



HipLink[®] Software

HipLink Mobile Setup and Administration Guide



HipLink® Software Mobile App Setup Guide

HipLink Software Copyright

The *HipLink Software Mobile App Setup Guide* is for use by permissioned Users only. This document contains proprietary information owned by HipLink Software and is protected by copyright law and international treaties. It may not be copied, published or used, in whole or in part, for any purposes other than as expressly authorized by HipLink Software. Any unauthorized copying, distribution or disclosure of information in any manner without the prior written consent of HipLink Software is a violation of copyright laws and will be prosecuted to the maximum extent possible under law.

Trademarks and Copyright

- HipLink® is a registered trademark of Semotus, Inc., DBA HipLink Software.
- All other trademarks and copyrights are the property of their respective owners.

Disclaimer

HipLink Software has made every effort to ensure the accuracy of information contained within this document. However, HipLink Software makes no warranties with respect to this document and disclaims any implied warranties of merchantability or fitness for a particular purpose. All screen images used in this document are for illustrative purposes and are only intended to provide an example of the screen. Screens may vary dependent upon the service provided. Information in this document is subject to change without notice.

Please carefully read the instructions provided in this guide before installing and administering HipLink Software. Retain these instructions for future use. If you do not agree with the terms of this license agreement, do not install, copy, or use this software.

For technical assistance, contact HipLink Technical Support:

Phone: 408-399-0001

Email: support@hiplink.com

HipLink Software Offices
20 S. Santa Cruz Ave
Suite 300
Los Gatos, California 95032

Tel: (408) 399-6120
Fax: (408) 395-5404

www.hiplink.com

HipLink Mobile Set-up & Administration Guide

Table of Contents

About this Guide	1
Process Overview	1
Application Download Options	1
System IP & Network Requirements	1
IP Considerations	1
Port Requirements	2
License Key	3
Check the License Key	3
Mobile User Group Permission & Control Policy Overview	3
Setting up HipLink Mobile	4
Global Settings	4
HNP Manager Configuration	6
General Settings	6
Advanced Settings	7
Push Notifications	8
Secure Internet Call	9
HipLink Alert App	9
Manage Mobile User Group	10
Permissions Configuration	12
System Configuration	13
Inbox Configuration	13
Alert Configuration	14
Message Configuration	15
Template Permission Settings	16
Response Action Permission Settings	16
Department Permission Settings	17
General Permission Settings Definitions	17
Manage HipLink Mobile Devices	18
Manage HipLink Alert Devices	20
Creating a Messenger for HipLink Mobile	21
Creating a HipLink Mobile Carrier	21
Creating a Receiver	23
Session Manager – HNP sessions	24
Desktop Sending for Location Tracking in HipLink Mobile	26
HipLink Mobile Location Tracking using the Primary Send Panel:	26
Tracking Progress for HipLink Mobile Location Tracking	27
View HipLink Mobile Location Details	29

About this Guide

This guide is organized to walk you through the process of Installing and Setting up and using HipLink Mobile. Please refer to the *HipLink Installation and Administration Guide* and the *HipLink User Guide* for complete details about HipLink.

Process Overview

There are several elements in HipLink that need to be modified or confirmed in the process of setting up HipLink Mobile. They are:

- Considerations for application download
- IP and Network setup and definitions
- Global Settings for specific feature enablement
- The HNP (HipLink Notification Protocol) Manager set-up
- Messenger definition and Services start
- Carrier definition
- New User Group definition or existing group permission changes
- User setup if required
- Defining the new receivers

Application Download Options

Customers have two options for the distribution of the HipLink Mobile Applications. This will be coordinated through your Sales Engineer and internal team.

The options available are as follows:

- Download the application from Apple App Store or Google Play Store
- Use an MDM solution to distribute the application to your internal staff. This will make updating the application in the future something that can be managed through Mobile Device Management Updates.

System IP & Network Requirements

Before you can set up your system to be able to use the mobile app, there are a few steps you will need to go through. The mobile application requires direct connectivity to your HipLink server and thus access through defined ports.

IP Considerations

Please be sure to confirm the following:

- If Mobile application users will be using their devices from locations outside of your organization, there must be an external IP address accessible to these devices which will route mobile application traffic back to the HipLink server.
- You will need to verify which ports you will be using for the HNP service (5222 for example), and make sure both these ports are Inbound open.
- Verify the networking infrastructure has port forwarding/NATing enabled between the external and internal IP addresses.

Port Requirements

The Mobile Application does require firewall modifications but HipLink has developed its requirements to separate inbound and outbound ports. The application only uses one direction for each port.

Host	Port	Protocol	Type	Remote	Purpose
HipLink Server	5222 default	TCP	Inbound <====	HipLink HNP Clients	HipLink communication over persistent connection between HipLink server and client apps. The port can be changed.
HipLink Server	5223 default	TCP	Inbound <====	HipLink HNP Clients	HipLink clients communicate with HipLink server. This port is configurable and can be changed.
HipLink Server	443	TCP	Outbound >====	APNS Gateway	Push notification handoff to APNS gateway through HTTP/2 provider API [api.push.apple.com]
HipLink Server	5235	TCP	Outbound >====	GCM Gateway	Push notification handoff to GCM gateway [gcm.googleapis.com]
HipLink Server	5236	TCP	Outbound >====	GCM Gateway	Push notification handoff to GCM gateway [gcm-staging.googleapis.com]
HipLink Server	587	TCP	Outbound >====	HipLink SMTP Relay Server	Push notification fallback to SMS through HipLink SMTP Relay Server [mail11.myoutlookonline.com]
iOS App	5223	TCP	Outbound >====	APNS Gateway	iOS device persistent connection to APNS gateway to register and receive push notifications
iOS App	443	TCP	Outbound >====	APNS Gateway	iOS device persistent connection to APNS gateway to register and receive push notifications, if 5223 outbound port is inaccessible
Android App	5228	TCP	Outbound >====	Google Play Services	Android device persistent connection to Google Play Services gateway to register and receive push notifications

IMPORTANT NOTE: Due to the nature of the required ports for the HipLink Mobile Application, it is common that these ports are not open by default. Please verify the HNP service ports are not blocked by either internal routers or firewalls.

License Key

Check the License Key

The first thing to check is your license key on your HipLink server. In order to use various features like the HNP Manager, Support Basic Mobile Usergroup or Support Advance Mobile Usergroup the license key must support it. To verify your license key supports the HipLink Mobile App, on your HipLink server navigate to the Sys Admin menu at the top of the screen, then navigate to the Upgrade & Maintenance section and click on the Install License link. Within the Install License panel, you can scroll down until you see the HNP Manager, Basic Mobile Usergroup or Advance Mobile Usergroup Supported line. If you see a check next to this feature, it is enabled and you may continue to the next step. If no, check with your administrator to make sure this feature is purchased.

Mobile User Group Permission & Control Policy Overview

Permissions for HipLink Mobile receivers can be set from the Mobile User Group.

This overview gives the administrator a high-level view of the structure available. Each of these aspects is covered in detail in the designated section.

1. **Mobile User Group:** The permissions set for HipLink Mobile receivers assigned in their Mobile User Group settings.
2. **Remote Administration:** The permissions assigned to an individual receiver through Advanced Messaging > Remote Administration feature.

The application of these permissions has certain dependencies that are explained in the following table:

Mobile User Group	Remote Administration	Permissions on Device
Enable	Enable	Enable
Enable	Disable	Disable
Enable	Enable / Disable	Enable
Enable	Enable / Disable	Disable
Disable	Enable / Disable	Disable

Setting up HipLink Mobile

Global Settings

There is a configuration settings screen on HipLink Server named Global Settings. This is very important to go through this section and made configuration changes before starting with the app usage.

There are different sections on Global Settings but following are some important areas that needs to be configured properly:

- **Response CC:** This feature sends alert responses from the recipients of the message to all participants.

Global Settings ?

