KEYWATCH ROC Server
User Manual

Last updated September 4, 2018

Contents

Introduction

Congratulations on choosing KEYWATCH Remote Operations Center (ROC) Software, which is the remote partner to your KEYWATCH mobile device(s). Not only can KEYWATCH apps record data on your mobile device in a standalone capacity, but the ROC also uses an Internet data connection to stream, record, and share data remotely. This allows remote monitoring and management of your KEYWATCH mobile devices and the data they capture.

The KEYWATCH ROC provides the following general capabilities:

hotMIC Audio Monitoring
Listening to audio streamed in real-time by KEYWATCH mobile devices, as well as enabling playback and download of previously recorded audio.

hotCAM Photo Monitoring
Viewing photos streamed in real-time and taken previously by KEYWATCH mobile devices, as well as enabling download of photos taken previously by the hotCAM.

geoTRACK Location Monitoring
Viewing location streamed in real-time and sent previously by KEYWATCH devices on Google® Maps, Street View and/or third-party mapping services, as well as enabling download of location beacons sent previously.

Exporting Location Data
Creating custom maps using location data with third-party mapping programs.

geoFENCING
Defining boundaries (geofences) on a map so that if a KEYWATCH mobile device crosses a boundary, the monitoring team is immediately notified.

remoteTRIGGER Management of the KEYWATCH Apps
Remotely triggering consensually armed hotMIC, hotCAM, vidREC, and/or geoTRACK apps on and off, thereby allowing authorized remote management of the apps on the KEYWATCH mobile device.

remoteSETTINGS Management of the KEYWATCH App Settings
Remotely changing the settings on consensually armed hotMIC, hotCAM, vidREC, and/or geoTRACK apps, allowing extensive remote management of the KEYWATCH settings on the mobile device.

mobilePBX Cover Number Set-Up and Monitoring
Setting up a local cover number with caller ID, 24/7 calling, messaging, and voicemail, and remote live-listening and recording.

Digital Signatures for Evidentiary Authentication
All recordings are digitally signed to enable evidentiary authentication.

The ROC provides different privileges depending on the type of user. Normal Users can monitor mobile devices that are assigned to them, and manage their own preferences, but do not automatically have access to information on other devices in the system unless they are granted specific permission. System and Group Administrative Users have additional privileges on the ROC and can (for example): manage Normal Users; remotely manage devices; trigger an app; and manage, and control access to, devices. Group Administrators can perform these tasks for all the devices in their specific Group(s), whereas System Administrators can automatically do so across the ROC for all users, Groups, and devices; System Administrators can also restart server services.

Note: Please refer to the KEYWATCH Mobile for iPhone or Android User Manual, as applicable, for a full description of the KEYWATCH mobile app features. Administrative ROC Users should make sure to read Appendix A - Administrator Actions to this user manual for more detailed information about administrative features and functions. Please refer to the mobilePBX User Manual for a full description of KEYWATCH mobilePBX features.

Getting Started

Web Browser Access

The Remote Operations Center (ROC) allows remote access to the KEYWATCH mobile device features and is accessed via its website, whose Internet address will be provided by your ROC Administrator.

The ROC has been designed for and tested using the following Internet browsers:

- Mozilla Firefox 60 and above - http://www.firefox.com
- Google Chrome 67 and above - http://chrome.google.com
- Safari 11 and above - http://www.apple.com/safari

Note: Users may find that other browsers work for some or all ROC features, but KEYWAVE Products does not guarantee their functionality or fitness for purpose.

Logging into the ROC

Enter the website address provided by your ROC Administrator into your browser to access your KEYWATCH ROC. You will see the following screen.
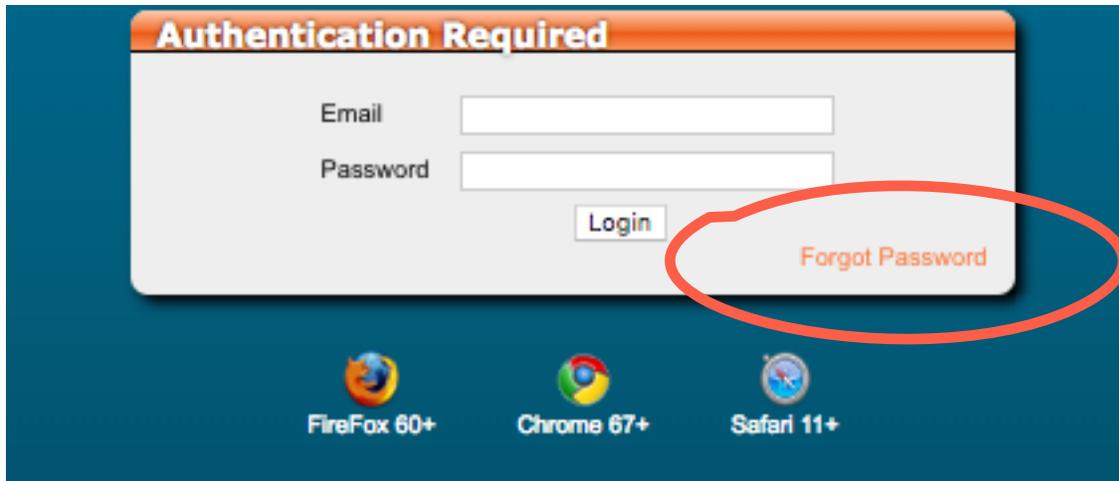
Log in using the credentials that were provided by your ROC Administrator. If you have forgotten your password, click the 'Forgot Password' link and follow the instructions that will be emailed to your registered email account to reset your password.

All the KEYWATCH operational functions are accessible through the Internet browser interface to the ROC. Administrators can also manage user accounts, group membership, permissions, etc., using this interface (see the KEYWATCH ROC Server - User Manual Appendix A: Administrator Actions for additional information). If questions arise for self-hosted server Administrators, users should see the KEYWATCH ROC Server Set Up Manual, as certain server configuration features are only accessible through the KEYWATCH console interface.
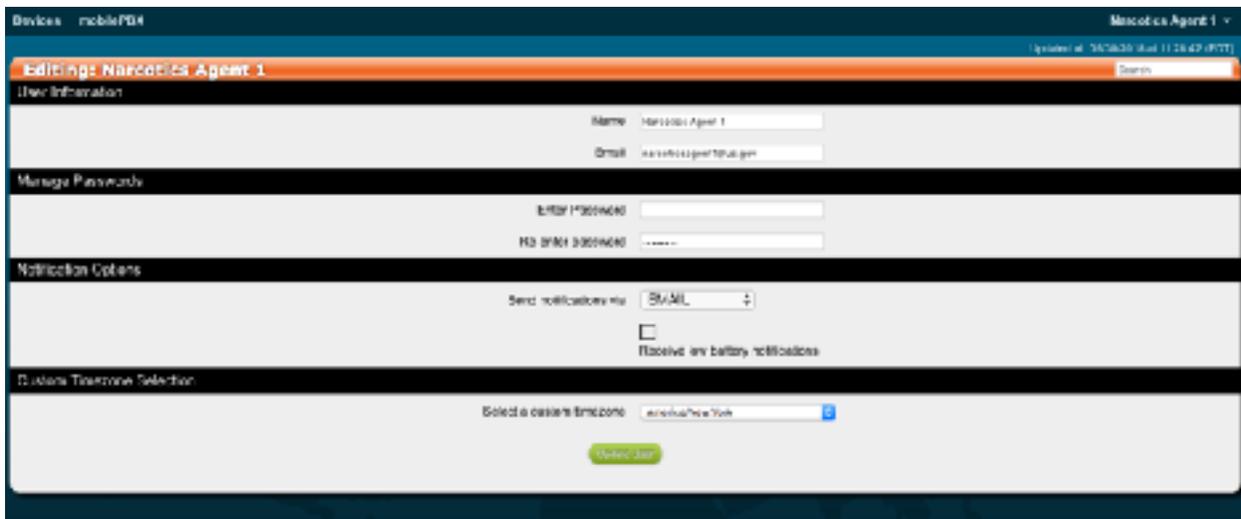
Navigation Bar

The dark blue **Navigation Bar** at the top of every page allows the ROC user to jump to either the KEYWATCH **Devices** page or the **mobilePBX** page from anywhere in the ROC, and to quickly access the **Username/Menu** pages. (See the mobilePBX User Guide for more information on the KEYWATCH mobilePBX features and capabilities, and the KEYWATCH ROC Server User Manual Appendix A: Administrator Action for Administrator views.)

Click on **Username/Menu** at the top-right of the **Navigation Bar** to access a drop-down menu for account management, and to log out.

Username/ Menu	Displays the user currently logged in to the ROC (e.g. 'Narcotics Agent 1'). Clicking on the **Username** will show a drop-down Menu from which you can access the **Account Settings** page, or where you can **Logout**.
Account Settings	Jumps to the user's Account Settings.
Logout	Logs the user out of the ROC. Users should log out when they are not actively using the ROC for safety, security, and/or privacy reasons.

