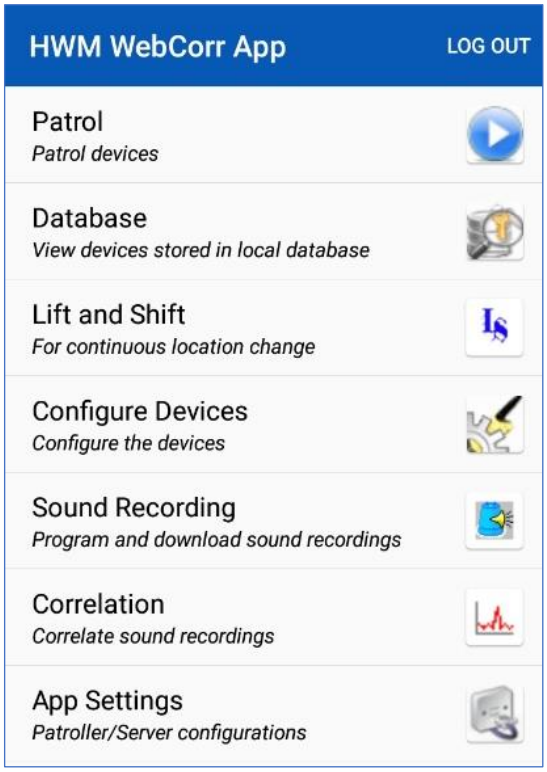
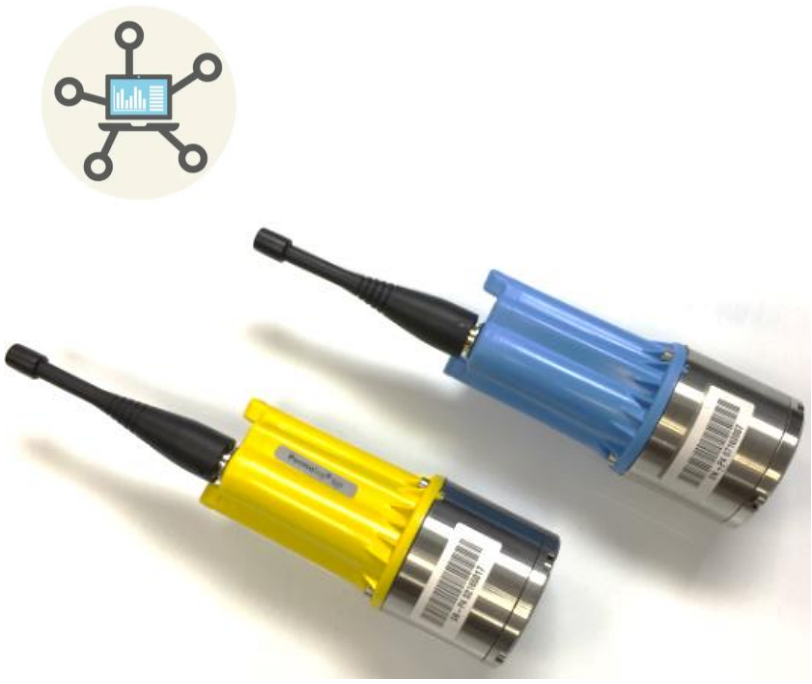
User Guide: PCorr+ and Permalog+
(Using the HWM WebCorr app).





Permalog+ PCorr+

TABLE OF CONTENTS

1 OVERVIEW

1.1 SYSTEM DOCUMENTATION AND SUPPORT OF PRODUCT

Read any "Safety Information" or "Safety Warnings and Approvals Information" documentation provided with the products prior to using.

Please also refer to the document MAN-031-0003 "User Guide: PCorr+ and PermaLog+ - (Description and uses)". This provides a description of PCorr+ and PermaLog+ logger devices, their functions, how they should be physically handled and examples of their use (e.g. Drive-by Patrol, Lift and Shift, Investigations).

This manual covers the use of the HWM WebCorr app to both set up the logger devices and collect data from them.

Note: Your phone may show views not identical to the pictures in this manual.
Pictures in the manual were created from screenshots using an Android phone.
Due to the wide variety of phones available to consumers, variations will exist.
Pictures in the manual are therefore presented for guide-lines only.
HWM will release software updates from time to time. These may also cause changes to the screen presentation and the functionality of the application.

It is recommended that you enable your phone to allow automatic updates of the WebCorr app.

HWM also provides support of the product by means of a webpage:

https://www.hwmglobal.com/pcorr-support/

Should you have any questions that are not covered by a manual, or Frequently Asked Questions (FAQs) provided online, please contact the HWM Technical Support team on +44 (0) 1633 489479, or email cservice@hwm-water.com

1.2 SYSTEM COMPONENTS

A system is comprised of:

- A set of logger devices (PCorr+ or Permalog+).
- A compatible Patroller unit (e.g. Patroller 4 radio transceiver with Bluetooth).
- A mobile phone.
- The HWM WebCorr app.
- An internet connection (for the mobile phone).
- A DataGate user-account and password
  (for the app to function and access the HWM database).

1.3 MOBILE PHONE – SPECIFICATION

The HWM WebCorr app is available on Android-based mobile phones and also on Apple iPhone mobile phones.

Minimum specification of phone:

Android: Android version 5 (Lollypop) minimum.
Device must have Bluetooth, GPS and Internet capability.
Memory (for application): 80MB
Memory (for data): 0.2MB typical per sound file.

Apple iOS: iOS version 8.0 minimum.
Device must have Bluetooth, GPS and Internet capability.
Memory (for application): 80MB
Memory (for data): 0.2MB typical per sound file.