The screenshot shows the 'Global Settings' interface. On the left is a sidebar with 'Settings Types' including Common, Receiver, Recipient User, Message Sending (selected), Common, Response CC (selected), Secure Web Dispatch, Departments, Session, Email Server, HTTP Proxy, Automatic User Disable, Direct Send, and Message Campaign. The main content area is titled 'Message Sending > Response CC' and contains the following settings:

- Enable Response CC for Send panels to notify the selected recipients of the receivers' responses.**
- Response CC**
- Enable Response CC:** Yes
- Response CC Message Subject Template ***: `[@MsgSubject][@JobID]`
- Response CC Message Template ***: `Response CC Message Body: [@MsgBody] sent by [@SenderName]`
- Automatically CC All Receivers & Groups From ?**: HNP Device, GUI, API

- **Enable Response CC:** Enable/Disable response cc functionality
- **Response CC Message Subject Template:** Response CC Alert subject template to be sent to the participants
- **Response CC Message Template:** Response CC Alert body template to be sent to the participants
- **Automatically CC All Receivers & Groups:** All the alert participants will be automatically added to the Response CC participants list based on the selection from this drop down, else sender need to add the receiver into the response cc list manually. This dropdown has following values:
 - **HNP Device,** Alerts sent from HNP devices
 - **GUI:** Alerts sent from GUI
 - **API:** Alerts sent through CLI or Gateways to the HipLink system
- **Other Settings**
 - Setup 'HipLink Hostname' for your server. HipLink App will use this as part of URL to access different app features.
 - Setup 'HipLink Port'. HipLink HNP services will be accessible to HipLink App over this port.
 - Setup 'HipLink Host Type' as Secure (HTTPS)

Global Settings ?

Settings Types	Other
Common	Define synchronization path; select an SMTP carrier for sending notification emails.
Response CC	
Secure Web Dispatch	
Departments	
Session	
Email Server	
HTTP Proxy	
Automatic User Disable	
Direct Send	
Message Campaign	
Receiver Groups Audit	
Location Extraction	
Other	

Other Settings	
Synchronization path	Email Notification Carrier SMTP
HipLink Hostname newhnp.hiplink.com	HipLink Port 5223
HipLink Host Type Secure (https)	HipLink HTTP API https://newhnp.hiplink.com/cgi-bin/action.exe

Note: Fields marked with an asterisk * * * are mandatory.

[Edit](#)

- **Receiver Settings**
 - Enable "Receiver Attributes"
- **Under Message Sending Settings**
 - Also check "Enable Confidential Messaging" checkbox
- **Location Extraction:** This feature must be enabled if you are using the HipLink Mobile Location Tracking module in HipLink mobile.

Global Settings ?

Settings Types	Location Extraction
Common	Extract target location address from message body or from address fields and send to recipients.
Response CC	
Secure Web Dispatch	
Departments	
Session	
Email Server	
HTTP Proxy	
Automatic User Disable	
Direct Send	
Message Campaign	
Receiver Groups Audit	
Location Extraction	
Other	

Enable No	
Place Name Pattern	Address Pattern
Cross Street Pattern	City Pattern
Latitude Pattern	Longitude Pattern
Extract Location From ? Location Tracking Fields	

Note: Fields marked with an asterisk * * * are mandatory.

[Edit](#)

Location Extraction allows admin users to enable/disable the extraction of the incident location from the content of an alert and sends it as part of the message body to targeted devices.

- **Enable:** Enable/Disable location extraction feature for receivers. If unchecked, the location will not be extracted from alert body but a location entered using the Location Tracking fields from send panel will still be functional.
- **Place Name Pattern:** Define regex pattern to extract place name from alert body
- **Address Pattern:** Define regex pattern to extract address from alert body

- **Cross Street Pattern:** Define regex pattern to extract cross street from alert body
- **City Pattern:** Define regex pattern to extract city from alert body
- **Latitude Pattern:** Define regex pattern to extract latitude coordinates from alert body
- **Longitude Pattern:** Define regex pattern to extract longitude coordinates from alert body
- **Extraction Location From:** Extract Location field has two dropdown values:
 - Location Tracking Fields
 - Alert Message Body

Based on the selection, it sets the priority from which field location will be extracted incase alert has data in both the fields.

- In case the selected field doesn't has location values the URL will be extracted from the other, if available.

HNP Manager Configuration

HNP Manager is an interface to manage different HipLink Mobile application settings. It gives the user control over to enable/disable advanced HipLink App features.

When setting up the HNP Manager there are different sections on HNP Configuration:

- General Settings
- Advanced Settings
- Push Notifications
- Secure Internet Call
- HipLink Alert

General Settings

This section is used to setup general configuration settings for the HipLink Mobile application.

HNP Configuration
Disable

General Settings
Advanced Settings
Push Notifications
Secure Internet Call
HipLink Alert

Persistent Connection

Enable Persistent Connection
Yes

Server Certificate (for TLS) C:/Program Files (x86)/HipLink Software/HipLink/config/hnp_cert.pem	Server Port 5222
Server Private Key C:/Program Files (x86)/HipLink Software/HipLink/config/hnp_key.pem	Acknowledgment Timeout 15 second(s)
Server Private Key Passphrase *****	

Session Settings

Access Token Expiry
480 minute(s)

Misc Settings

Organization Name HipLink Softwares	HNP Communication Logging Yes
--	----------------------------------

Edit

Persistent Connection: A persistent connection allows HipLink Mobile apps to remain connected with the HipLink Server over a persistent socket connection while running in foreground. Persistent connection allows a direct connection between application and the server.

- **Enable Persistent Connection:** Enable/Disable persistent connection functionality
- **Server Certificate (for TLS):** Provide the path to the Server Certificate to be used for TLS connection. For the server certificate that comes bundled-in with HipLink, the path is provided by default
- **Server Private Key:** Provide the path to the Server Private Key used for the above certificate. Leave the default value if you are using the default certificate.
- **Server Private Key Passphrase:** Server private key passphrase to secure the communication channel
- **Server Port:** HipLink Mobile Apps connect persistent connection over this port with server
- **Acknowledgment Timeout:** If message is not received on the mobile app before this time (in seconds) the server will send message through alternate push notification channel

Session Settings: Session settings reset the mobile application session after configured time.

- **Access Token Expiry:** Application session refresh automatically on the timeout. This process is seamless and invisible for the users but helps in securing the application session.

Misc. Settings: These are the additional settings used in the application

- **Organization Name:** This is the text field and the name you enter here will be shown on Mobile App Login screen. This feature will be part of Universal Application builds available on Apple App Store and Google Play Stores
- **HNP Communication Logging:** If enabled this will write additional logs on disk

Advanced Settings

This section is used to setup advanced features for HipLink Mobile

HNP Configuration Enable

General Settings **Advanced Settings** Push Notifications Secure Internet Call HipLink Alert

Location Tracking

Enable Location Tracking
No

Maximum Tracking Duration
30 (Minutes)

Google Maps API Key

Quick Dispatch

Enable Quick Dispatch
No

Carrier For Email Messages

Carrier for text messages

HipLink Mobile Data Archive

Archive Data After
30 day(s)

Request Page Size
100

Edit

Location Tracking: Allows you to see information about the incident location, who is responding to an alert, routing information, map navigations, and real-time location of other responders on the map from HipLink Mobile as well as from server.

- **Enable Location Tracking:** Enable/Disable location tracking feature from server
- **Maximum Tracking Duration:** Default time in minutes for which device keep transmitting its location if has confirmed the received alert
- **Google Maps API Key:** Google Maps API value to be used by the HNP client apps to show map directions on client

Quick Dispatch: Quick dispatch allows mobile application users to send an alert to users who are not registered to HipLink system.

- **Enable Quick Dispatch:** Enable/Disable the functionality for mobile app users
- **Carrier for Email Messages:** Alerts sent to unregistered users email addresses will be processed through this carrier
- **Carrier for Text Messages:** Alerts sent to unregistered users phone numbers will be processed through this carrier

HipLink Mobile Data Archive: HipLink Mobile Data archive allows the users to archive their data on the server for a configured number of days. Data archived on the server will be synced across multiple devices when the user logs in.

- **Archive Data After:** Data older than configured number of days will be cleaned from the server automatically
- **Request Page Size:** Configured number of records will be sent to devices in response to each data sync request. Devices will keep requesting data until complete data is sent from server

Push Notifications

This section is used to setup push notifications for Android mobile app devices

The screenshot shows the 'Push Notifications' settings screen. At the top, there are navigation tabs: 'General Settings', 'Advanced Settings', 'Push Notifications' (selected), 'Secure Internet Call', and 'HipLink Alert'. Below the tabs, there are two main sections: 'Push Notification Settings' and 'Push Reminder & Fallback Settings'. In the 'Push Notification Settings' section, 'Enable FCM (Firebase Cloud Messaging)' is set to 'Yes'. Below this, 'Server Id' is '405308864899' and 'Server Key' is 'AlzaSyA5fqNe6oBp1uGZRMuq72UXISw6zI8L24g'. In the 'Push Reminder & Fallback Settings' section, 'Push Reminder Attempts' is '3 (Attempts)' and 'Push Reminding Timeout' is '30 (Seconds)'. At the bottom, 'Enable HNP Message Fallback' is set to 'Yes'.