Account Settings

The **Account Settings** page can be accessed under the first option on the **Username/Menu** drop-down menu and allows the user to manage their own user information, password, and notification settings.

Devices Page

A new device may only be added to the ROC via the 3-step activation process where:

• The device user presses 'Activate License' on the KEYWATCH mobile device,
• A ROC administrative user authorizes corresponding licenses for the device,
• The device user presses 'Activate License' on the KEYWATCH mobile device again.

The activation procedure is also described in the KEYWATCH Mobile for iPhone and Android User Guides. Please refer to the relevant guide for your mobile device.

The ROC **Devices** page shows all the KEYWATCH devices that are currently partnered with the ROC and that the user has access to. The hotMIC, hotCAM, and geoTRACK status conditions are updated dynamically on the Status Indicator 'traffic lights'. For instance, when a KEYWATCH mobile app is triggered on (or off), it will display green (or red).
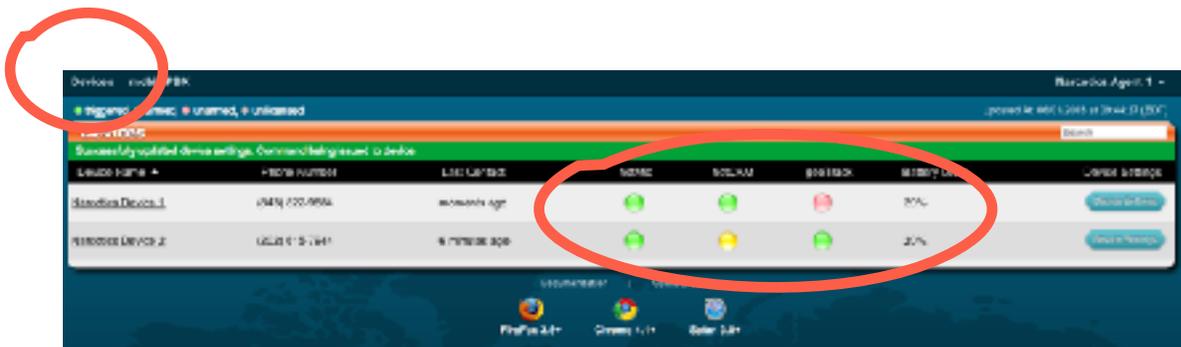
The Status Indicators show the last-known state of each data type, within the limitations of the traffic light color scheme. Because of these color scheme limitations, a GREEN traffic light, for instance, may indicate recording, streaming, or both. In this case, if a KEYWATCH device user chooses to turn off streaming, but is recording to the device, the indicator will still show GREEN because the app remains triggered, even though data is not being streamed to the ROC. A YELLOW light generally indicates that the app is armed but not triggered (i.e., it has not been activated but can be triggered from the ROC). A RED light generally indicates that the app is disarmed and not triggered. A CLEAR light indicates that the app is not currently licensed so cannot be utilized without the device being assigned to a group and licensed by an Administrator.

Note: If a device loses its network connection and its user changes the arming or triggering status of an app while there is no network connectivity, the ROC will not update the Status Indicator until there is an active network connection and it receives an update. Other similar situations may also lead to a mismatch between the actual status of the mobile device versus its status as reported on the ROC.

Device Information Page

On the **Devices** page, clicking on 'Device Name' loads the **Device Information** page for that mobile device, providing icons to navigate quickly to each of the KEYWATCH apps, a map showing the most recent geoTRACK locations (beacons), and certain device information.

Quick Navigation Icons to Access the KEYWATCH Apps

The following icons are displayed at the top of the **Device Information** page.

Device Information	Displays detailed device information for the KEYWATCH mobile device.
hotMIC	Displays the KEYWATCH mobile device's **hotMIC** page. The user may listen to a real-time hotMIC audio stream, and/or download previous audio streams.
hotCAM	Displays the KEYWATCH mobile device's **hotCAM** page. The user may view photos coming in in real-time, and/or download previous photo albums. *Note: vidREC records locally to the KEYWATCH mobile device but cannot be viewed remotely on the ROC.*
geoTrack	Displays the KEYWATCH mobile device's **geoTRACK** page. The user may view the map as it updates to show new location beacons as they arrive in real-time, and/or download files of the previous location beacons sent to the ROC.
Device Settings	Displays the KEYWATCH mobile device's **Device Settings** page. If the device has been pre-armed it also allows the user to remotely (de)trigger the hotMIC, hotCAM, vidREC, or geoTRACK apps on the KEYWATCH device, and/or remotely update the hotMIC, hotCAM, or geoTRACK app settings. This page is unavailable to Read-Only Users.

Google Map, Street, and Third-Party Mapping Views

The top half of the **Device Information** page provides a Google map detailing the current and past locations of the device. For further information on this functionality, please go to the geoTRACK section of this User Guide.
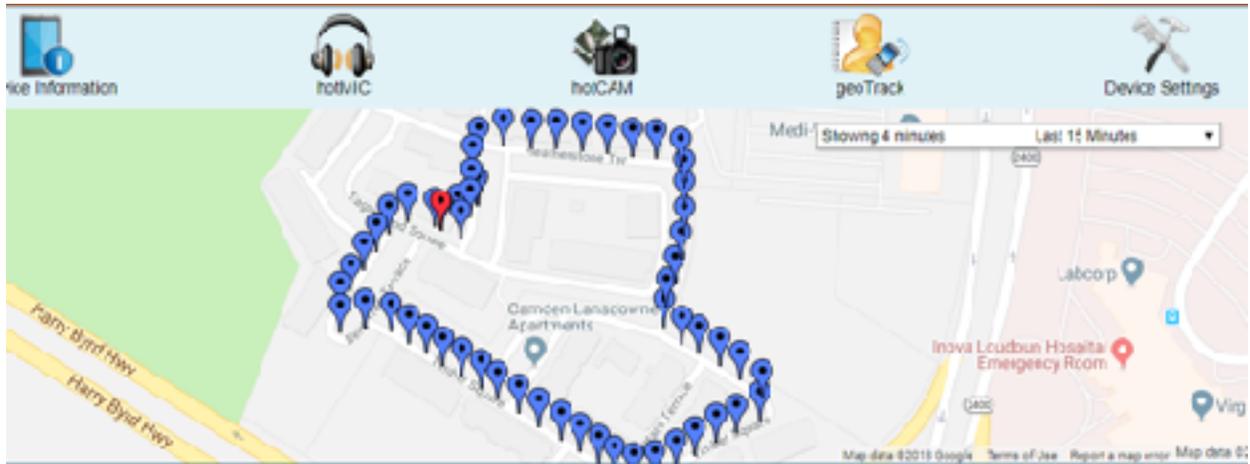
Device Information

The bottom half of the **Device Information** page provides the information set out below pertaining to the mobile device.

hotMIC

To access hotMIC audio on the ROC, click the 'hotMIC' icon, which will take you to the **hotMIC** page. The top half of this page provides a Google map detailing the current and past locations of the device, and the bottom half provides the hotMIC functionality. For further information on the Google maps functionality, please go to the **geoTRACK** Section of this User Guide.

hotMIC audio can be live streamed from the KEYWATCH device and securely monitored via the ROC, and either:

1. Recorded on the ROC in real-time for later playback and download; or
2. Unrecorded on the ROC if operational needs require (by navigating to 'Admin SIP Settings' on the **Device Settings** page and toggling ROC Server Recording to 'OFF' (see Admin SIP Settings under the section on **Device Settings** for more information)).

To listen to real-time streaming hotMIC audio directly via the ROC website, you may use a supported web browser or a SIP client software (i.e., 'softphone') application to monitor the live audio. For more information on how to install and operate SIP client software, please see the Softphone Set-Up User Guides for iOS, Android, or Desktop, as appropriate.