1.4 Mobile Phone – Swapping Issues

Caution: Once a phone has been used by an installer it will contain data.
The installer should continue to use the same phone. Each time the installer swaps to using a different phone, unless it is handled carefully there is a risk of creating data issues due to a disruption in the synchronisation of data between DataGate and the mobile phone.
(See also sections 14.7 and 14.8 regarding misplaced or new phones).

1.5 WebCorr App – Installation

The app is available for Android phones, from the Google "Play Store".
The app is available for the Apple iPhone, from the Apple "App Store".

- Search for and locate the HWM WebCorr app.
- Install the app.
- The installed app will have an icon, as shown, when installed.

Occasionally, updates become available at the stores. It is recommended to install these updates.

1.6 Patroller

The app uses a Bluetooth connection to a compatible Patroller (e.g. HWM Patroller 4). Refer to the Quick Start Guide of the Patroller device for instructions regarding its safety, installation and use.

To work, the phone must have Bluetooth enabled and it must be connected to the Patroller (see section 3). Bluetooth radio has a range limit. Keep the phone close to the Patroller to ensure the Bluetooth radio connection can function.

The Patroller acts a communications relay between the loggers (using a proprietary radio-link) and the mobile phone (using a Bluetooth radio-link).

The Patroller is battery powered. It must be turned on to use. It can only communicate to loggers that are within radio range and also have an active radio-link.

1.7 PERMANETWEB - ACCOUNT AND PASSWORD

The WebCorr app operates with HWM's cloud-based logger database. These are known as "DataGate" and "PermaNETWeb". The app uploads its data to this database. DataGate and PermaNETWeb act as the store and main viewing portal for the data. The database can be accessed via webpages to view logger locations and results (not covered in this manual). Other webpages give access to administrative functions (also not covered in this manual).

A user-account must be used within the phone to give access to the online database. The account also acts as a security feature, with certain functions of the app hidden (or disabled) unless the app has recently logged into DataGate. Please contact your system administrator for the account and password allocated for the user of the phone app.

When the phone app logs in, it receives a token permitting it to be used for a short time. The app will require the user to log in again once the token expires.

1.8 DATAGATE – GIVING THE APP ACCESS TO LOGGER DEVICES

All PCorr+ and Permalog+ loggers must be registered on DataGate in order for the WebCorr app to use them. DataGate must be set to give the user of the app the required permissions to use the loggers.

Note: For a brief description of DataGate, and how to register both the loggers and also users of WebCorr, see section 13.

There is a security measure within the app, regarding logger data privacy…
The app will ignore any logger devices, or data that it receives from logger devices, that the user has no permission to use.

Note: If a logger is not appearing on the app it does not imply that it is not functioning correctly. Check with your system administrator that the logger device is correctly setup on DataGate for use with your user-account.

1.9 LOGGER – DATA DESTINATION

DataGate and PermaNETWeb webpages are the main viewing portal for logger data. This implies that the final destination of all logger data is the DataGate system.

The scheme is summarised here…

PCorr+ and Permalog+ **logger devices** produce measurement **data**. The logger device obtains several forms of data, each of which can be considered as a data **channel**. The data is meaningless, unless it represents a measurement actually made on the pipe network. Access to the pipe network is often available through various chambers that house (and give access to) valves or hydrants. These chambers can be used as an installation **site** for a logger device. A site may be one of many in an area or suburb, with the pipe network interconnecting them. Sites may therefore be collected together in a group, often referred to as a zone or **DMA**. Each of these separate entities may be represented on a **database**, such as one used by **DataGate**, which links some of them to a **user** of the system.

Or, put in reverse order…

- **DataGate** contains a database.
- A **user** of Datagate can be linked with multiple DMAs.
- Each **DMA** can contain multiple sites.
- Each **site** can have one logger device installed (maximum, at any given time).
- Each **logger device** can produce multiple **channels** of data.
- The **data** of a channel may be a one-off sample, or multiple samples that are obtained at different times.

The WebCorr app and DataGate are concerned with collecting data from the logger devices, linking it to the correct site and storing it.

Devices such as PCorr+ and Permalog+ can either be permanently installed or used as a **mobile** measuring device.

A mobile logger is time-shared by multiple sites and transferred from one site to another. The transfer process is known by various terms, including “Lift” and “Shift”.

In the time-share scheme, it is not necessary for *a particular logger* to be returned to a previously measured site that requires new data; *any equivalent logger* may be deployed to the site for producing new data.

The WebCorr app and DataGate manage the location of the loggers, the data collection and linking of the data to the correct site. This process relies heavily on the exchange of data between the WebCorr app and DataGate, in a process known as synchronisation.

Initially, when the app is first installed, DataGate is driving the data exchange and loads starting-point data into the app. The roles are then reversed… The app drives the data-exchange and keeps DataGate up to date with any new information.

The phone obtains some initial data from DataGate at each log-in time. This information includes lists of various parameters, including which logger devices the phone has access to, what installation sites exist, and which site (if any) a logger is installed at. The app adds any new information to its internal database.

As the app is put into use, further (newer) information is stored by the phone.
(e.g. New measurements obtained from the loggers and changes in their location of deployment). Each item of new information is tagged as an unsent data item.

DataGate must be brought up to date with this new information (stored by the app).
This is done as part of the synchronisation process.

Note: It is important to synchronise frequently to avoid loss of data.
Data held within a phone that becomes mis-placed (without it being synchronised) cannot be recovered.

Some of the data held within the phone is also made visible to users of the app.
This data includes:

- Deployment details (changes of location driven by the app).
- Measurement details (Leak status, Noise Level, Noise Spread) read using the app.
- Sound Recordings obtained using the app.
- Site locations (e.g. via a map display).