Push Notification Settings:

Apple Push Notification Service is configured and hardcoded in HipLink server.

- **Enable FCM:** Enable/Disable Google FCM service for Android devices
- **Server ID:** FCM server ID
- **Server Key:** FCM server key

Note: It is mandatory to setup push notifications, otherwise app will not be able to receive messages in real-time.

Push Reminder & Fallback Settings: Push reminder & fallback settings section allows to setup additional reminders in the event HipLink is not able to get the message to the phone in first attempt.

- **Push Reminder Attempts:** In addition to first push these many reminder push notifications will be sent to devices if device is not able to receive the message in first push
- **Push Reminding Timeout:** If device is not able to get the message in first push, reminder push will be sent after configured timeout value
- **Enable HipLink Mobile Text Message Failover:** In the event the phone does not get the message and all push reminder attempts are exhausted, an SMS text message will be sent to the phone number defined to notify him/her about pending message on the server. This is very rare and usually happens when the phone is out of network or not connected to server. The User is notified regarding the pending messages with a text message to the phone number defined. The message content is not sent but an alert to login to HipLink.

Secure Internet Call

This section is used to setup HipLink VoIP call functionality between HipLink Mobile clients. It does require an account with Tokbox for the service to work.

HNP Configuration Disable

General Settings Advanced Settings Push Notifications **Secure Internet Call** HipLink Alert

VoIP Call Configuration Settings

Enable Secure Internet Call Yes	Tokbox API ID 45953442
Secure Key ce083a6309961557819bf7efc01ae11074d6fe8f	

VoIP Call Configuration Settings: If enabled an option will be shown with HipLink Mobile contact to dial a secure audio or video call.

- **Enable Secure Internet Call:** Enable/Disable secure internet call feature
- **Tokbox API ID:** Tokbox API Id
- **Secure Key:** Tokbox API secure key

To setup this feature, the organization needs to buy subscription from Tokbox to setup their account or contact HipLink.

HipLink Alert App

This section is used to setup HipLink Alert. HipLink Alert is light-weight version of HipLink that is only used for one-way broadcast alerts that doesn't require receiver licenses. This feature must be licensed separately from the standard HipLink Mobile licenses.

General Settings Advanced Settings Push Notifications Secure Internet Call **HipLink Alert**

HipLink Alert Settings

Enable HipLink Alert Yes	Push Reminder Attempts 1 (Attempts)
Expiry Time 1440 (Minutes)	Push Reminding Timeout 10 (Seconds)

- **Enable HipLink Alert:** Enable/Disable HipLink Alert. If enabled HipLink Alert will be able to connect to the server and an additional option will appear on send panel to send broadcast alert to all connected HipLink Alert phones.
- **Expiration Time:** When an admin sends a broadcast alert from the server, all connected devices will get the message. If any new devices login to the service before the expiry time they will also get the message but the devices connect to server after timeout won't be able to get the message and broadcast alert will expire.
- **Push Reminder Attempts:** Configured number of push notifications will be sent to connected offline devices
- **Push Reminding Timeout:** Timeout value between two consecutive push reminders
- **Access Code:** This code value is used for HipLink Alert app authentication purposes and users are required to enter this value in HipLink Alert app after entering their organization Id to connect with the correct server

Manage Mobile User Group

Mobile User Group defines the level of access that a HipLink Mobile receiver will have to the features and contacts. Administrators can create new Mobile User Groups, in addition to the predefined group **Basic Mobile User Group**. All of the existing Mobile User Groups are displayed as entries in the drop-down field on HipLink Mobile Receiver Add/Edit page. In addition to that, Permissions of Department, Templates, Response Action, General Policy and few General Settings for HipLink Mobile Client will now be controlled from Mobile User Group.

To access Mobile User Group tab, choose Mobile User Group from Settings section

Settings	Mass Alerts	Recipients	Send	Queues	Reports
Accounts	Integration	HipLink Mobile	Templates		
Users	Alarm Notification Gateway	HNP Configuration	Message Templates		
User Groups	File System Interface	Manage HNP Devices	Schedule Templates		
Mobile User Groups	Email Gateway	Manage HipLink Broadcast Devices	2-Way Actions		
Departments	SNPP Gateway	HipLink Mobile Releases	Feedback		
	TAP Gateway		Response Actions		

From Mobile User Group screen user can Add, Update, and Delete mobile user group.

Mobile User Groups Add Mobile User Group Refresh

Displaying 1 - 16 of 16 records First Back 1 of 1 Next Last

Actions	Mobile User Group Name	Description	Member Count
<input type="checkbox"/>	App Review	Mobile User Group for App Reviews	3
	Default Mobile Usergroup		0
<input type="checkbox"/>	Demonstration Mobile Users	Demo MUG	1
<input type="checkbox"/>	Engineering MUG		15
<input type="checkbox"/>	FirstNet MUG	First Net Demo	2
<input type="checkbox"/>	Franklin County MUG	Franklin County, PA EVAL	10
<input type="checkbox"/>	HipLink Staff MUG	Non-Sysadmin users	9
<input type="checkbox"/>	HipLink Support MUG		1
<input type="checkbox"/>	HipLink-L-MUG		0
<input type="checkbox"/>	Hiplink-MGroup		0
<input type="checkbox"/>	internal mobiles users	internal test MUG	0
<input type="checkbox"/>	PHA-Bahamas MUG	Bahamas Hospital EVAL	29

Delete Copy Rows Refresh

Mobile User Group Name: Shows the name of added mobile user group.

Member Count: Shows total number of HipLink Mobile receivers associated with this mobile user group.

Edit Button: Edit the selected mobile user group from server and new changes should reflect on the HipLink Mobile receiver's device.

Delete: Deletes the selected mobile user group from the server.

Detail icon appearing in Action column with only default mobile user group.

Default Mobile User Groups

Default Mobile User Group gives HipLink Mobile receivers access to receive alerts and messages. The group cannot be edited or deleted.

To view Default Mobile User Group, click on the detail icon against default mobile user group.

View Mobile User Group ?

Mobile User Group Parameters

Name * Description

General Department Response Action Templates **General Policy**

General Policy Settings

<p>Settings Types</p> <ul style="list-style-type: none"> Permissions Configuration System Configuration Inbox Configuration Alert Configuration Message Configuration 	<p>Permissions Configuration ?</p> <p>Receive Alert Yes <input type="text"/></p> <p>Send Alert No <input type="text"/></p> <p>Access Template No <input type="text"/></p> <p>Disable Logout Button No <input type="text"/></p> <p>Allow Compromised Device / Jail Broken Device</p>	<p>Receive Message Yes <input type="text"/></p> <p>Send Message No <input type="text"/></p> <p>Access Custom Actions No <input type="text"/></p> <p>Settings Access Full Access <input type="text"/></p> <p>View Contacts</p>
--	---	--

General Policy Permission Settings

General Policy screen has multiple sections, each section has similar set of permissions grouped together, and this general policy will applied to those entire receiver's mobile devices who have selected this mobile user group.

To add custom Mobile User Group, click on the Add Mobile User Group button on Mobile User Group Panel screen.

General Policy

General Policy Settings

Permissions Configuration

Receive Alert: Yes

Receive Message: Yes

Send Alert: Yes

Send Message: Yes

Access Template: Yes

Access Custom Actions: Yes

Disable Logout Button: Yes

Settings Access: Full Access

Allow Compromised Device / Jail Broken Device

View Contacts

Return to top

Note: Fields marked with an asterisk * * * are mandatory.

Cancel | Reset | Save

After

applying General Policy, do not forget to restart Hiplink Mobile Manager and Push Notification Service.

Permissions Configuration

Permissions configuration controls the access permissions to different features available on mobile app and has default value of 'Yes'.