Live Monitoring hotMIC Audio from within the Browser

To listen in real-time to streaming audio from the KEYWATCH mobile device you are monitoring from within a browser when logged into the ROC, click the green 'Live Listen' button found on the device's hotMIC page.
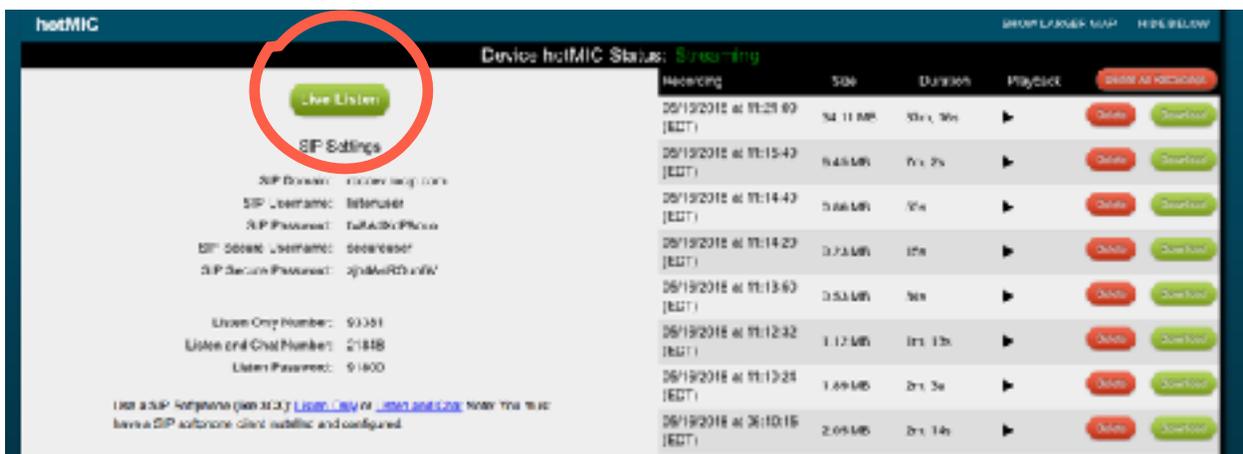
Click the red 'Close' button to stop monitoring the device's hotMIC audio stream.
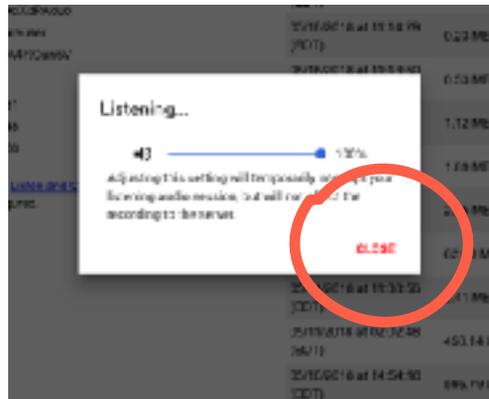
Multiple users may monitor a hotMIC audio stream at the same time.

Live Monitoring hotMIC Audio from a SIP Client

hotMIC audio can also be monitored using a softphone app. This is a particularly useful alternative if you do not have access to a supported browser or you prefer a more 'phone-like' interface. To monitor hotMIC audio in this way, you will need to install and configure a softphone app. In order to do so, you will need the SIP Domain, SIP Username and SIP Password, all of which can be found on the **hotMIC** page or on the **Device Settings** page under 'Admin SIP Settings'. For detailed instructions on correctly installing and configuring the selected softphone app, see the Softphone Set-Up User Guides for Android, iOS, or Desktop, as appropriate.
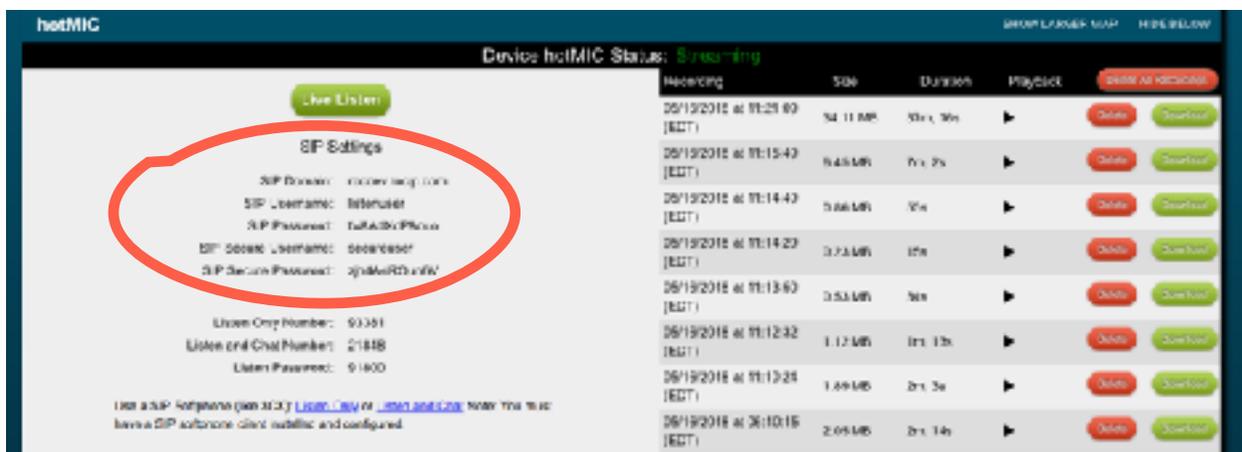
Once you have correctly installed and opened the softphone app, you are ready to live-monitor the hotMIC audio from the KEYWATCH mobile device. This can be done in two ways:

1. Dial the unique Listen Only Number or Listen and Chat Number for the KEYWATCH mobile device you wish to live-monitor. When the call is connected, enter the unique Listen Password to access the device's hotMIC audio stream. The Listen Password is used both to access the Listen Only and the Listen and Chat audio stream. Please review the information below to determine which number is most appropriate for your purposes.
2. Click the 'Listen Only' or 'Listen and Chat' blue hyperlinks on the **hotMIC** page. *Note that the hyperlinks will work only if you have the third party softphone apps installed on your device.*

Listen Only Button	Typical for live-monitoring audio from the hotMIC app. Users listen to the one-way real-time audio stream coming from the KEYWATCH mobile device, but cannot be heard by each other or by the KEYWATCH device.
Listen Only Number	Typical number for live-monitoring audio from the hotMIC app. Users listen to the one-way real-time audio stream coming from the KEYWATCH mobile device, but cannot be heard by each other or by the KEYWATCH device.
Listen and Chat Number	Allows multiple users to talk to each other while simultaneously monitoring the one-way real-time audio stream audio from the hotMIC app, without being heard by the KEYWATCH device. Users dialed into the Listen Only Number (including ROC users who are listening via the button in their browser) will hear any comments by users using the Listen and Chat number.
Listen Password	Password required for a user dialing with a Listen Only Number or Listen and Chat Number to access the audio from the hotMIC app on the KEYWATCH device.

hotMIC Audio Playback and Download

All audio that is streamed by hotMIC is also securely saved to the ROC (unless ROC Server Recording is toggled to 'OFF' under 'Admin SIP Settings' on the **Device Settings** page (see section on [Device Settings](#) for further information), and can be played back, downloaded with digital signatures for evidentiary authentication, and/or deleted.

▶	Allows the user to play back the recorded audio file without downloading it. *Note: Starting any recording will cancel playback of any currently playing recording, but will not stop the ROC recording any audio that is currently streaming from a KEYWATCH device.*
Delete	Deletes the recording. Read-Only Users may not delete recordings.
Download	Downloads a zip archive containing the audio recording from the server with digital signatures for evidentiary authentication. *Note: The audio on the ROC may not be identical to the recording downloaded directly from the KEYWATCH device due to compression, transmission drops, etc.*
Delete All Recordings	Deletes all the recordings for this KEYWATCH device. Read-Only Users may not delete all recordings.
Download All Recordings	Downloads all the audio recordings for this KEYWATCH device with digital signatures for evidentiary authentication.

hotCAM

To access hotCAM photos on the ROC, click the 'hotCAM' icon, which will take you to the **hotCAM** page. The top half of this page provides a Google map detailing the current and past locations of the device, and the bottom half provides the hotCAM functionality. For further information on the Google maps functionality, please go to the [geoTRACK](#) section of this User Guide.

hotCAM photos can be live streamed from the KEYWATCH mobile device and securely monitored via the ROC, and either:

1. Recorded in real time for later viewing and download; or
2. Unrecorded on the ROC if operational needs require (by navigating to 'Admin SIP Settings' on the **Device Settings** page and toggling ROC Server Recording to 'OFF' (see section on [Device Settings](#) for more information).

hotCAM photos are displayed and organized into albums as they are uploaded to the ROC server; a new album is created for each day that a KEYWATCH device transmits photos to the ROC. Uploading the photos may take a few seconds. If the frequency of photos being taken and streamed is higher than the network connection can handle, the server will queue the photos until they can be uploaded. Albums can be viewed, downloaded with digital signatures for evidentiary authentication, and/or deleted.

Please note that although the vidREC app can be used to record locally onto the KEYWATCH device, it cannot be monitored by, or streamed to, the ROC at this time.

|	
Show Photos	Shows a thumbnail gallery of all the photos in an album (newest at the top left). A user can view a larger version of the photo with its EXIF metadata by clicking an individual thumbnail. Individual photos can be deleted by clicking the red 'X' button at the top right corner of the photo.
Show Location	To show the location of each hotCAM photo, click on 'Show Photo', select the relevant photo, and then click on the blue 'Show Location' button on the left. *Note that the Location will be shown only if 'Geotag Images' is enabled on the KEYWATCH mobile device.*
Delete Album	Deletes the album and all the photos in that album. Read-Only users may not delete albums.
Download Album	Downloads a zip archive containing all the photos in that album from the server with digital signatures for evidentiary authentication.
Delete All Albums	Deletes all the albums for this KEYWATCH device. Read-Only Users may not delete all albums.
Download All Albums	Downloads all albums for this KEYWATCH device with digital signatures for evidentiary authentication.

geoTRACK

To access geoTRACK location data on the ROC, click the 'geoTRACK' icon, which will take you to the **geoTRACK** page.