2 RUNNING THE SOFTWARE APP – FIRST-TIME SETUP

Note: HWM revises software from time to time, so the screenshots provided in this guide may be different from what you experience when you download the app.

2.1 LAUNCHING THE APP

Find the HWM WebCorr app on your mobile phone.

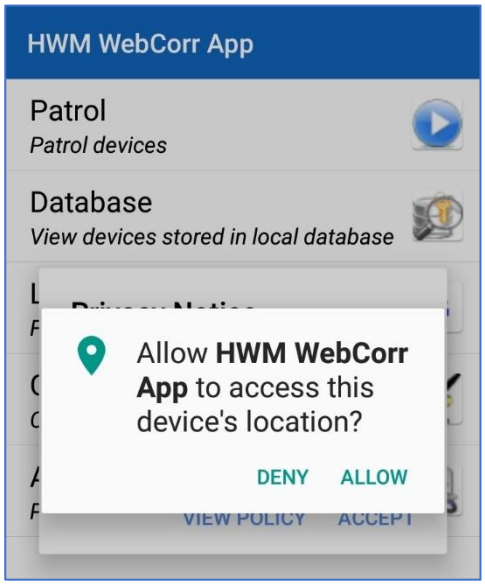
Launch the app by tapping the icon.

The first time an app is run, or after it has been upgraded to a new version, the phone makes a sequence of one-off requests.

It may ask the user for permission for the app to use the phone location services.

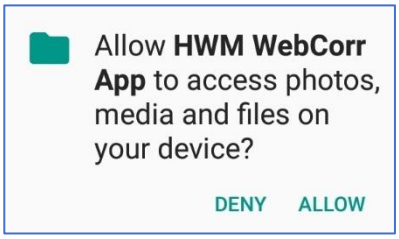
Tap on ALLOW...

Note: The phone should be set to give "high-accuracy" location details to the app. (This is a setting within the operating-system of the phone).

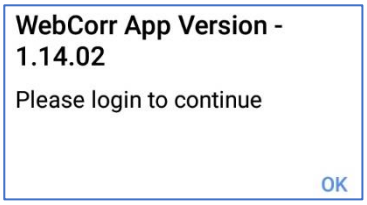


The app may also request permission to have access to the files on the phone.
(The app requires this permission to allow it to store data).

Tap on ALLOW...

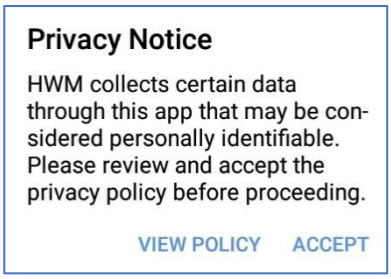


You are required to log in, to verify you are a valid user.



View and accept the Privacy Notice.

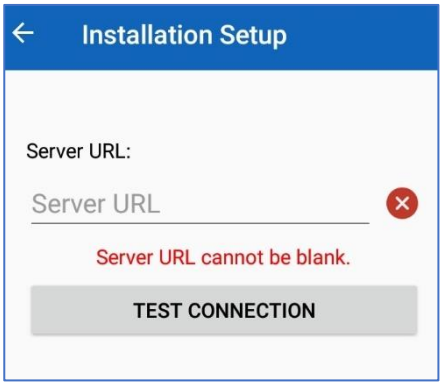
Once accepted, the app will continue to load and operate.



The app must be given the URL of the server, so it can find the correct internet address to communicate with.

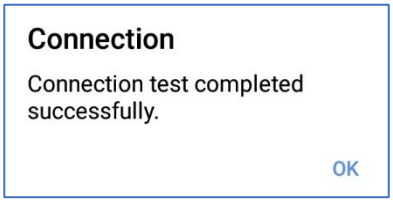
Enter the details provided by your system administrator.

Tap the "TEST CONNECTION" button; This checks the mobile phone can connect with the server.



If communication is possible, the app will confirm that the connection test succeeded.

Note: This process does not authenticate the phone for use. User details must be entered at a later stage.

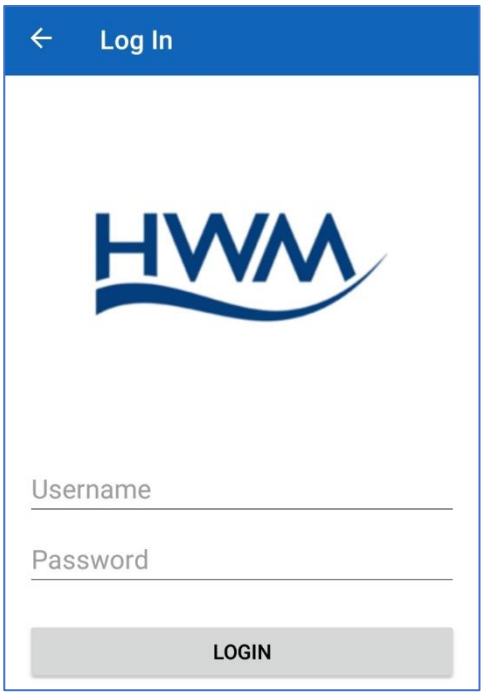


Tap the back-arrow on the top-left of the display.

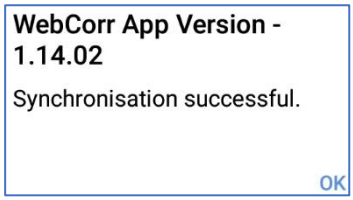
The user login screen appears.

