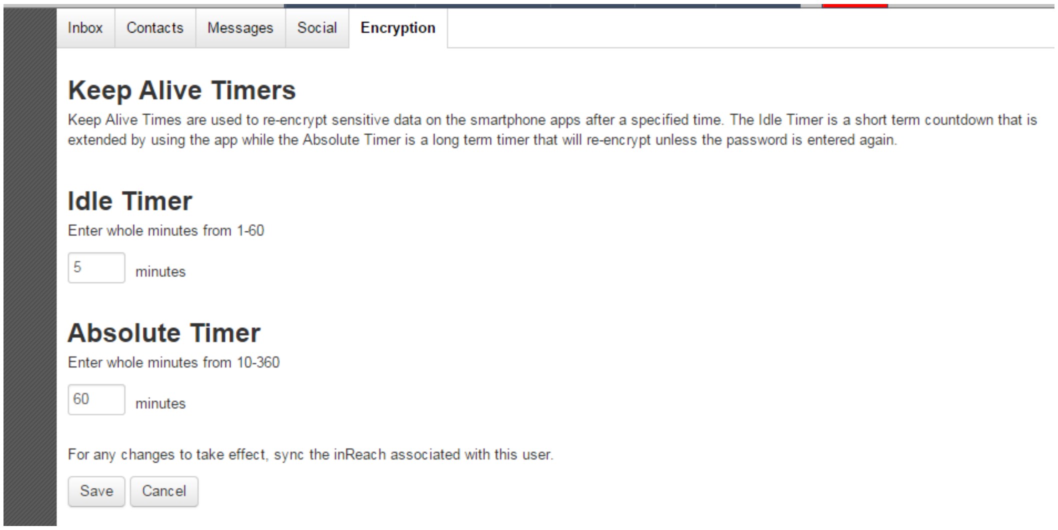


- If you are an admin, to edit the settings for a particular user, select the Groups and Users tab, select the user of interest, and push the More Details button.



Name ▲	Email Address	Device IMEI	Device Status	Group
Another User	anotheruser@delorme.com			[redacted]

- Select the Encryption tab and set the timers. The Idle Timer needs to be one minute or more less than the Absolute Timer



Keep Alive Timers

Keep Alive Times are used to re-encrypt sensitive data on the smartphone apps after a specified time. The Idle Timer is a short term countdown that is extended by using the app while the Absolute Timer is a long term timer that will re-encrypt unless the password is entered again.

Idle Timer

Enter whole minutes from 1-60

5 minutes

Absolute Timer

Enter whole minutes from 10-360

60 minutes

For any changes to take effect, sync the inReach associated with this user.

- The timers will be sent down the next time the user syncs with enterprise.delorme.com

3.3.8 Step 8 – Install Earthmate *(Optional if using inReach Encryption, only do this if pairing a smart phone to the device)*

- Check the mobile device associated stores to make sure the most up-to-date Earthmate application is stored on the device

3.3.9 Step 9 – Update Firmware

- Check the DeLorme support pages for the most recent firmware for the inReach device - http://support.delorme.com/

3.3.10 Step 10 – Sync Devices *(Only necessary if using Earthmate Encryption)*

- Have each user sync their mobile devices to the DeLorme Gateway to enable the encryption functionality.

3.3.11 Step 11 – Add Key/Password

- Make sure each device has the correct key or password

3.3.12 Step 12 – Send Test Message

- Send an encrypted message to your server as a test. To send an encrypted message to another inReach user your server has to handle the message routing or the DeLorme Gateway can be installed on your server which can handle the routing of encrypted messages between devices.

4 DeLorme's Encryption Gateway Server Application

For those customers who do not have their own server setup to handle the encrypted messages they can use the DeLorme Encryption Gateway server to manage encrypted messages. (This is distinct from the DeLorme Gateway which handles transmission through the satellite network.) Along with setting up the routing tables for encrypted messages the server web pages allow the administrator to send and receive encrypted messages without having to use the Earthmate application on their mobile device.

4.1 Setup

4.1.1 Minimum Specifications

- Windows 7 or Windows 2008 R2
- 2 GB of RAM
- 20 GB or hard drive space
- 64-bit processor – 2 GHz or higher
- Open port 8080 on the firewall to allow DeLorme to send message traffic to the server through the Internet

4.1.2 Prerequisites

- **Microsoft Internet Information Services (IIS) 7.5**

  IIS 7.5 is used to host the Gateway Administration Website. Below are the instructions per supported operating system.