This page:

1. Provides a Google map detailing the current and past locations of the device; and
2. Displays a table showing the last 25 location updates sent to the server from the KEYWATCH mobile device (if the mobile device has streamed more than 25 location beacons to the ROC, those beacons can be accessed by clicking on the additional pages of the table).

Google Map View

The map shows the latest reported device location in red and previous locations in blue. As long as geoTRACK is triggered and streaming on a KEYWATCH device, the map updates in real-time as new geoTRACK locations are received.
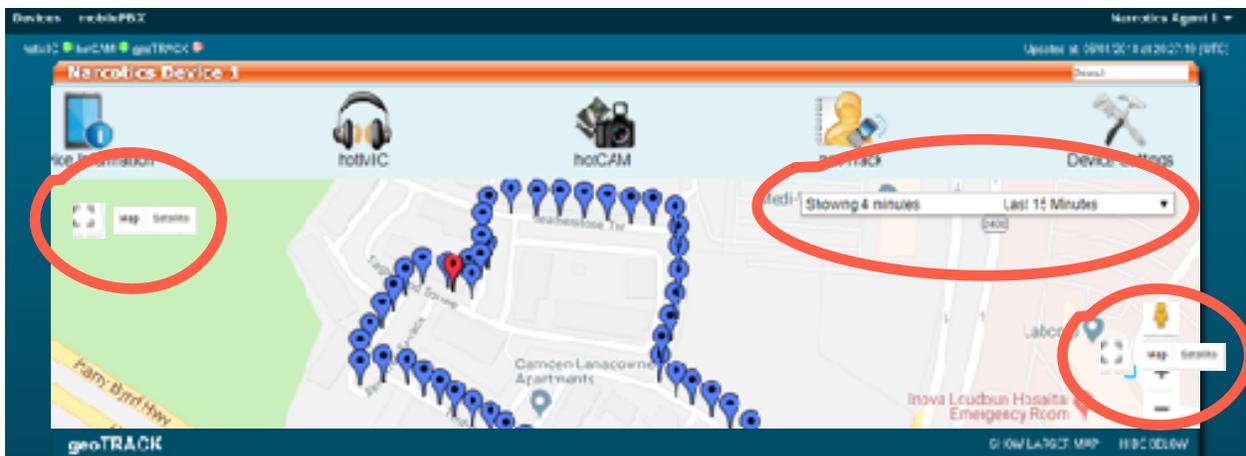
At the top right of the map is a control that allows a user to show past geoTRACK locations within certain defined time periods. Upon loading the map, or once a time period has been selected, the 'Showing x minutes' next to the control will update in realtime, showing all visible geoTRACK locations within the selected time period.

At the bottom right of the map is an orange 'person', which can be clicked and dragged onto the map to change it to Street View. Note that photos shown in Street View are provided by Google, are not available in all areas, and are not intended to accurately reflect the current situation. Users can also switch between Map and Satellite views, full screen and normal views, and zoom in and out.

Location Beacons

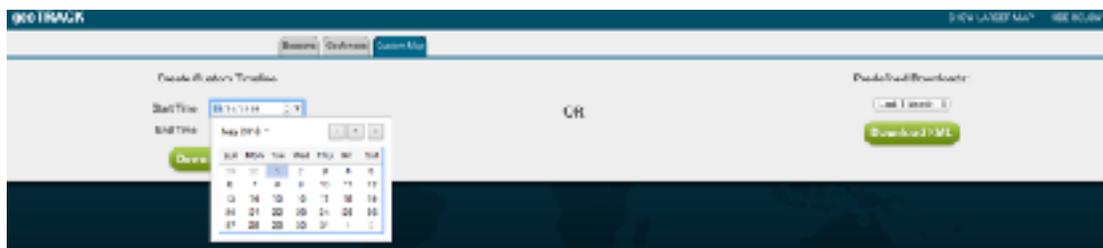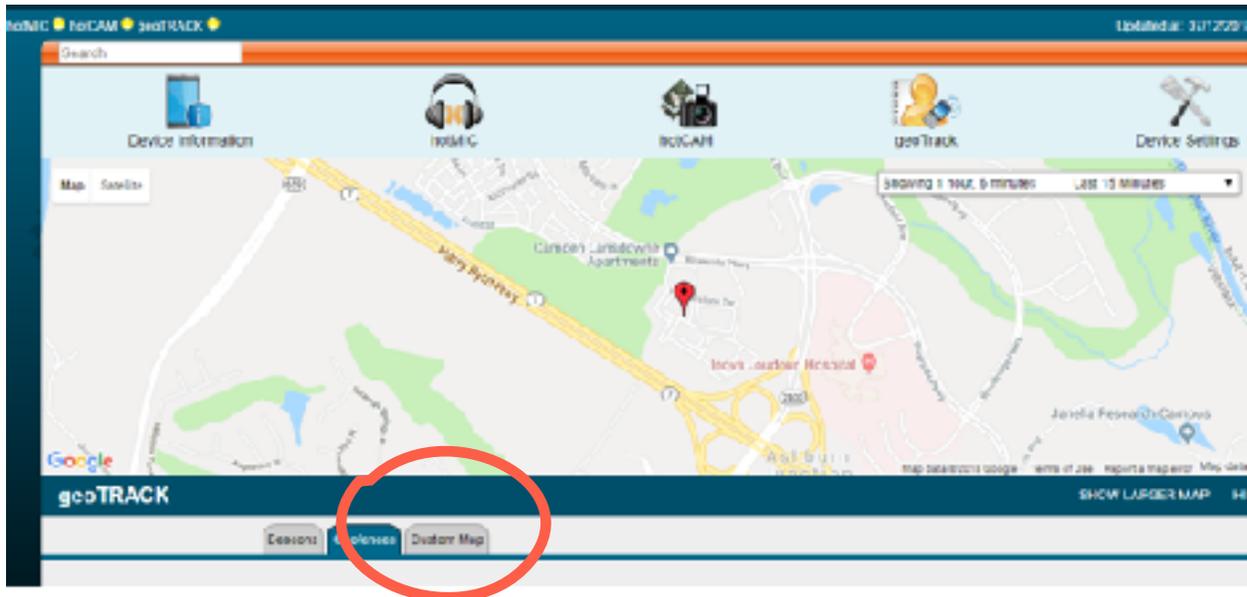Each row of the table displays information from a single geoTRACK location.

| Latitude, Longitude	The location reported by the geoTRACK beacon. The horizontal accuracy of each location is provided in meters.
Altitude	The altitude of the beacon from sea level in meters. The vertical accuracy of each location is provided in meters and is generally significantly less accurate than that of latitude and longitude.
Battery Level	The battery level of the KEYWATCH mobile device reported by the geoTRACK beacon.
Speed	The approximate speed at which the device is traveling at the time of the geoTRACK beacon in meters per second. (If the device is stationary, this value will be blank.)
Direction	The direction the device is travelling in degrees from North. (If the device is stationary, this value will be blank.)
Timestamp	The date and time of the geoTRACK location beacon.
Show Beacon	Brings up a new tab with a Google Maps page showing the geoTRACK location beacon.
Delete Beacon	Deletes the selected beacon for this KEYWATCH mobile device. Read-Only users cannot delete location beacons.
Delete All Beacons	Deletes all the location beacons for this KEYWATCH device. Read-Only users cannot delete all beacons.
Download All Beacons	Downloads a zip archive containing all the beacon locations in that album from the server with digital signatures for evidentiary authentication.

Custom Map Creator

Using the Custom Map Creator, the device's geoTRACK data for the time period selected by the user can be imported into a third-party mapping program for viewing, animation, and processing. To access this feature, click the 'Custom Map' tab directly below the map on the **geoTRACK** page.

|	
Create Custom Timeline	The pop-up calendar allows the user to select a Start Time and an End Time for the location history to view. Click 'Download KML' and a mapping file filtered to include only the dates specified by your start and end times will be downloaded through your browser. This file can be viewed, animated, and analyzed using a third-party mapping program.
Predefined Downloads	Users can also select a pre-defined timeframe to view the location history. Use the drop-down menu to choose one of the pre-defined time periods. Click 'Download KML' and a mapping file will be downloaded through your browser.