Each permission dropdown has 2 different possible values:

- **Yes:** User will have access to this permission from client and able to use this feature
- **No:** User does not have access to this permission from client and could not able to use this

Receive Alert: Users will be able to receive Alerts on device if this permission is Yes otherwise, no alerts will be received on device

Receive Message: Users will be able to receive messages on device if this permission is Yes otherwise, no alerts will be received on device

Send Alert: Users will be able to send alerts on device if this permission is Yes otherwise, the Send Alert option does not appear on device

Send Message: Users will be able to send messages on device if this permission is Yes otherwise, the Send Message option does not appear on device

Access Templates: Users will be able to access templates only on device if this permission is Yes otherwise, the template option does not appear on device

Access Custom Actions: Users will be able to access custom actions only on device if this permission is Yes otherwise, the custom actions option does not appear on device

Disable Logout Button: If enabled, users will not be able to Logout from the application manually because Logout button will not be accessible from the application.

Settings Access: Settings drop down has multiple options and each option applies different permission set on application settings screen on device

- **Full Access:** Users will have full control over the application settings and they can customize all settings from their device
- **Limited Access:** Users will have full control over the application settings except 'Security and Advanced Setup' which will become Read Only
- **Very Limited Access:** User will be able to customize settings for 'My Profile', 'Message Tones' and 'General Settings' only, all other sections become Read Only
- **Read Only:** Users will not be able to customize settings on device and all sections become Read Only
- **Lock:** Users will not be able to access Settings from device and setting option will hide on device screen

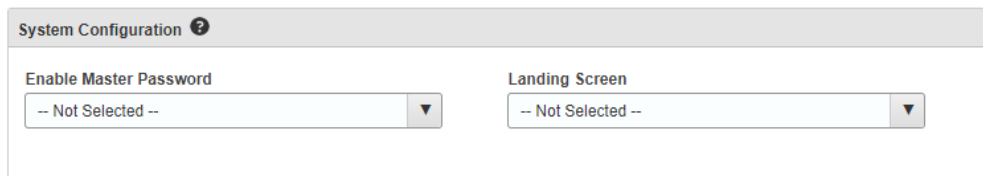
Allow Compromised Devices / Allow Jail Broken Devices: If enabled, jail broken or compromised devices will also be able to use HipLink Mobile and connect with the server otherwise, these devices will not be able to connect with HipLink server.

View Contacts: Users will be able to access contacts only on device if this permission is yes otherwise, the contacts option does not appear on device.

View Access Alert Topic: Users will be able to access alert topic only on device if this permission is yes otherwise, the alert topic option does not appear on device.

System Configuration

System configuration controls the app security related configuration settings



The screenshot shows a 'System Configuration' window with a title bar containing a question mark icon. Below the title bar, there are two dropdown menus. The first is labeled 'Enable Master Password' and the second is labeled 'Landing Screen'. Both dropdown menus currently display '-- Not Selected --'.

Enable Master Password: If this permission is ON, a notification will be sent to the device to setup a Master Password on client application. This can be a numeric code or fingerprint.

Landing Screen: Landing screen allows user to set default landing screen every time user launch hiplink application.

Inbox Configuration

Inbox configuration section has message/alert view and settings permissions grouped together

General Department Response Action Templates **General Policy**

General Policy Settings

Settings Types	Inbox Configuration ⓘ Auto Delete -- Not Selected -- Enforce Confidential Messaging -- Not Selected -- Clean Sent Alerts -- Not Selected -- (Days) Clean Messages -- Not Selected -- (Days) Save Sent Alerts -- Not Selected -- Clean Inbox Alerts -- Not Selected -- (Days) Clean Draft Alerts -- Not Selected -- (Days) Access Media Library -- Not Selected --
Permissions Configuration	
System Configuration	
Inbox Configuration	
Alert Configuration	
Message Configuration	

[Return to top](#)

Note: Fields marked with an asterisk * * * are mandatory.

Cancel | Reset | **Save**

Auto Delete: If enabled, alerts will be deleted from client app as soon as user responds to an alert they receive. This feature is only for Android and Desktop client apps.

Save Sent Alerts: If enabled, all alerts sent from client will be saved as sent items on client app

Enforce Confidential Messaging: If enabled, confidential messaging will be enabled by default for all alerts and user will not be able to send any alert without the confidential check enabled

Clean Inbox Alerts: N day's older inbox data will be archived on client application per the defined number of days

Clean Sent Alerts: N day's older sent alerts from inbox will be archived on client application per the defined number of days

Clean Draft Alerts: N day's older draft alerts from inbox will be archived on client application per the defined number of days

Clean Messages: N day's older chat messages from chat conversations will be archived on client application per the defined number of days

Access Media Library: If disabled, users will not be able to access media library from client application when sending an attachment with alert or message

Alert Configuration

Alert configuration section has configuration settings specific to alert ringtones. There are five different types of severity alerts and user can set custom ringtone for each severity alert using this section and from device settings as well.

General Department Response Action Templates **General Policy**

General Policy Settings

- Settings Types
- Permissions Configuration
- System Configuration
- Inbox Configuration
- Alert Configuration**
- Message Configuration

Alert Configuration ?

Normal Alert

Ring Counter: -- Not Selected -- Ring-tone: -- Not Selected --

Important Alert

Ring Counter: -- Not Selected -- Ring-tone: -- Not Selected --

Warning Alert

Ring Counter: -- Not Selected -- Ring-tone: -- Not Selected --

[Return to top](#)

Note: Fields marked with an asterisk * * * are mandatory.

[Cancel](#) | [Reset](#) | [Save](#)

Message Configuration

Message configuration section has configuration settings specific to chat message ringtones. Users can send two different types of severity chat messages and can set custom ringtone for each of those using this section and from device settings as well

General Department Response Action Templates **General Policy**

General Policy Settings

- Settings Types
- Permissions Configuration
- System Configuration
- Inbox Configuration
- Alert Configuration
- Message Configuration**

Message Configuration ?

Normal Message

Ring Counter: -- Not Selected -- Ring-tone: -- Not Selected --

Emergency Message

Ring Counter: -- Not Selected -- Ring-tone: -- Not Selected --

[Return to top](#)

Note: Fields marked with an asterisk * * * are mandatory.

[Cancel](#) | [Reset](#) | [Save](#)

Template Permission Settings

On the Add/Edit Mobile User Group page, the HipLink administrator can set permissions that allow a HipLink Mobile receiver to view and use a template. All existing templates are listed on the Template tab. Permissions can be assigned by checking the checkbox against the Template.

General Department Response Action **Templates** General Policy

Assign Templates Permissions

Templates	Use Templates
0 - Confirmation Code	<input checked="" type="checkbox"/>
00 - H - Hosp Trauma Lv1	<input checked="" type="checkbox"/>
00 - PS - Active Shooter v2	<input type="checkbox"/>
00 - PS - Off Duty Overtime	<input checked="" type="checkbox"/>
00 - PS - Officer Assist2	<input checked="" type="checkbox"/>
00 - PS - SWAT Callout	<input checked="" type="checkbox"/>
00 - URGENT Employee Product Line Emergency	<input checked="" type="checkbox"/>
01- Demo Grp Broadcast	<input checked="" type="checkbox"/>
012 - HipLink Mobile download instructions	<input type="checkbox"/>
A Team Meeting	<input checked="" type="checkbox"/>
All hands to assembly room	<input checked="" type="checkbox"/>
CODE BLACK	<input checked="" type="checkbox"/>
CODE GREEN	<input checked="" type="checkbox"/>
CODE ORANGE	<input checked="" type="checkbox"/>
CODE PINK	<input checked="" type="checkbox"/>
CODE PURPLE	<input checked="" type="checkbox"/>
CODE RED	<input checked="" type="checkbox"/>
CODE SILVER	<input checked="" type="checkbox"/>
CODE YELLOW	<input checked="" type="checkbox"/>
Fire at the plant - Hershey	<input checked="" type="checkbox"/>
H - Air Pollution	<input checked="" type="checkbox"/>
H - Aircare	<input checked="" type="checkbox"/>
H - Appointment Confirmation	<input type="checkbox"/>

Response Action Permission Settings

On the Add/Edit Mobile User Group page, the HipLink administrator can set permissions that allow a HipLink Mobile receiver to view and execute a response action. Any existing response action are listed on the Response Action tab; Permissions can be assigned by checking the checkbox against the response action.