  - Windows 7 - http://technet.microsoft.com/en-us/library/cc725762.aspx
  - Windows 2008 R2 - http://technet.microsoft.com/en-us/library/cc771209.aspx

- **Microsoft Message Queuing (MSMQ)**

  MSMQ is used as a cross thread communications service by the Gateway Windows Service.

  http://msdn.microsoft.com/en-us/library/aa967729.aspx

- **Microsoft .NET Framework 4.5**

  The Microsoft .NET Framework 4.5 is required for the Admin Site and Windows Service.

  http://www.microsoft.com/en-us/download/details.aspx?id=30653

- **Microsoft Web Deploy 3.5**

  The Microsoft Web Deploy 3.5 software is required to install the Admin Site.

  http://www.iis.net/downloads/microsoft/web-deploy

- **Microsoft Visual Studio 2013 Redistributables**

The Visual Studio 2013 Redistributables are required to use inReach Encryption

http://www.microsoft.com/en-us/download/details.aspx?id=40784

- **Microsoft SQL Server 2012 SP1**

SQL Server 2012 SP1 is required for the Gateway site to work. SQL Server Express can be used. Install database engine with SSMS. Install SQL Server instance in Mixed Mode (support for SQL Accounts).

Express - http://www.microsoft.com/en-us/download/details.aspx?id=35579

4.1.3 Configuring SQL Server

1. Ensure that you have adequate Sysadmin permissions to add users to the server
2. Open Microsoft SQL Server Management Studio
3. Log into localhost
    1. Server type: Data Engine
    2. Server name: '{name of server set at installation}
    3. Authentication: Windows Authentication
4. Expand **localhost**
5. Expand **Security**
6. Right click **Logins** and click "**New Login...**"
7. Enter the following information and keep notes of what you enter!
    1. Enter a Login name - **Gateway**
    2. Select SQL Server authentication
    3. Enter Password – **Password1**
    4. Uncheck "User must change password at next login"
    5. Select Server Roles from the left.
    6. Check "sysadmin"
    7. Click OK
8. Copy the Gateway software to the computer onto which you're installing the Gateway. Copy revinator.exe and dll to Gateway3 folder
9. Open the Gateway3\Database\Baseline directory and then open the script in SQL Server Management Studio
    1. **2013_01_28_Gateway3_schema.sql**
10. Execute the Script.
11. Open a cmd window as Admin
12. Change directory to the Database folder
13. Run .*Revinator.exe –s=”(local)” –db=”Gateway3” –dir=”database/revs/”* where “(local)” is your SQL server. Gateway3 is the databases created with the 2013_01_28_Gateway3_schema.sql script.

4.1.4 Installing the Hub

The Hub is the Windows Service that handles the processing and dispatch of the encrypted text messages.

1. Open the **Start Menu.** Right-click on "**Computer**" and select "**Manage**"
2. Expand **Local Users and Groups**
3. Right Click **Users** and click **New User**
4. Enter the User Credentials
    a. User name: **Hub**
    b. Full name: Hub
    c. Description: DeLorme Messaging Hub
    d. Password: Enter a password – **Password1**
    e. Confirm password: Reenter the password
    f. Uncheck **User must change password at next logon**
    g. Click **Create**
5. Go to **Users**
6. Right Click Hub and select **Properties**
7. Click **Member Of** tab
8. Remove **Users** group and add **Administrators** group
9. Click **OK** and close **Computer Management**
10. Open File Explorer
11. Navigate to the location that you would like to install the Hub.
    a. For this example we install the hub off of the root directory C:\
    b. Create a new folder and label it **services**
12. Open another File Explorer and navigate to the Hub binaries.
13. Copy the HubService folder into the **services** directory
14. Go into the directory and look for the **Gateway.Services.Hub.WinService.exe.config**
    a. Change the following values in
    <add name="DeLormeGatewayDB" providerName="System.Data.SqlClient" connectionString="Server={SERVER};Database=Gateway3;user Id={Username};password={Password};MultipleActiveResultSets=true;" />