Using a Third-party Mapping Program
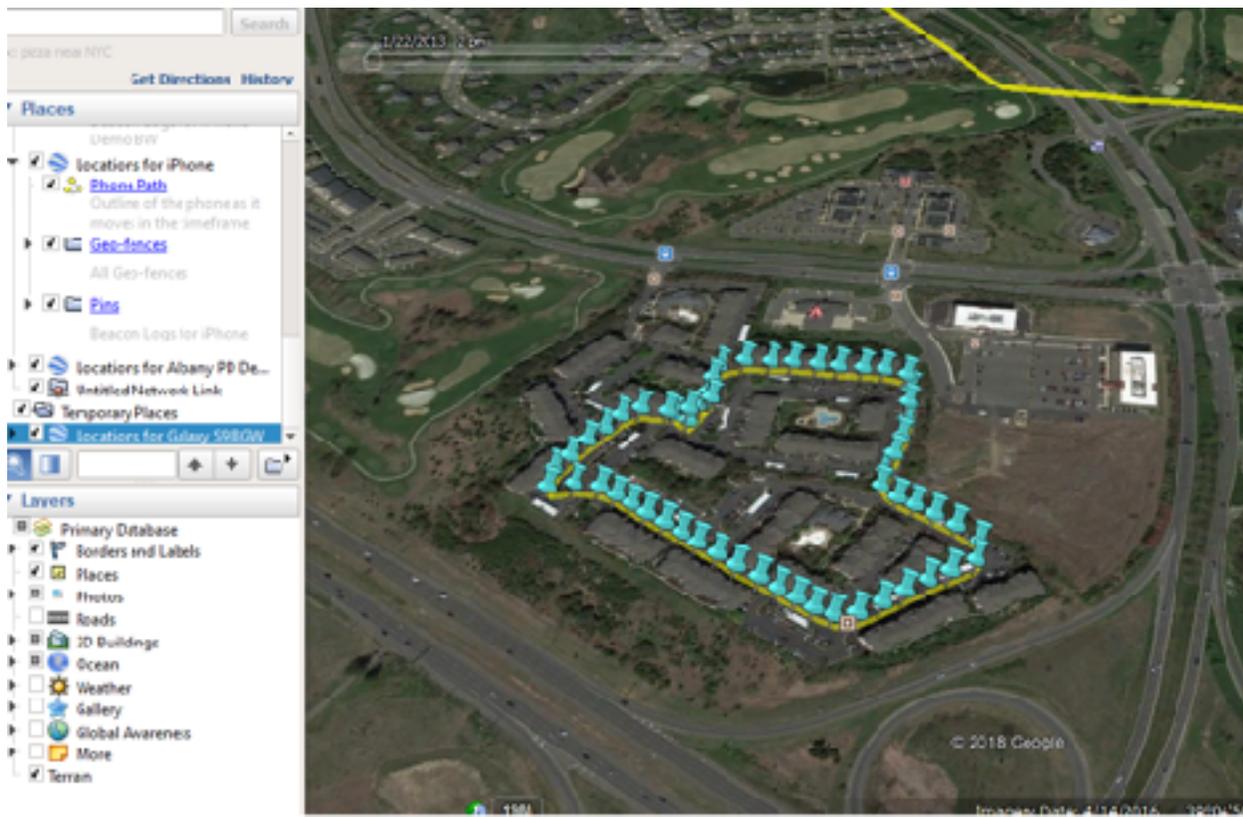
If the mapping program of choice is installed and launched, it will automatically zoom to display the device's location history over the selected duration. The map will display each geoTRACK location received during the specified time range. Multiple map files can be overlaid on top of each other in the mapping program.

The controls at the top of the screen select the range of pins to display and control animation of the data.

geoFENCE Feature

The KEYWATCH geoFENCE is a feature that automatically alerts selected users whenever a device enters or leaves a specified, configurable area. Geofences are device-specific, so that a geofence must be created for a each KEYWATCH mobile device. For example, if you would like to know whenever device 'Narcotics Device 1' enters or exits the area around Baltimore-Washington International (BWI) Airport, you can create a geofence around that area. Please note that the geoFENCE feature is not available to Read-Only Users.

To access the geoFENCE feature, click on the 'Geofences' tab directly below the map on the **geoTRACK** page.
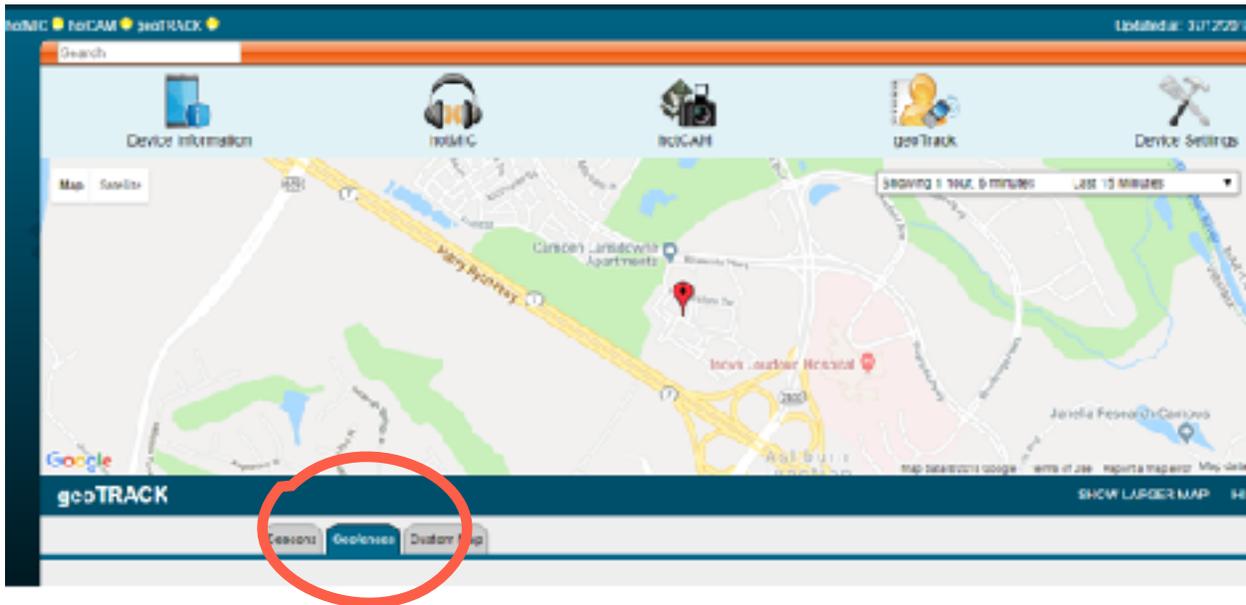
Click the orange 'Add Fence' button to open a new geofence window with a new fence around the most recent location for 'Narcotics Device 1'.
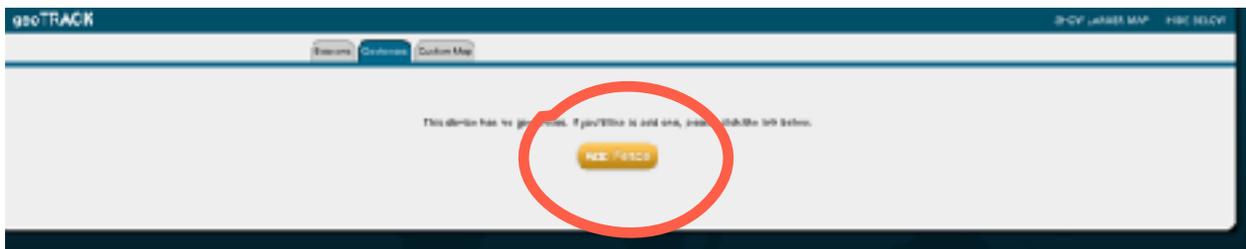
The geofence can be adjusted by dragging the edge dots of the geofence circle to the location surrounding BWI airport or by setting a radius in the box below. The map will automatically zoom to fit the frame. The user can name the geofence and select its color, and select which users will be notified when the mobile device enters/exits the geofence boundary. Click the green 'Save geofence' button to finalize the geofence. Users can add multiple geofences and edit/delete existing geofences.
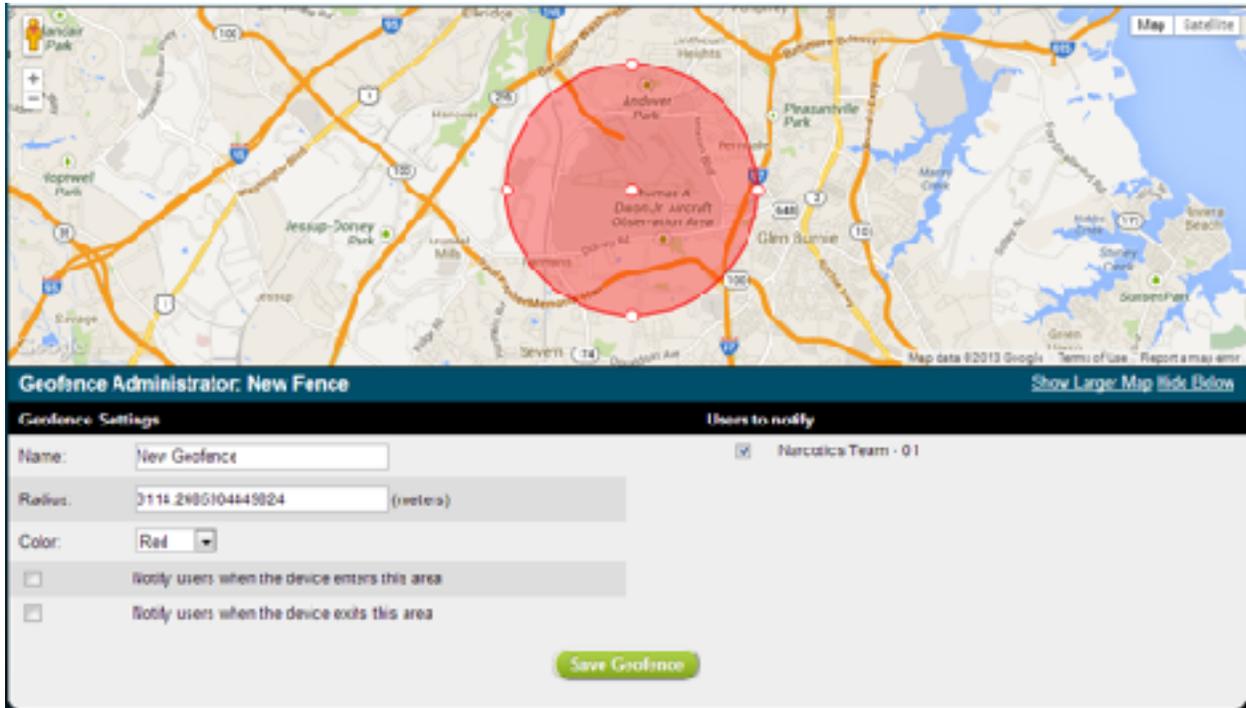
remoteTRIGGER and remoteSETTINGS