General Department **Response Action** Templates General Policy

Assign Response Action Permissions

Response Action	Type	Execute Response Action
--HL2Way Integration	Reply	<input type="checkbox"/>
0	Reply	<input type="checkbox"/>
1	Reply	<input type="checkbox"/>
Accept Message	Reply	<input type="checkbox"/>
Accept Message MTD	Reply	<input type="checkbox"/>
Accept_Servicenow	Standard	<input checked="" type="checkbox"/>
Call Security Staff	Standard	<input checked="" type="checkbox"/>
Confirm	Reply	<input type="checkbox"/>
Date Info	Standard	<input checked="" type="checkbox"/>
Decline Message	Reply	<input type="checkbox"/>
defaultconfirm	Reply	<input type="checkbox"/>
Driver Log	Standard	<input checked="" type="checkbox"/>
Email to Shoab	Standard	<input checked="" type="checkbox"/>
Failed Alerts Notification	Reply	<input type="checkbox"/>
IT service check	Standard	<input checked="" type="checkbox"/>

Department Permission Settings

On the Add/Edit Mobile User Group page, the HipLink administrator can set permissions that allow a HipLink Mobile receiver to send alert and message to the Receiver and Receiver Group of a specific Department.

General **Department** Response Action Templates General Policy

Assign Departments All ▾
 Departments that do not have any permissions checked off will not be visible by the Mobile User Group in any screen.

Department	Department Receivers		Department Groups	
	Send		Send	
Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1 - HipLink Corporate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Click to select/unselect all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

App Review ▾ [Add Department](#)

[Return to top](#)

Note: Fields marked with an asterisk "*" are mandatory. Cancel | Reset | [Save](#)

General Permission Settings Definitions

Add Mobile User Group ?

Mobile User Group Parameters

Name * Description

General **Department** Response Action Templates General Policy

Assign General Permissions

Allow	Permission	Allow	Permission
<input type="checkbox"/>	ability to override Receiver On-Call Status	<input type="checkbox"/>	automatically assign permission to newly created Templates
<input type="checkbox"/>	automatically assign permission to newly created Response Actions		
<input type="checkbox"/>	Click to select/unselect all		

[Return to top](#)

Note: Fields marked with an asterisk "*" are mandatory. Cancel | Reset | [Save](#)

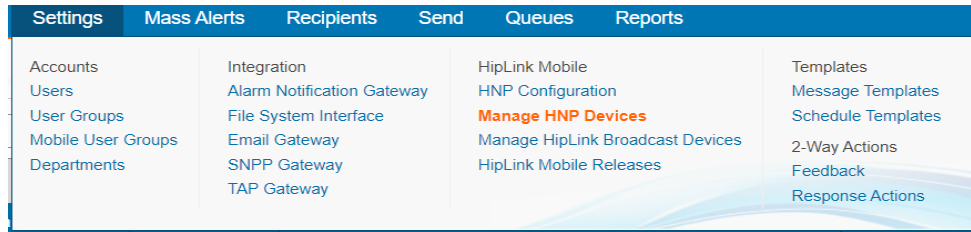
Ability to Override Receiver On-Call Status: This option will allow HipLink receiver to send an alert/messages to unavailable/offline receiver.

Add All New Created Response Actions to This Group: Enabling this option will automatically assign permission to mobile user group to add any newly created response action in the system.

Add All New Created Templates to This Group: Enabling this option will automatically assign permission to mobile user group to add any newly created template in the system.

Manage HipLink Mobile Devices

Manage HNP Devices screen allows HipLink Admins to monitor and control activated device list. To access the Manage HNP Devices screen, choose Manage 'Manage HNP Devices' from Settings section



From Manage HNP Devices screen user can Delete, Block and Unblock activated device activations

Action	Receiver Na...	User Name	Platform	Device Key	OS Version	App Version	Blocked	Blocked Since
<input type="checkbox"/>	Nasir1	iPhone-iOS12, ...		bb9ea099-3c8d-49f2-b41a-ce89784...	6.0.1	6.5.3.28.0	No	
<input type="checkbox"/>	Nasir	Nasir, Muhammad		7ce4b2a8-625a-4b47-a682-c03f0ad...	iOS-iOS-12.0.1-...	7.0.1.13.0	No	
<input type="checkbox"/>	Nasir2	Nasir2		ee298906-ba8a-4e6e-9046-b3e70b...	8.0.0	6.5.3.28.0	No	

At the bottom of the table, there are buttons for **Delete**, **Block**, **Unblock**, **Copy Rows**, and **Refresh**.

Number of Activated HNP Receivers: Shows total number of activated HipLink Mobile receivers out of allowed license limit


Delete: Deletes the selected device activation from the server

Block: Blocks the selected device activation from server and users won't be able to login to HipLink server

Unblock: Unblocks the selected device activation from server and allow users login to HipLink server

Detail icon appearing in Action column with each record shows the detail of the connected receiver including his location

Device Details [Close]

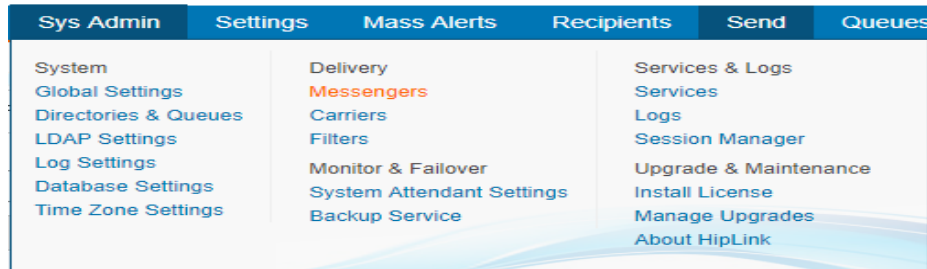
User Full Name: yury	Vendor: Apple	Last Known Device Location:  <p>The map shows the state of California with major cities labeled: Sacramento, San Francisco, San Jose, Los Angeles, San Diego, and Las Vegas. A red location pin is placed in the San Francisco area. The map includes the Google logo and the text 'Map data ©2018 Google, INEGI'.</p>
Device Key: 6cd16870-91b7-43d6-b09b- fe0888cc4994	Platform: iOS	
Activation Time: Fri Oct 12 12:23:11 2018	OS Version: iOS-iOS-11.4.1-Apple-iPhone	
Last IP Address: 172.16.10.19	App Version: 7.0.1.13.0	
Push Notification Type: APNS	Blocked: No	
Push Notification Device ID: 56d612dc8f424066b6c2a8fdda8ee8 718b42f6dbc13ba6c9b171a4333f5d a267		

[Close]

Creating a Messenger for HipLink Mobile

A messenger and carrier are mandatory on your HipLink server in order for messages to work. You must create a messenger on the server before creating a carrier. To create a messenger:

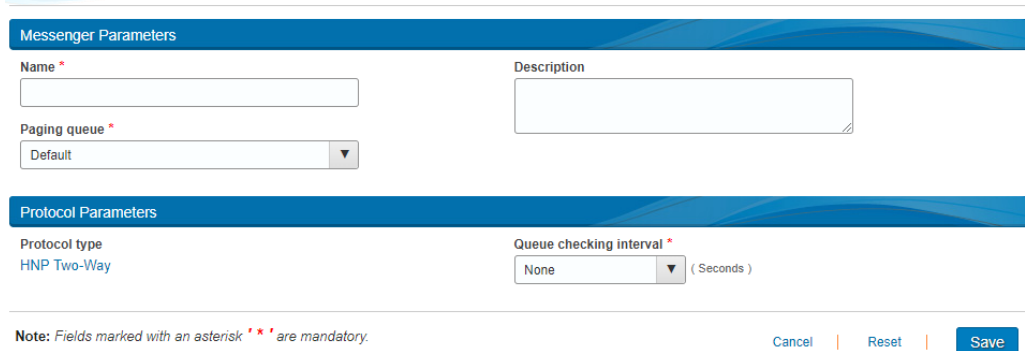
- Choose Messengers under the Sys Admin



From Messengers screen

- Choose 'HipLink' from Protocol and 'HNP 2 Way' in the list and click on Add Messenger button
- **Name:** Enter Messenger name

Add HNP Two-Way Messenger ?