Enter the Username and Password for the user into the phone.
These are required for the app to be able to log in.

The tap on the "LOGIN" button.



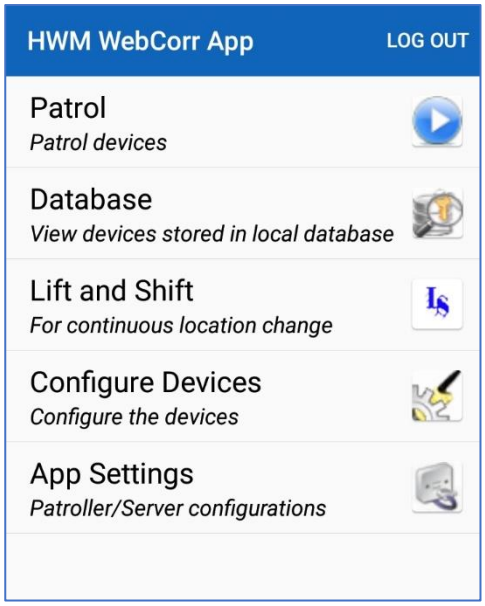
If log-in is successful, the phone will do an initial synchronisation.



**** The initial setup of the phone, including the link to the server is now complete. ****

The app will then show the main screen:

More icons will become visible after the app itself is connected to the Patroller4.

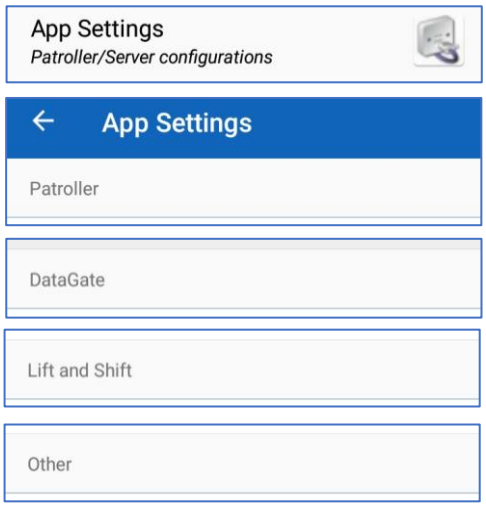


2.2 Setting of App Options

From the main window, tap on “App Settings”.

The app settings view is divided into several areas:

- Patroller
  (Covered in section 3).
- DataGate
  (Covered later in this section).
- Lift and Shift
  (Covered in section 8.2).
- Other
  (Covered later in this section).



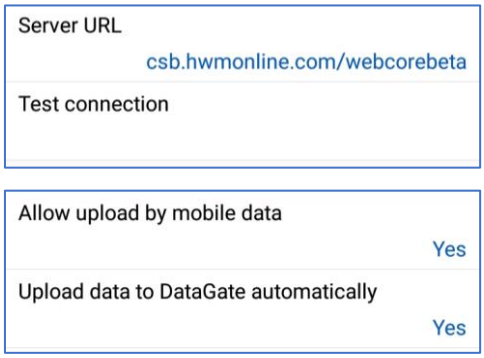
2.2.1 App Options – DataGate

“Server URL” will have been completed by the setup process (see 2.1). Tap on “Test connection” if you wish to re-run the internet connectivity test.

“Upload of Data to DataGate automatically”:

When set to “Yes” (recommended):

- The app syncs in the background immediately after each lift or shift.



- Manual sync should be done by the user at the start and end of each day, especially if the user is not using lift and shift functionality daily.

When set to “No”:

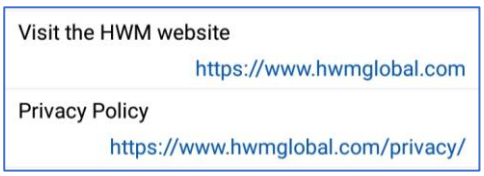
- The app will ask the user if it can sync, every time it writes new information into its database.

“Allow upload by mobile data” is recommended to be set to “Yes”. However, if the user wishes to delay sending of information until a Wi-Fi connection exists, set to “No”.

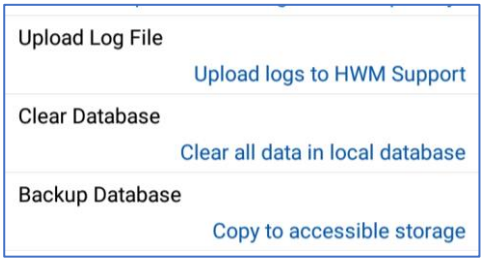
2.2.2 App Options - Other

Tap on App Information to see app information including the software version.

There are links to the HWM website and also the privacy policy.



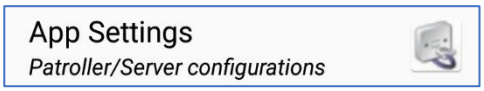
Options exist for various functions that may be requested to help HWM to support the product.
e.g.: Database Backup and Clear.
Upload of Log files to HWM.



3 CONNECTING THE PATROLLER AND APP OVER BLUETOOTH

Check the Patroller is switched on prior to trying to connect the app with it.

Tap on “App Settings”.

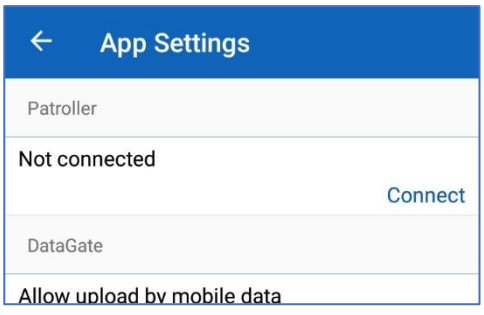


Find the “Patroller” section within the App Settings window.