        - {SERVER} - The location of the server. e.g. "(local)\SQLEXPRESS"
        - {Username} - From the Configuring SQL Server Step 7
        - {Password} - From the Configuring SQL Server Step 7

    b. Save changes
15. Open Command Prompt as Admin
16. In the Command Prompt navigate to the directory that you copied the Hub into
    - "cd \services\HubService"
17. Install the Hub by running the following command in the prompt.
    - C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe Gateway.Services.Hub.WinService.exe
18. Open the Services application

. Windows **Start:Administrative Tools:Services**
    a. Look for the **DeLorme Messaging Hub Service.**
    b. Right Click and select **Properties**

19. Click **Log On** tab
20. Check **This account** and enter the user credentials from step 4.
21. Click **OK**

22. Right Click **DeLorme Messaging Hub Service** and select **Start**

4.1.5 Installing the Admin Site

1. Open Internet Information Services (IIS) Manager
2. Expand Server (On the left)
3. Expand Sites
4. Make sure there is a **Default Web Site**. If it does not exist, use the steps below to create it.
   a. Right Click Sites and select Add Web Site...
   b. Enter the following

      i. Site name: Default Web Site
      ii. Select Application pool: ASP.NET v4.0
      iii. Assign it a Physical path and IP Address
      iv. Click OK
5. Open Command Prompt as Admin
6. Navigate to the AdminSite folder
7. Run the following command
   - **Gateway.Presentation.AdminSite.deploy.cmd /Y**
8. The application should now be install. Go to the IIS Manager and make sure it shows up under the Default Web Site.
9. Right Click the **AdminSite** and select Explore
10. Copy the **Web.config** file to your desktop
11. Edit the Web.config file
12. Change the following values in
    <add name="DeLormeGatewayDB" providerName="System.Data.SqlClient" connectionString="Server={SERVER};Database=Gateway3;user Id={Username};password={Password};MultipleActiveResultSets=true;" />
      i. {SERVER} - The location of the server. This will probably be {local} for IPCTEST
      ii. {Username} - From the Configuring SQL Server Step
      iii. {Password} - From the Configuring SQL Server Step
13. Save changes
14. Copy the **Web.Config** back into the AdminSite directory.

4.1.6 Configuring the Gateway

1. Open a browser and go to the Admin Site (machine/AdminSite)
2. Click **Settings**
3. Select your Encryption Scheme. You will be prompted with a dialog. Click **Change**.
4. Click on **Connections**
   a. Add an Inbound Connection. Example address: http://localhost:8080/
   b. Click **Save**
2. Add an Outbound Connection.
   a. Example address: https://enterprise.delorme.com /IPCInbound/V1/Messaging.svc
   b. Username: some IPC Inbound Username
   c. Password: some IPC Inbound Password
   d. Click **Save**
3. Click **Devices**
4. Add some devices
5. Click **Add IMEI**

   a. IMEI: Device IMEI
   b. Password / Key: Depends on Crypto Settings
   c. Address: This is your device Alias address. Enter an email address.
   d. Routing: Select Enabled
   e. Click **Save**
   f. Repeat step 7 until all devices added

6. Open Services window and restart the **DeLorme Messaging Hub Service**

4.2 Operations

4.2.1 Devices Page

This page provides:

- Registration of encrypted devices
- Editing of device characteristics, encryption keys and routing
- A table of messages received from the device
- An editor where the operator can send an encrypted message to the inReach device (using inReach Encryption) or to the Earthmate app associated with the device (using Earthmate Encryption).

4.2.2 Map Page

- Displays locations of incoming messages from devices that are registered in the Encryption Gateway
- The map updates automatically once every five minutes.
- Click on an item to display details about the message

4.2.3 Addresses

Associates email-like addresses with a destination device's imei number. Remember that all communications are between devices so an address needs an associated imei number to be able to receive an encrypted message.

4.2.4 Connections

Configure the Encryption Gateway inbound and outbound connections. For Inbound Connections from the DeLorme the messages are typically coming on port 8080 so the address is http://localhost:8080. Make sure that the firewall has port 8080 open. For Outbound Connections to DeLorme Enterprise Server connect to https://enterprise.delorme.com/IPCInbound/V1/Messageing.svc. The Username and password for the account is set up by using the Portal Connect page on the Enterprise.delorme.com site.

4.2.5 Settings

Additional Encryption Gateway settings.