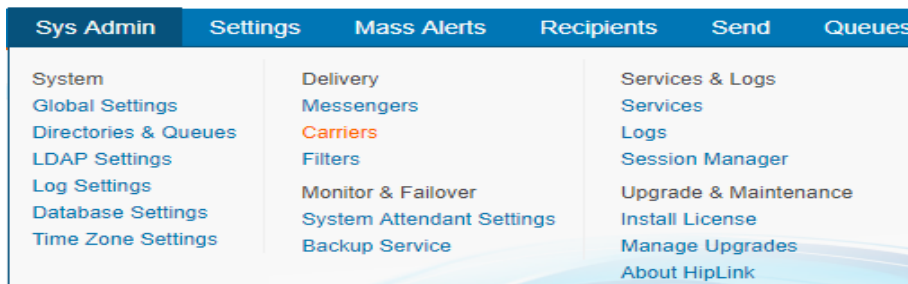
A screenshot of the 'Add HNP Two-Way Messenger' configuration form. The form is divided into two sections: 'Messenger Parameters' and 'Protocol Parameters'. In the 'Messenger Parameters' section, there is a 'Name *' text input field, a 'Description' text area, and a 'Paging queue *' dropdown menu currently set to 'Default'. In the 'Protocol Parameters' section, there is a 'Protocol type' dropdown menu set to 'HNP Two-Way' and a 'Queue checking interval *' dropdown menu set to 'None' with '(Seconds)' next to it. At the bottom of the form, there is a note: 'Note: Fields marked with an asterisk ** are mandatory.' and three buttons: 'Cancel', 'Reset', and 'Save'.

- **Description** (Optional): Enter description for your messenger
- **Paging Queue:** If you are using multi-queue license, select a paging queue to assign this messenger service to process messages from that specific queue only
- **Queue checking Interval** (seconds): Messenger will check assigned queue after configured time to process any pending messages. None is the default value which checks queue multiple times within a second.

Creating a HipLink Mobile Carrier

To create a HipLink Mobile carrier:

- Choose Carriers under the Sys Admin



From Carriers screen

- Choose 'HipLink' from Protocol and 'HNP 2 Way' in the list and click on Add Carrier button


Add HNP Two-Way Carrier

Carrier Parameters

Name *	<input type="text"/>	Paging queue *	Default ▼
Description	<input type="text"/>	Backup carrier	▼
Device Type	None ▼	Backup carrier 2	▼
		Confidential message dispatch type	Allowed ▼

HNP Two Way Protocol Parameters

Logout User Settings *	Put on hold in Waiting Queue ▼	Maximum Lifespan of Message *	10 min(s) ▼
Push on Logout *	Enabled for last device ▼		

[Return to top](#) 

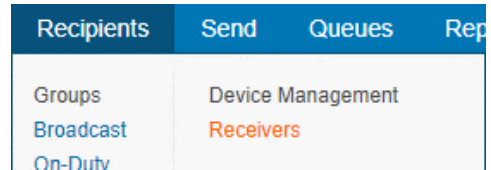
Note: Fields marked with an asterisk * * * are mandatory.

Cancel | Reset | **Save**

- **Name:** Enter carrier name
- **Description** (Optional): Enter description for your carrier
- **Device Type:** Choose your device type icon
- **Paging Queue:** If you are using multi-queue license, select a paging queue to assign this messenger service to process messages from that specific queue only
- **Logout User Settings:** There will be 2 different options shown in **Logout User Settings** dropdown
 - **Fail Backup Plan:** If selected, Messages sent to Logged out HNP receivers will be directly marked as failed and delivered to receiver through its alternate configured channel if configured
 - **Put On-Hold in Waiting Queue:** If selected, Messages sent to Logged out HNP receivers will be moved to waiting queue and a push message will also be sent
- **Push on Logout:** There will be 2 different options shown in **Push on Logout** dropdown
 - **Enabled for Last Device:** If enabled, Push notification will be sent to Logged out HNP receivers on sending any message to logged out receiver
 - **Disabled:** If Disabled, push will not be sent on sending message to Logged out HNP receiver
- **Maximum Lifespan of Message:** This is the total lifespan of a HipLink Message on HipLink server.
When a HipLink message is sent server will keep this message into his queue till the configured time and query for its response as well, but incase message is failed to deliver or receiver is unable to respond the message in configured time, server will discard this message from its queue and does not perform any action on responding this message after configured time.

Creating a Receiver

To create a receiver, choose Receivers from Recipients section



Click on the Add Receiver button at the right top of the receiver screen.

Primary Membership Schedule Receiver

Receiver Status: Available

General Information


Receiver Name *
PamLaPineLaptop

Description
DESKTOP (Laptop) Pop-up

First Name
Pamela

Last Name
LaPine

Email Address
pamela@hplink.com
 Email CC Email Fallback


Change

Time Zone
Server Time

Member of Department *
Default

Attributes

<input type="checkbox"/> French - conversational	<input checked="" type="checkbox"/> French - Fluent	<input checked="" type="checkbox"/> German	<input type="checkbox"/> Korean	<input type="checkbox"/> Mandarin
<input type="checkbox"/> Spanish	<input checked="" type="checkbox"/> West Coast Time	<input type="checkbox"/> Mountain Time	<input type="checkbox"/> Central Time	<input type="checkbox"/> East Coast Time
<input checked="" type="checkbox"/> C Level	<input type="checkbox"/> VP	<input checked="" type="checkbox"/> Director	<input type="checkbox"/> Regional Manager	<input type="checkbox"/> Manager
<input checked="" type="checkbox"/> Supervisor	<input checked="" type="checkbox"/> Anesthesiology	<input type="checkbox"/> Cardiology	<input type="checkbox"/> Radiology	<input checked="" type="checkbox"/> IT Support

Carrier Information

Receiver Type
2 Way
 Keep Alpha Characters in Numeric

Primary Carrier/Delivery *
HNP Carrier for DeskTop

Primary Number/PIN/Username *
pamlapinelaptop

Authentication Type
HipLink

HNP Password is Set
Change Password

Alternate Carrier/Delivery

Alternate Number/PIN/Username

Call Back Number
(408) 667-4653
 Use for Voice Send

Text Fallback Number
4086674653

Mobile User group

Security Code
45678

Mobile User Group *
sysAdmin MUG

Receiver Signature
Pam LaPine - HipLink Software - 408-399-6120

Advanced Messaging

Enable Advanced Messaging Remote Administration

Send a test message after 'Save' operation

Note: Fields marked with an asterisk * * * are mandatory.

Cancel | Reset | Save

There are several fields those needs to be filled in properly to uniquely identify and differentiate receivers from other receivers.

Fields marked with asterisk are the mandatory fields

Name: Enter a unique name for the receiver

Description: This field can be a very helpful look-up tool when trying to identify receivers within HipLink. The description can be viewed in the send screens as well as the detail screens in the Favorites list on the HipLink Mobile app. We recommend that you establish a common theme for your organization for this field such as department or specialty, location and even phone numbers. This information can be searched on in all send screens and on the mobile app.

Primary Carrier/Delivery: Select the carrier you created in the previous step

Primary PIN: This will automatically be populated based on the receiver name but can be edited to your user preferences. This will become the User ID used to login from the mobile smartphone.

HNP Password: Enter the password you would like to use for the receiver. This will have to be entered from the Mobile Application for authentication.

Receiver Type: Select 2-Way

Receiver Attributes: If enabled in your license key, you can assign a defined Attribute in this area. These Attributes are used for ad-hoc lookup in the Attribute send as well as in the Favorites in the Mobile App.

Receiver Email: This should only be defined if the device owner wishes to have a copy of messages sent to their email and the email system is secure.

Owner First Name, Last Name: These are also important fields to be sure to enter accurate data. This is used in the send screens for lookups and in the Mobile App for *Favorites* queries.

Mobile User Group: Select the Mobile User Group to assign HipLink Mobile permissions to the HipLink Mobile receiver.

Receiver Signature: Enter receiver signature that will determine the signature of the Sender of a message when sending from the device.

Call Back Number: This is used for a User to give the number they wish people to reach them on. Many times, this won't be their cell phone number but maybe an office or a department central phone number. This number will be shown in the Contact details screen of the Mobile App.

Text Failover Number: The failover number should be entered with a 1 and then the ten-digit cell phone number. If for some reason HipLink can't deliver a message it will send a notice to the User as a standard SMS text message and tell them a message is waiting, please login to HipLink. All HipLink Mobile Users should have a failover number designated.

Session Manager – HNP sessions

To access HNP Sessions tab, Choose Session Manager from Sys Admin section and open HNP Sessions tab from Session Manager screen

Sys Admin	Settings	Mass Alerts	Recipients	Send	Queues
System	Delivery			Services & Logs	
Global Settings	Messengers			Services	
Directories & Queues	Carriers			Logs	
LDAP Settings	Filters			Session Manager	
Log Settings	Monitor & Failover			Upgrade & Maintenance	











This tab shows all the HNP users that are logged into the device application, and that have active sessions present. When user logout from the application their session record will be removed from this panel but remain available on Manage HNP Devices screen. The panel also displays their IP addresses, Client names and OS versions.