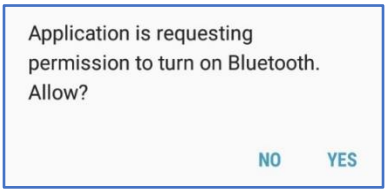
This section shows the connection status.

There is a control to connect (or disconnect).

Tap the “Connect” line to start the connection process.

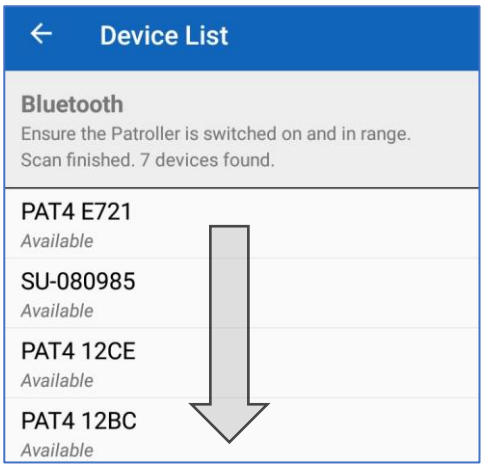


If required, give permission for the app to use Bluetooth.



The app searches for Bluetooth devices and lists them.

The Patroller will be identifiable by the Bluetooth-ID matching a part of the serial number, or some other identification on its label.



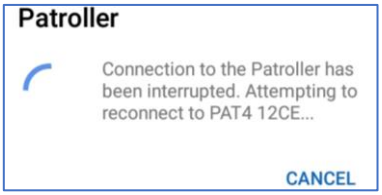
If the Patroller is not listed, gently swipe the list on the screen downwards (as shown) to re-start the search for Bluetooth devices.

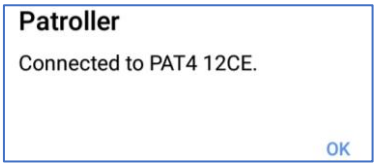
When the Patroller is listed, tap the line to attempt to connect to it.

Progress of the attempt to connect will be shown, along with a confirmation message when connection is successful.

If the connection attempt is not successful, try again, until the "Connected to ..." message is displayed.

Note: Bluetooth is a short-distance radio link. It is possible for the link between the phone and the Patroller to drop for a variety of reasons (e.g. If the phone is taken too far from the Patroller).
If the link drops, the app will continue to look for the Patroller for a short time (up to 10 minutes), and will attempt to reconnect automatically.
When re-connection is successful, a "Connected..." message appears on the phone display for 5 seconds, then normal operation resumes.





If the user considers the process is taking too long, they can cancel the operation and manually re-connect to the patroller.

When the Patroller is powered over USB is it always on. If NOT powered by USB, check the Patroller is still on.

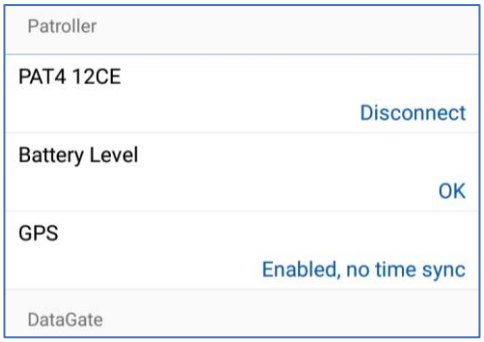
Note: If the Patroller is battery powered, it can switch itself off when it has not been used for some time (approx. 30 minutes); It does this to conserve battery use. It will also disconnect if the battery runs very low.

Once connected, an indication of the battery level of the Patroller can be obtained.

Tap the “Battery Level” line to get the current level.

OK = More than 15% charged.
Low = Below 15% charged; Charging advised.
Charging = Plugged in and charging.

The user can periodically check the battery level by returning to this screen.



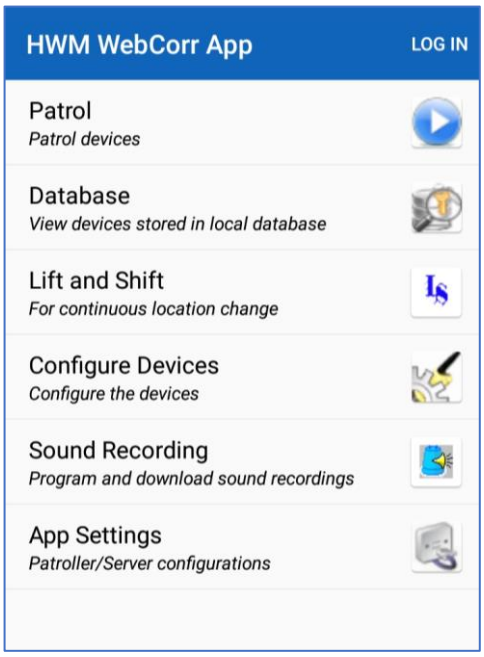
The status of the “GPS time-sync” is shown (either “no time-sync” or “time-sync OK”).
GPS can provide a very accurate time to the Patroller, but when not available the Patroller uses the time available from the phone.

Tapping the “GPS” line shows more details.

4 App – Main Window

The main window of the app is shown opposite.

The window is used to navigate to the various functions of the app.



In summary…

The “App settings” window concerns:

- Connecting the phone with a Patroller device over a Bluetooth radio connection. Obtaining status info about Patroller health.
- Setup of the app to use DataGate for authentication and data upload.
- Allowing automatic upload of some data.
- Lift & Shift options for downloading sound files from each logger device.