Before Using remoteTRIGGER and remoteSETTINGS

If you are not using the remoteTRIGGER or remoteSETTINGS capability, you can skip this section.

Please note that the remoteTRIGGER and remoteSETTINGS functionality are not available in all countries. You can contact your dealer for up-to-date information regarding availability in your country. Also note that remoteSETTINGS requires remoteTRIGGER in order to function. Ensure that the device has activated both remoteTRIGGER and remoteSETTINGS licenses if attempting to use remoteSETTINGS.

There is a slight difference between the layout of the ROC when connected to iOS vs Android mobile devices in terms of remoteTRIGGER. On a ROC connected to iOS mobile devices, the user must manually set the remoteTRIGGER number, whereas on a ROC connected to Android mobile devices this is not necessary. There is, however, no functional difference in operation of either remoteTRIGGER or remoteSETTINGS.

Please ensure you have correctly configured your device phone number before you attempt to remoteTRIGGER an app or update an app's settings.

On a ROC connected to an iOS mobile device only (i.e., not an Android mobile device) you will also need to update the trigger number. If you change the trigger number, the KEYWATCH mobile device user must reactivate the remoteTRIGGER license by going to KW Settings > Phone Management and tapping 'Activate License' on the device.

Finally, in order to use remoteTRIGGER and/or remoteSETTINGS, the KEYWATCH app must be armed on the mobile device. In order to do this, the mobile device user must access KEYWATCH Settings > [Application] and toggle the 'Armed' switch to 'ON' (see the KEYWATCH Mobile for iPhone or Android User Guide, as appropriate, for further instructions).

If remoteTRIGGER and remoteSETTINGS are available in your country and licensed to your KEYWATCH mobile device, the **Device Settings** page allows a ROC user to remotely trigger on (activate) or off (deactivate) armed KEYWATCH apps, and remotely adjust the settings for those apps. Read-Only Users cannot access the **Device Settings** page.

remoteTRIGGER

If the app is armed on the KEYWATCH mobile device, it will display a toggle switch showing whether it is currently triggered or not. If it is not armed, it will only display '[Application] not armed' in its place and it will need to be armed directly from the device.

To use remoteTRIGGER to remotely change the trigger status of one or more apps on the KEYWATCH mobile device, simply toggle the switch from 'OFF' to 'ON' (or vice versa) for each app you would like to change the status of, and then click the green 'Send Settings to Device' button on the right. The changes to be made will appear directly above the button. You may trigger multiple apps at one time. You may also use remoteSETTINGS and remoteTRIGGER to simultaneously trigger apps and adjust their settings.

A dialog box will pop up with the following message:
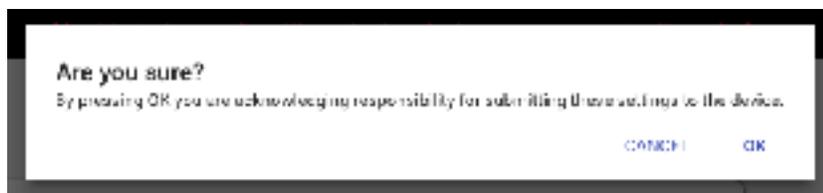
Click 'OK' and the following message will display.

remoteSETTINGS

If the app is armed on the KEYWATCH mobile device, the sections detailing the settings for each app on the **Device Settings** page will display adjustable toggle switches. If it is not armed, the information will simply be displayed in a non-adjustable format. See for example the difference between the two hotMIC (Audio) Settings sections set out below:

hotMIC (Audio) Settings Armed vs. Not Armed

To use remoteSETTINGS to change app settings on an armed KEYWATCH mobile device, toggle the settings under the section corresponding to the app. For example, to set hotMIC settings, expand the 'hotMIC (Audio) Settings' section and make the necessary adjustments. The settings controls should operate similarly to the app settings on the mobile device. After adjusting the desired settings, click the green 'Send Settings to Device' button. You may send settings for multiple apps at one time.

After clicking the 'Send Settings to Device' button, the remoteTRIGGER and remoteSETTINGS toggle buttons and controls will be disabled while the settings are being sent. You will be updated on the device status in the text above the buttons.
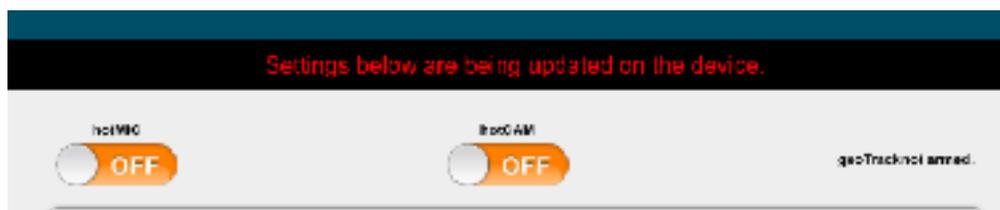
If for some reason the remoteTRIGGER and/or remoteSETTINGS command is unsuccessful, the ROC website will display 'Unable to transmit settings to the device', as shown below. This can happen, for instance, if the device encounters network connectivity issues. In this situation, you can resend the remoteTRIGGER and/or remoteSETTINGS command as set out above.

Note: If the contents of a settings section are read-only text values, it means either the device is not correctly licensed for both remoteTRIGGER and remoteSETTINGS, the app is not armed, or a remoteTRIGGER/remoteSETTINGS command is already in transit. A ROC user may still view these settings to help diagnose problems if the KEYWATCH device user has improperly configured the device, or if the system is not working as expected, but cannot remotely change those settings. For example, if the ROC user cannot live-listen to hotMIC audio, they can check whether 'Remote Streaming' is enabled in the hotMIC Settings; if not, then hotMIC audio will not be available for monitoring even though hotMIC is triggered on the device.
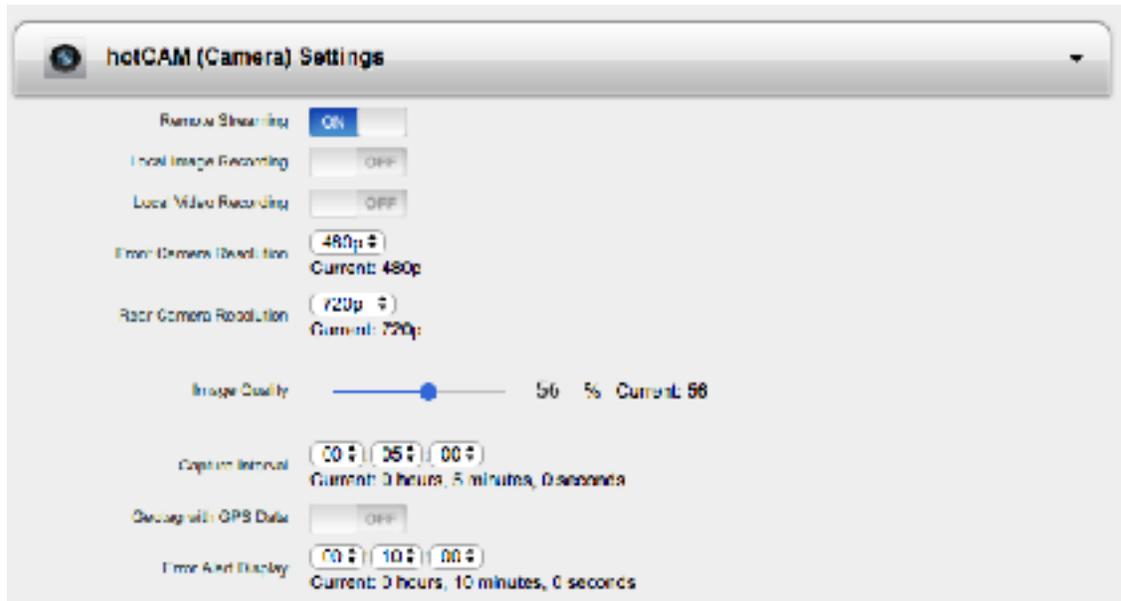
hotMIC (Audio) Settings