Session Manager Refresh

User Sessions **HNP Sessions**

search by keyword Receiver A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Others All

Apply Filter Displaying 1 - 37 of 37 records First Back 1 of 1 Next Last Advanced

Actions	Receiver Name	Assigned Mobile Use...	Device Key	Created At	IP Address	Platform	OS Version	App Version	Access Token	Is Connected
 	PamLapineOfficeDes...	sysAdmin MUG	ffcdaad9-6f6b-4a06-b...	Fri Dec 16 11:00:59 2...	25.86.187.227		10.0	6.6.53	663000b386f6e3b76...	
 	pamlapine	sysAdmin MUG	d3212947-4692-4ad3...	Mon Dec 5 17:38:32 ...	10.46.110.136		iOS-iOS-16.1.1-Appl...	8.6.2.12	e21bac1cc476d229e...	
 	Lauren Colebrooke	PHA-Bahamas MUG	87546fb1-6e9a-4816...	Wed Oct 19 11:28:40 ...	10.153.53.67		11	8.3.5.5	c40f6ad705e460f4ad...	

Green tick icon: It shows that the client app is in foreground and can communicate with the HipLink server over socket

Detail icon: Detail icon in Actions column with each record shows the detail of the connected receiver including his location

Edit icon: The Edit icon against each user opens up the pop-up window for **Remote Administration**

Advanced Messaging - Remote Administration

Push Settings Wipe User Data

Settings Types

Permissions Configuration

System Configuration

Inbox Configuration

Alert Configuration

Message Configuration

Configure Permissions

Receive Alert

-- Inherit Policy --

Send Alert

-- Inherit Policy --

Access Template

-- Inherit Policy --

Disable Logout Button

-- Inherit Policy --

Allow Compromised Device / Jail Broken Device

Receive Message

-- Inherit Policy --

Send Message

-- Inherit Policy --

Access Custom Actions

-- Inherit Policy --

Settings Access

-- Inherit Policy --

View Contacts

Note: Selecting -- Inherit Policy -- will inherit default values from Receiver, User Group Permissions and HNP General Policy.

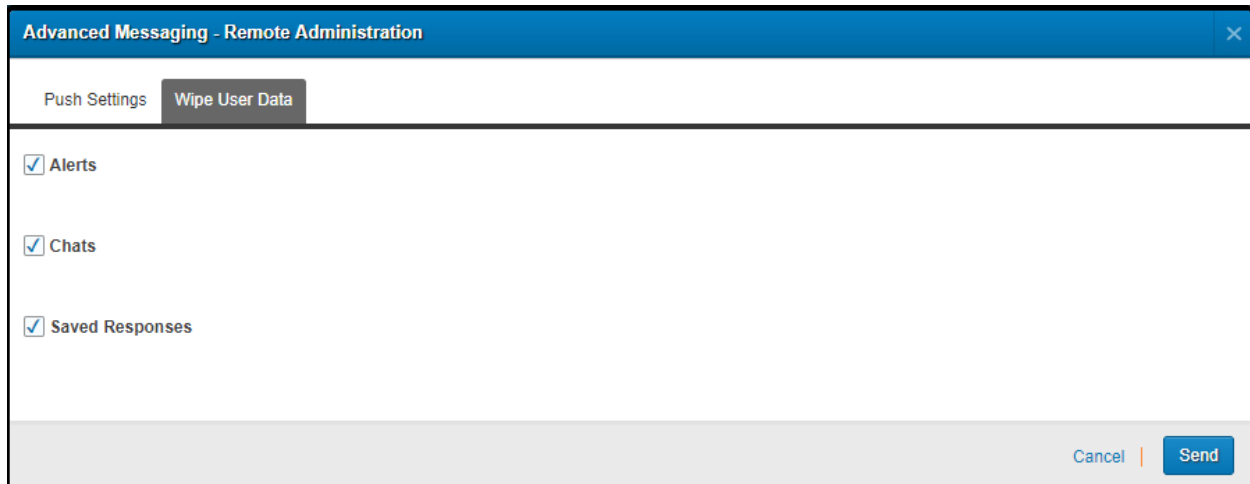
Cancel | Save | **Send**

Remote Administration allows HipLink admin users to set permissions for an individual HNP receiver (but if General Policy is applied it will take precedence over individual permissions).

Remote Administration has 2 tabs:

- **Push Settings:** Push settings has same set of features as the Mobile User Group screen. The only difference is that Remote Administration is for individual receivers whereas mobile user group is for all those receivers who have belong to the same Mobile User Group.

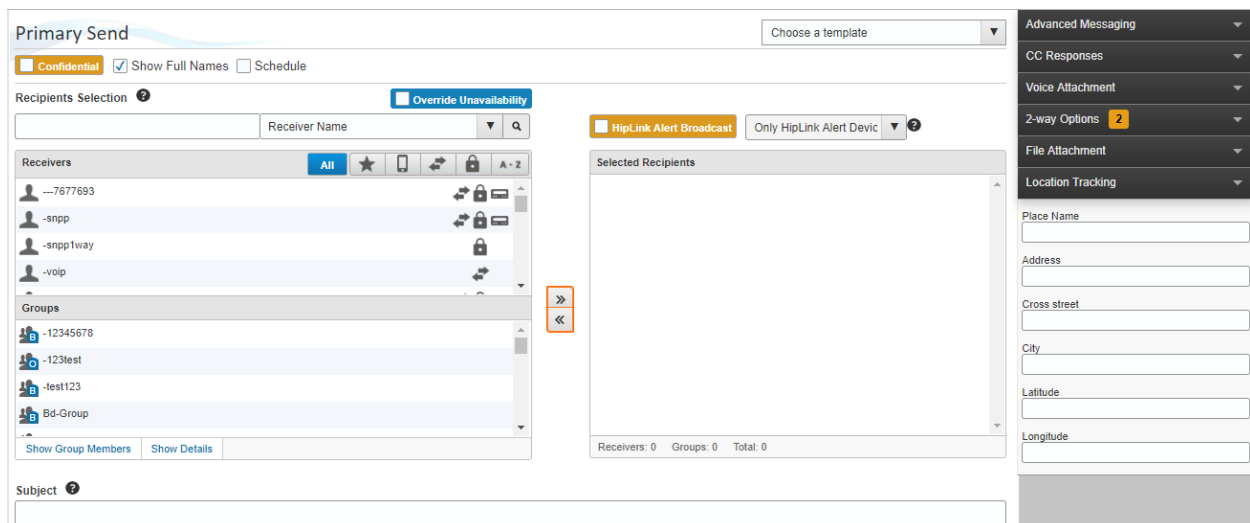
- Wipe User Data:** Wipe User Data has three check boxes as Alerts, Chats and Saved responses. On sending these permissions as checked will deletes the data from client for selected screen and if all three checkboxes checked permission is sent client will consider this as master cleanup and completely wipeout application data. After receiving Wipe out permissions application will become unusable



Desktop Sending for Location Tracking in HipLink Mobile

This section provides information for the 'HipLink Mobile Location Tracking' feature when sending Alerts. For additional details on the remaining features when dispatching Alerts from the Send Panel, please refer to the HipLink User Guide.

HipLink Mobile Location Tracking using the Primary Send Panel:



Location Tracking:

Place Name: Enter a valid name of the location that you would like to use as the destination i.e. “Civic Center” or “State Fair Grounds”.

Address: Enter the street address of the location that you would like to use as the destination. This can include the City and State as part of the field.

Cross Street: Enter a Cross street of the location that you would like to use as the destination.

City: Enter just a City name

Latitude & Longitude: Use decimal degree format (45.123456, 123.123456). If coordinate information isn't available, HipLink will plot the map using the address information.

NOTE: All fields in the Location Tracking section are optional values. HipLink will attempt to provide mapping information using any combination of the provided values that have been entered.

HipLink also allows you to enter address information directly into the message body within the Send Panel. In order to use this feature, ensure that the Location Extraction option has been configured within the Global Settings of your HipLink system.

HipLink allows the use of API's, Gateways, and CLI modules to send Location Tracking information to Alert recipients. In order to use these features, Location Extraction must be enabled within Global Settings.