- App information (e.g. Software version).
- Options (mainly used if requested by HWM providing support of the app):
    - Backup or erase the app database (measurements and deployments) from the phone.
    - Send event log data to HWM.

The “Patrol” window concerns:

- Obtaining data: Leak-status and measurement summary from devices that come into radio range during a “patrol” or “drive-by patrol”.

The “Lift and Shift” window concerns:

- Creating new installation sites (if required).
- Deploying logger devices to installation sites.
- Lifting loggers from installation sites to make them available for re-deployment.
- Obtaining data: Leak-status and measurement summary from devices as part of the Lift process.
- Downloading Sound Recordings from devices (dependant on settings).

The “Database” window concerns:

- The history of logger deployments to sites made by the phone
  (Sites that a device has been installed on, start date and end date).
- Leak-status and measurement summary obtained from loggers using the app.
- Sound recordings obtained from logger devices by the app.
- Visible markers of any un-synchronised data, between the phone memory and DataGate; Synchronisation can be initialised from this window.

Note: The phone has to have actually been “driving” the logger for any entry into the visible database. Only data from the phone’s actions are displayed. No historic data is downloaded from DataGate into the displayed database (although some may be used by the app, invisible to the user).

The “Configure Devices” window concerns:

- Setup of the Patrol Window (radio-link availability) of the logger device.
- Setup of the time that the daily leak-evaluation will run.
- Setup of whether the logger-devices should auto-record the sound upon finding a new leak.
- A facility to read the settings from a logger device.

The “Sound Recording” window concerns:

- Making a one-off scheduled sound recording at a set time (the regular logger program is suspended until the 1-off scheduled recording is completed).
- Download of a completed sound recording file.

5 MANAGING LOGGER LOCATION AND DATA

A “DMA” is a means of grouping sites, typically those interconnected by the pipe network in a local area.

A “Site” is a location on the pipe network (typically a chamber giving indirect access to the pipe, via a valve or hydrant) where a monitoring device (logger) can be installed.

From the **database** point of view, a site can contain zero or one loggers.

The app regards loggers to be in one of three states …

- Deployed.
  (i.e. Installed on a Site).
- Non-Deployed.
  (i.e. Not installed on a Site; Being stored at an undefined location).
- Non-existent.
  (i.e. DataGate has not given the app authority to use the logger. This could be intentional, or DataGate data is incorrectly set up, or the app requires synchronisation with DataGate to be able to use newly added logger devices).

The app is so constructed that it shares information with DataGate.

DataGate regards loggers to be in one of two states …

- Deployed.
  (i.e. Installed on a Site).
- Non-Deployed.
  (i.e. Not installed on a Site; Being stored at an undefined location).

One of the purposes of the app is to feed information into DataGate. The information it sends includes:

- Changes in a logger location.
- Measurement data collected from a logger.
- Sound files collected from a logger.

The app uses the memory of the phone to locally store data. To do so it creates a local database. Upon first installing the app, the database is empty. The app has no knowledge of what logger devices it is going to be managing or where the loggers are currently located. To obtain this information it must contact DataGate, log into it and synchronise with it. After the initial synchronisation, the app can update its internal database with data describing its starting position. From that point on, it will be “in the driving seat”, storing any location changes or newly collected measurements locally, pending upload to DataGate. The new information is uploaded to Datagate as part of the information exchanged during subsequent synchronisations.

Note: It is important to synchronise frequently with DataGate so that office staff can respond to the leak-status information collected from the loggers in a timely manner.

Note: Any unsynchronised data stored on a misplaced phone becomes lost.
In such a scenario, DataGate may give inaccurate information regarding logger locations to a replacement phone.

Once the app is operational, and has an initial database, its main activities can be summarised as follows:

- Only non-deployed (stored) loggers can be installed (deployed).
  (This is known within the app as a "Shift").
  A "shift" is required to deploy any logger to its new site; It does not matter if the installation of the logger is intended to be short-term or long-term.
- Only deployed loggers can be removed from their site (un-deployed).
  (This is known within the app as a "Lift").
- The phone app keeps track of location changes within its local database until it has uploaded them to DataGate. The location changes then become visible to other users (e.g. Office staff).
  The app keeps track of what information is already sent and what is yet to be sent.
- Deployment can be to an existing site, as long as the site is unoccupied.
  It may also be to a new site; The app can create new sites when required.
  The app requires that new sites must be part of a "DMA". Usually this will be an existing DMA, but new DMAs can also be created when required.
- Measurement data can be collected from the loggers by either of two activities…
  - If there is no intention to remove the logger from its installation site, data for the site is collected using a "patrol".
  - If a logger is being removed from its site, final measurement data for the site is obtained as part of the "Lift" process.
- Measurement data is saved in the local database until it can be uploaded to DataGate; The app keeps track of what data is already sent and what is yet to be sent.
- If there is a sound recording within a logger, it can be downloaded (PCorr+ loggers can contain a maximum of one sound recording).
  These are then stored on the phone. They are already time-stamped by the logger with the recording date and time. The app keeps track of what sound files are already sent to DataGate and what is yet to be sent.
- The app synchronises with DataGate including an upload of its new data items.
- Measurements or sound recordings made by the loggers whilst in storage may also be sent by the app to DataGate, but DataGate will discard them; The loggers were not deployed to any site when the data was obtained.

The app can also be used for additional purposes:

- It can be used to program the loggers in order to set the time of their repetitive daily activities (leak detection time, etc).