This section lists the last uploaded settings for the device's hotMIC. It shows whether the device has streaming, local recording, or both enabled. It also shows details regarding the audio stream between the phone and the server, the local recording's sample rate, and file splitting settings.
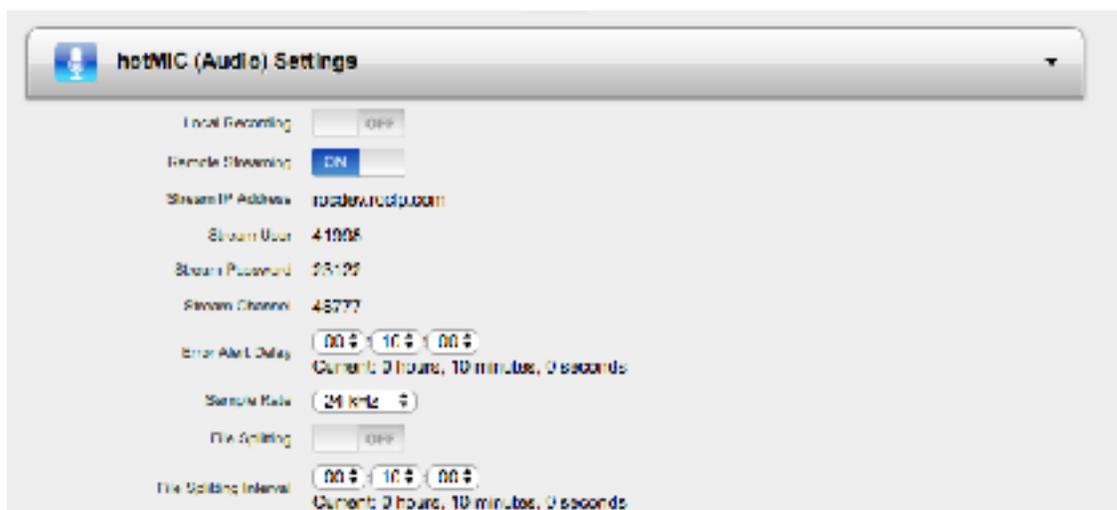
hotCAM (Camera) Settings

This section lists the last uploaded settings for the device's hotCAM feature. It shows whether the device has streaming, recording locally, or both enabled. It also shows additional settings such as image quality, capture interval, and geotagging availability.

geoTRACK (Location) Settings

This section lists the last uploaded settings for the device's geoTRACK feature. It shows whether the device has streaming, local recording, or both enabled. It also shows additional settings such as distance and timer beacons as well as their intervals.
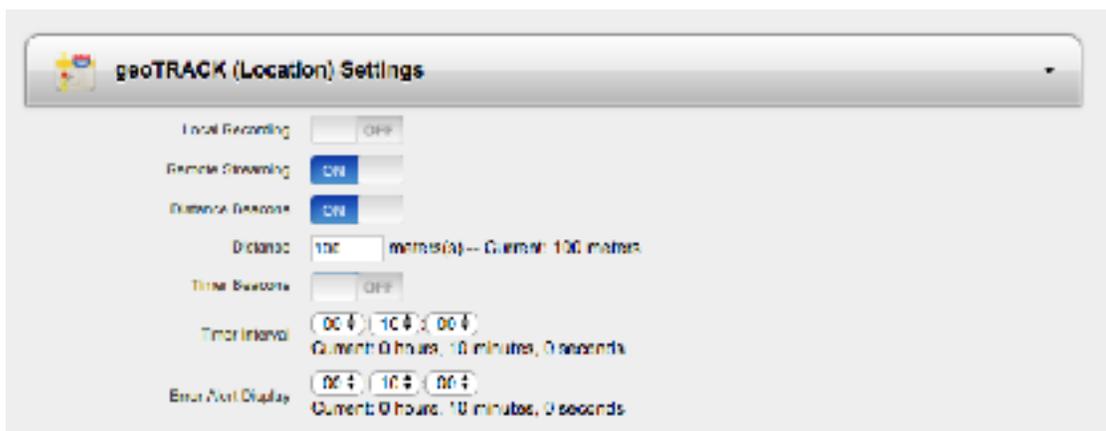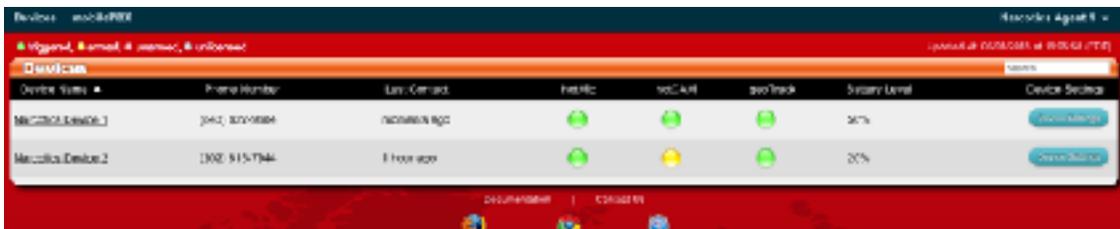
Distress Signal

Sending a Distress Signal from the KEYWATCH device to the ROC

By entering the Distress code, a KEYWATCH mobile device user can cause an alert to display on the ROC. Users monitoring this device will receive an email, SMS message, or both, based on their notification preferences. The default Distress code depends on the type of KEYWATCH mobile device. For an iOS mobile device (e.g., an iPhone), the default is *Volume Down, Volume Up, Power/Lock, Volume Up, Volume Down. For an Android mobile device, the default* is *Volume Down, Volume Up, Volume Up, Volume Up, Volume Down*. A user may assign a new custom code. For further details, please see the KEYWATCH Mobile for Android or iPhone User Manual, as appropriate.

The ROC tab will display a flashing 'ALERT! ALERT! ALERT!' message to notify a ROC User that is currently active in another TAB of the web browser.

The main **Devices** page will turn red to notify the ROC User of the alert.

All other pages related to the device will display an alert. The ROC User must click the link on the alert to dismiss it. Read-Only Users may not dismiss distress alerts.

Sending a Distress Signal from the ROC to the KEYWATCH device

If the KEYWATCH mobile device has the reverse distress feature enabled, the ROC operator may send a distress signal to the KEYWATCH device in order to alert the operator of the device of an urgent situation. In order to send the signal, simply navigate to the **Device Settings** page and press the red 'Send Distress to Device' button on the right immediately below the Google Map.

Then, confirm that you want to send the distress signal if you are absolutely certain you wish to do so. Sending the distress signal uses the same mechanism as remoteTRIGGER, so the success and error messages are the same as for remoteTRIGGER and remoteSETTINGS.
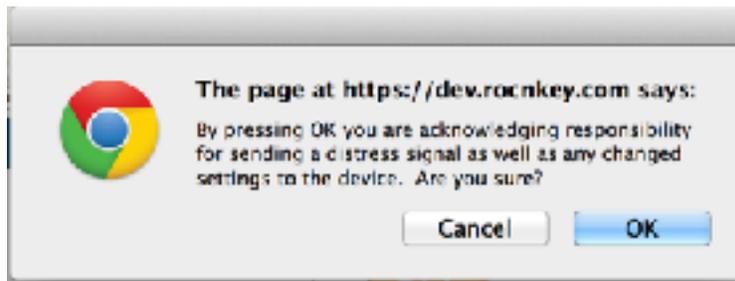
The KEYWATCH mobile device will vibrate subtly five times, or if the KEYWATCH device is connected via Bluetooth to a Key Fob, the Fob will vibrate five times.

Note: If using an iOS mobile device (e.g., an iPhone), if hotMIC is triggered, the KEYWATCH mobile device will not vibrate in order to prevent interference with the recorded and/or streamed audio, but a connected key fob will still vibrate regardless of whether hotMIC is triggered. If using an Android mobile device, even if hotMIC is triggered, the device will still vibrate.

Device Settings Page

In addition to enabling the remoteTRIGGER and remoteSETTINGS functionality, the **Device Settings** page also lists the device name, and device phone number. Devices with no SIM will not have a phone number; therefore remoteTRIGGER and remoteSETTINGS will not work for those devices. On a ROC connected to iOS mobile devices only (i.e., not an Android mobile device), the **Device Settings page** will also display the remote trigger number(s).