Tracking Progress for HipLink Mobile Location Tracking

The Campaign Progress panel from the GUI interface allows HipLink users to view or track details of an alert dispatched using the location tracking features.

HipLink Mobile Location Tracking is accessible from Send -> Campaign Progress -> HNP Location Tracking

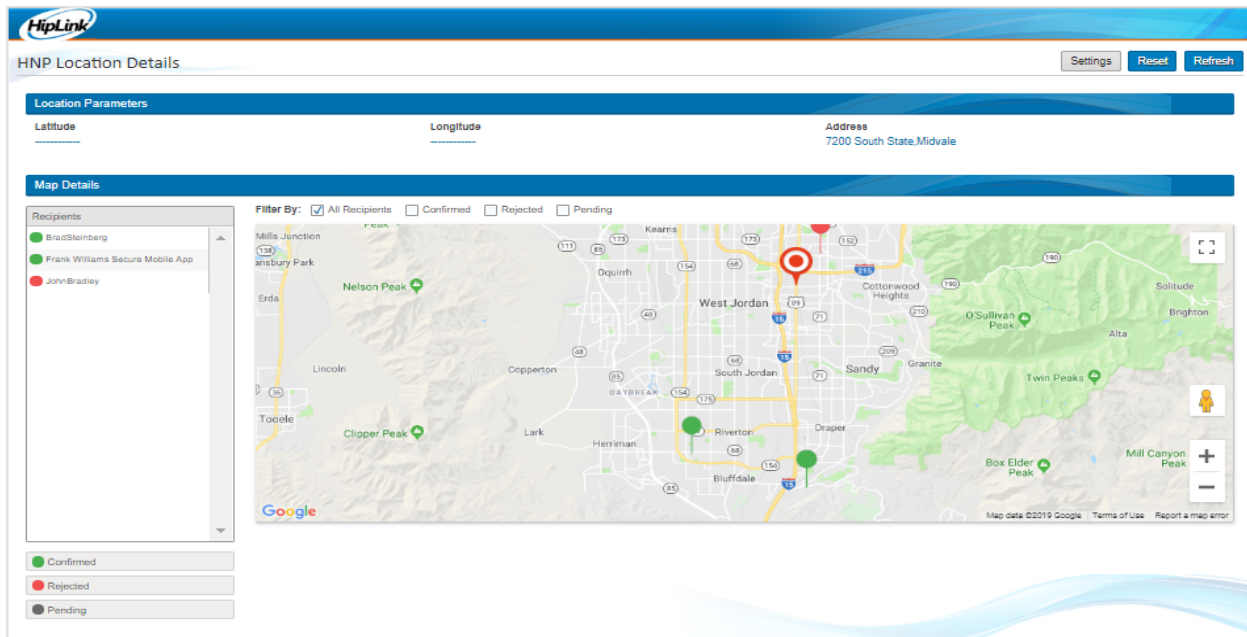


This tab shows all the alerts which were sent with a Location indicator and displays Action, Job ID, Message, Dispatch Time, Total Recipients, Confirmed, Rejected, and Pending

The screenshot shows the 'Campaign Progress' panel with the 'HNP Location Tracking Progress' tab selected. The panel displays a table of alerts with the following columns: Action, Job ID, Message, Dispatch Time, Total Recipients, Confirmed, Reject, and Pending. The table contains three rows of data.

Action	Job ID	Message	Dispatch Time	Total Recipients	Confirmed	Reject	Pending
	347120	this is new message contains spaces Place:Saratoga Street Utah Address:Springs City:USA and other ...	Tue May 7 04:47:...	1	0	0	0
	347119	this is new message contains spaces Place:Saratoga Street Utah Address:Springs City:USA and other ...	Tue May 7 04:47:...	1	0	0	0
	347117	PLACE: San Jose State University Hello Guys	Tue May 7 00:18:...	4	0	0	4

To view map details and track alert responders, use the icon in the Action column associated with the message you want to view.



Location Parameters: Shows the address parameters extracted from message body or from location address fields. Latitude/Longitude values will be provided if only available.

Map Details: This section shows a detailed map screen with the destination and markers for each responder sent the message. It will update with each person's real-time location if they selected this option from the message.

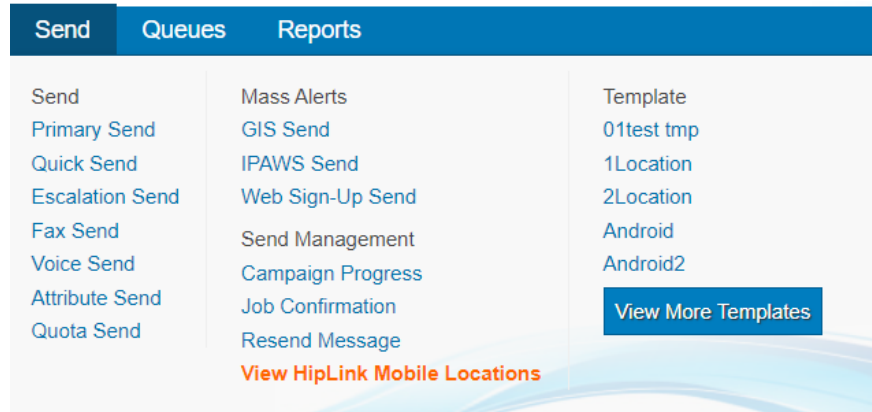
Recipients: All the alert responders who received alert will appear in the Recipient list will be distinguished with color codes of their status. The codes are shown below the list. Clicking on any responder name will make that particular pin marker prominent on map screen.

Filter By: Filters available to view only specific type of recipients and pin markers on map

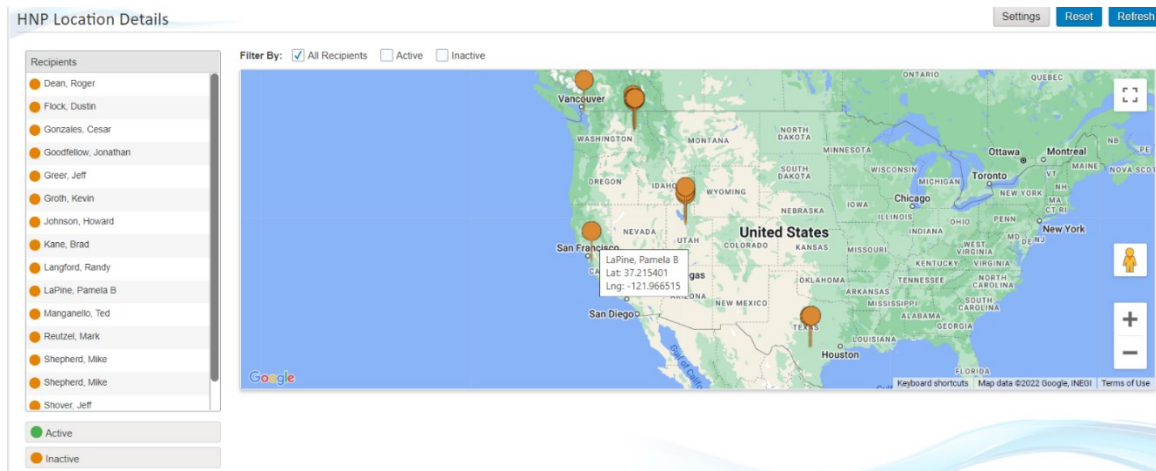
View HipLink Mobile Location Details

The View HipLink Mobile Locations panel from the GUI interface allows HipLink users to view the live location of the HipLink mobile device.

View HipLink Mobile Location is accessible from Send -> View HipLink Mobile Location -> HNP Location Tracking



This screen shows all the receivers who have shared their locations along with their active and inactive statuses.



Location Parameters: By hovering on the pin location markers, it will show the receiver name along with Latitude/Longitude values.

Map Details: This section shows a detailed map screen with each person's real-time location if the location sharing button is ON from the HNP Devices.

Recipients: All the HL Mobile receivers who have shared its live location will appear in the Recipient list will be distinguished with color codes of their status. The codes are shown below the list. Clicking on any responder name will make that particular pin marker prominent on map screen.

Filter By: Filters available to view only specific type of recipients and pin markers on map.

Active: Shows that the HL Mobile device shared its live location in the last 5 minutes.

Inactive: Shows that the HL Mobile device has not shared its live location for over 5 minutes or it has turned off the location sharing from the application.