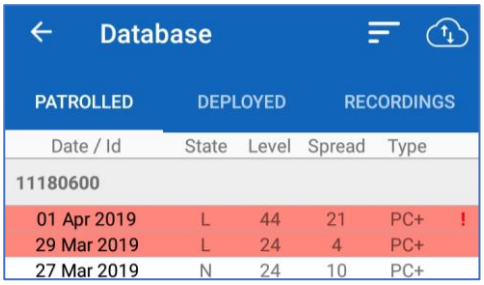
- It can be used to temporarily suspend logger's regular activity in order to make a one-off scheduled sound recording (PCorr+ only). It can download the sound recording after it has been made.
- It can be used to put the loggers into a mode suitable for long-term storage.

6 APP – DATABASE

From the main window, tap on the "Database" line.

The Database window consists of 3 tabs:

- "Patrolled"
  (Lists leak-status measurements).
- "Deployed"
  (Lists deployment periods).
- "Recordings"
  (Lists sound recordings).



On the Deployed and Recordings tabs, the app lists only data from activities the phone itself has been responsible for. Initially, no data is listed.

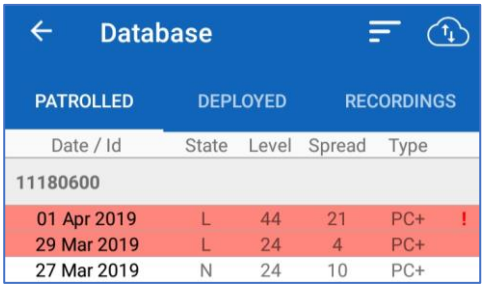
As the app becomes used, each tab will fill with data. When too much data is available to fit on the screen, it can be scrolled by placing a finger on the screen and moving the list up or down. The app removes data more than 3 months old to reduce memory use.

6.1 DATABASE – PATROLLED TAB

The "Patrolled" tab contains a list of data items regarding the leak-state of the logger devices.

The list can be ordered in several ways – choose from the local options menu.

There is no indication in the list of the site the logger was on when it made the measurement (linking to a site is described later).

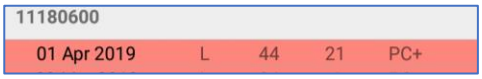


Note: The list will contain a maximum of one measurement per site per day for each logger. This is because the normal activity of the logger is to produce just one leak evaluation per day.

Any unsent data items have an exclamation mark next to them to indicate it is unsent (see diagram above).

Tapping on the Sync icon will initiate a synchronise with Datagate including sending all unsent data items.
(You may be requested to enter your password and log in as part of the sync process).

Data that has been sent to DataGate no longer has an exclamation mark next to it.



"Level" and "Spread" indicate the noise-level and noise-spread of the measurement, which together form an indication of how persistent a noise-source is.

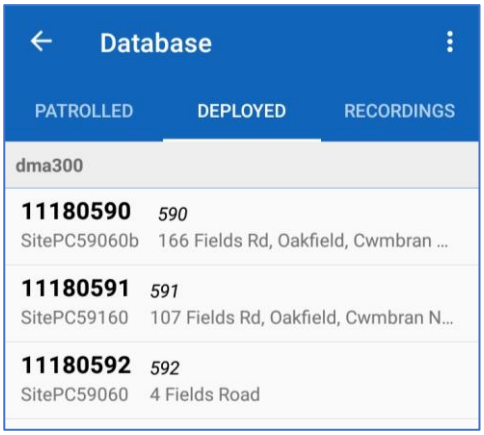
"State" is the logger judgement of either a leak being present (shown as "L") or no leak being present (shown as "N").

A no-leak status is listed with a white background. A leak status is listed with a coloured background to draw attention to it.

Linking the logger measurement to the site on which the measurement was made is readily done using Datagate. It can also be made using the phone by noting the logger number and the date the measurement was made. The "Deployed" tab data can be used to identify where the logger was. This should be no issue for a permanently installed logger, which will still be on the same site. For a mobile (Lift and Shift) logger, the measurement will have been taken a few seconds before it was lifted from a site, and the user has to identify the correct time period of deployment.

6.2 DATABASE – DEPLOYED TAB

The "Deployed" tab contains a list of records regarding the deployment periods of the logger devices.



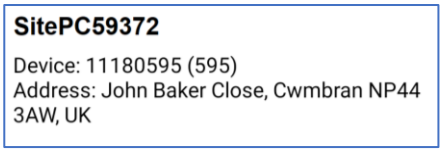
Each line represents a deployment interval for the logger.

The serial number is shown, along with an "easy-ID" (a user-defined name) of the logger device.

The site and address of the deployment are shown.

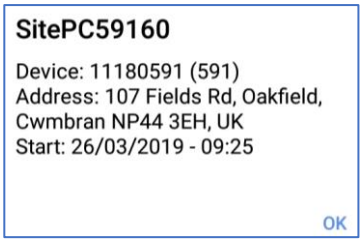
Tap a line to show more detail, which appears in a pop-up box.

The app only shows times for actions it itself has driven.

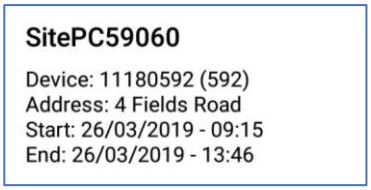


Sites with a deployed logger, but no start or end date have been uploaded with this information by DataGate.

Sites with the logger deployed by the phone have only a start time.

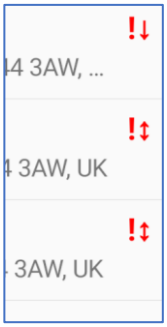


Sites with the logger deployed and removed by the phone have both start and end times.



Any unsent deployment data items will have an exclamation mark next to them in the "deployed" tab list. Sync if required (as described earlier).