If the device's phone number changes, or (on a ROC connected to iOS mobile devices only) a ROC user changes the trigger number(s), the device user must go to KW Settings > Phone Management and tap 'Activate License' on the device.
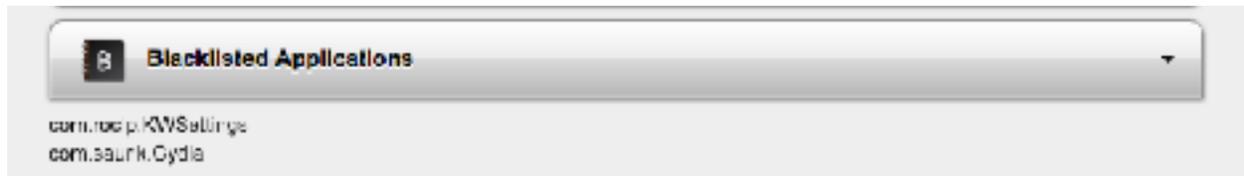
ROC Device Settings

Name or Identifier	Change the KEYWATCH device's name as shown on the ROC by typing a new name in the text box and clicking. *Note: Changing the device name here will not change the name stored on the device and may cause confusion. We recommend that if you change the name on either the mobile device or the ROC, that you take action to change it to exactly the same name on the other. For devices running iOS, the name may be changed at Settings > General > About > Name. For Android mobile devices, the name may be changed at Settings > About Phone and by tapping the 'EDIT' button.*
Phone Number	Change the KEYWATCH device's phone number as shown on the ROC by typing a new number in the text box and clicking. *Note: Changing the phone number here will not change the phone number on the device. The correct country code must also be selected to ensure all appropriate area prefixes are set for remoteTRIGGER operations.*

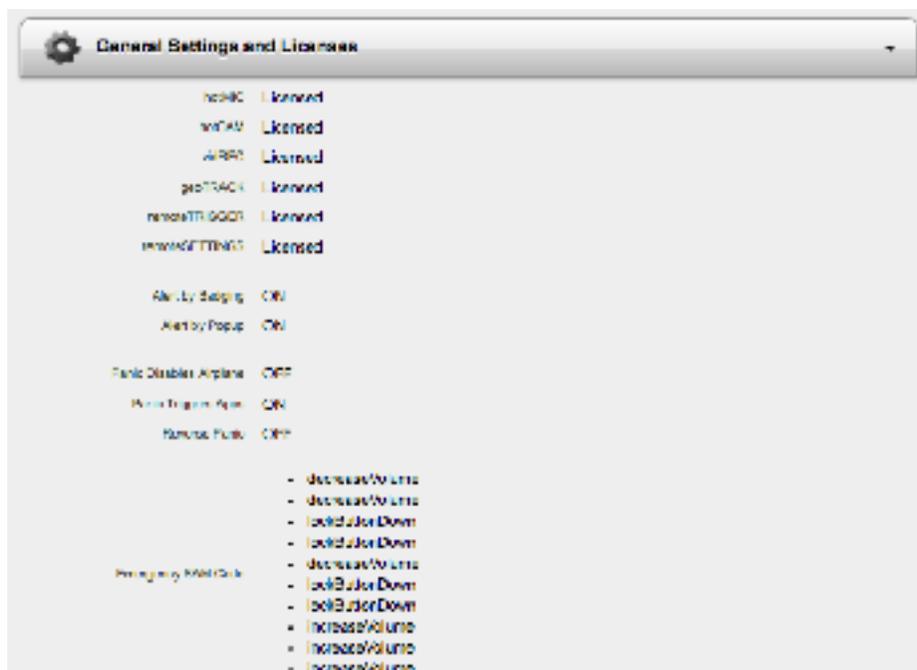|	
Trigger Number (for a ROC connected to iOS mobile devices only)	If the device has remoteTRIGGER capability, the ROC User must enter at least one trigger number to send to the device as a caller ID. The correct country code must also be selected. For additional security, in case a KEYWATCH mobile device phone records from the telecoms provider come under scrutiny, more than one trigger number can be selected. This will cause the ROC to alternate between the trigger numbers on each remoteTRIGGER or remoteSETTINGS command. In order to set two trigger numbers, separate each number by a comma. When a remoteTRIGGER command is sent, the mobile device verifies the incoming caller ID and knows it needs to execute a command being sent by its ROC. If you are using Flowroute as the remoteTRIGGER method, this caller ID can be any valid local number(s) you want, but should have a valid local area code for the device. If not, the cellular provider may not be able to read the proper caller ID, causing the trigger to show up on the device. The number(s) should not contain a trunk code (i.e. leading 1 in the US, leading 0 in the UK, etc) or contain any non-numerical values such as ' ' or '+'. *Note: When updating a trigger number, the KEYWATCH mobile device user must re-activate the licenses for that mobile device for the update to take effect.*
KEYWATCH-mobile Version	The KEYWATCH version installed on the device.
OS Version	The iOS or Android version installed on the device.
Device Serial Number	The manufacturer serial number of the phone.
UUID	'Universally Unique ID' number for this device.
Hardware Model	The hardware model of the device, e.g., iPhone 6, or Android.

Blacklisted Applications (only appears on mobile devices that are jailbroken or rooted)

For mobile devices that are jailbroken or rooted to install KEYWATCH mobile, this section lists the last uploaded list of apps that are 'blacklisted' on the device so that their presence on the device will be actively blocked from being observed by users of the device.

General Settings and Licenses

This section lists the general KEYWATCH settings including the status of its licenses, alert / badging modes, and its Emergency Special Access Mode (SAM) code, which can be used if a user forgets the SAM code that they have customized and temporary access to KEYWATCH Settings needs to be gained in order to reset the SAM code. For obvious operational security reasons, this Emergency SAM code should be treated as highly sensitive and not divulged to those who do not have a pressing 'need to know'. For additional information on these features, please see the KEYWATCH Mobile for iPhone or Android User Manual, as appropriate.

hotMIC, hotCAM, vidREC, geoTRACK, remoteTRIGGER, remoteSETTINGS	Shows the status of the software license on the mobile device. Shows 'Licensed' if the KEYWATCH app has a valid software license that has been activated from the device, 'Unlicensed' if not.
Alert by Badging	If Badging is enabled on the KEYWATCH mobile device, a badge with a value of '1' appears on the appropriate icon when the KEYWATCG app is triggered on (i.e., 'Voice' icon for hotMIC, 'Camera' icon for hotCAM, and 'Maps' icon for geoTRACK).
Alert by Popup	When enabled, an alert or notification will appear informing the user that a KEYWATCH app has been started, stopped, or that an error has occurred.
Panic Disables Airplane	Determines if airplane mode will be disabled (if enabled) when the distress signal is entered. This functionality is available only when using iOS (and not Android) mobile devices.
Panic Triggers Apps	When enabled, all (licensed) KEYWATCH apps will be triggered when the distress signal is entered by the mobile device user.
Emergency SAM Code	The emergency Special Access Mode sequence to access KEYWATCH Settings for a mobile device that requires a SAM sequence if the sequence is forgotten or lost.

Admin SIP Settings

This section provides the information necessary to set up and use a Softphone app in order to monitor hotMIC audio (see the [hotMIC](#) Section of this user guide for additional information).

This section also provides the user control for selecting whether to record on the ROC Server or not. By toggling the 'ROC Server Recording' to 'ON' or 'OFF', the user can enable or prevent all recording to the ROC for a particular KEYWATCH mobile device. By default, this setting is 'ON'.

Best Practices

The following is a list of recommended best practices that should be considered when planning an operation:

- Field test using the ROC in a situation resembling the intended operational use in advance of deploying it with the KEYWATCH mobile device(s) to become comfortable and proficient with operational use. In particular, we recommend that members of the monitoring team should also practice using remoteTRIGGER and remoteSETTINGS from the ROC and be comfortable with handling delays and momentary loss of data connection to the KEYWATCH mobile device due to gaps in cellular coverage and handoffs between cellular towers.
- Consider whether the operation requires recording to the ROC or not. Go to the device's **Device Settings** page and toggle the switch for 'ROC Server Recording' to the desired position.
- Prior to the operation, go to the device's pages to make sure that hotMIC, hotCAM, and geoTRACK evidence recordings from previous operations have been downloaded from the device in order to follow proper evidence handling procedures and maximize available recording space for the upcoming operation.
- After the operation, download the hotMIC, hotCAM, and geoTRACK evidence recordings from the mobile device and from the ROC server. If the operation is ongoing for multiple days, we strongly recommend downloading the evidence from the KEYWATCH mobile device on a daily basis. This will help control the space usage on the device and server, as well as help safely and properly maintain the evidential chain of custody. Once downloaded, delete the data from the phone to maximize available storage and decide if the evidence should be retained on the ROC for convenient review in the future. Good operational security (OPSEC) requires evidence to be downloaded after each operation; doing so will ensure evidence is current and organized and the device and ROC are ready for the next operation. OPSEC also strongly suggests that unnecessary evidentiary copies be deleted.

--- Support --- Legal