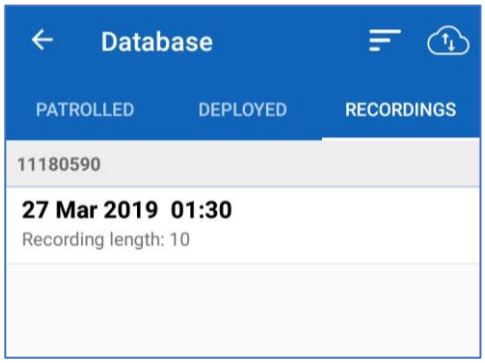
Next to the exclamation mark for unsent data is an arrow indicating what events have not been sent to DataGate.
Up arrow = Lift
Down arrow = Shift
2-headed arrow = Both Lift and Shift.



The sites where loggers are currently installed can be shown... Tap "Show on Map".

6.3 DATABASE – RECORDINGS TAB

The "Recordings" tab contains a list of data items representing sound recordings that have been downloaded from the logger devices.



Each line shows the logger number, date and time the recording was made.

Any unsent data items have an exclamation mark next to them to indicate it is unsent (Not shown).
Sync if required (as described earlier).

Note: Any sound items having an "E" next to them (not shown) indicates an error when uploading to DataGate. Usually it is because DataGate could not link the sound recording to a site. Typically, the logger was not deployed when the recording was made. The user may investigate if the sound file should be re-made.

Linking the logger to the site on which the sound recording was made is readily done using Datagate. It can also be made on the phone by noting the logger number and also the date on which the sound recording was made. The "Deployed" tab can be used to identify where the logger was (but only if the phone itself deployed the logger to the site).
If the phone cannot identify where the logger was when the sound recording is made, it will still upload the file and it is left to DataGate to resolve which site the recording was made on.

This window can also be used to playback sound recordings – See 11.3.

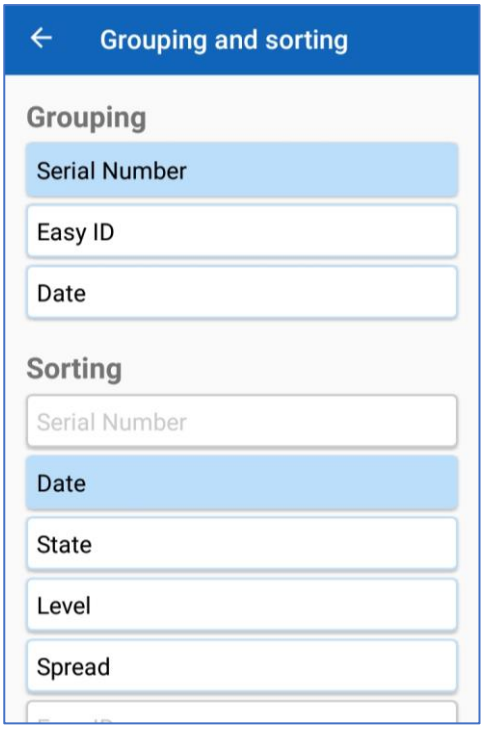
7 APP – LOCAL DISPLAY OPTIONS

Many windows will have local options for the information being displayed.

Tap on one of the local options icons (shown) to select an option for the current display.

Sometimes a simple "selection menu" is produced for the user to select from.

At other times a new window will display in order to make the required selections.
(e.g. the "Grouping and sorting" window, shown opposite).



8 APP – LIFT AND SHIFT

The "Lift and Shift" window is designed primarily for mobile loggers that are time-shared between multiple sites. Strictly speaking, it is used to manage the **location data** of **all logger devices**. It tracks the location change within the app database whenever the installer both deploys them to a site and (later) removes them from the site.

When deploying a logger to a site, the app can re-use existing sites or, when necessary, create new sites within the database for use.

"Shift" is the action of deploying a logger to a site (i.e. Installing it).

"Lift" is the action of removing an installed logger from its site.

The combined process of "Lift and Shift" moves a logger from one site to another within the database. Invariably, there is a mid-point in the logger relocation process where the logger is temporarily being stored (e.g. in a vehicle) whilst it is being moved, and the exact location does not matter since it will not be producing useful data.

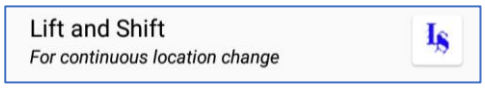
Loggers repetitively make measurements, but no measurement is meaningful unless a logger is actually installed on a site at the time it makes the measurement.

8.1 DEPLOYMENT OF A LOGGER DEVICE TO A SITE (SHIFT)

Select a logger for installation and find a suitable installation site.

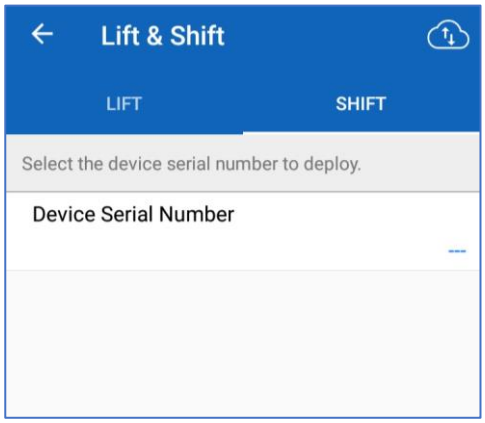
Note: The Patroller should be left in the vehicle whilst installing the logger.
(This protects it from damage due to adverse weather).

Tap the “Lift and Shift” line in the main window.



Select the “SHIFT” tab.

This information shown in the window must be built, one line at a time, with details of the logger’s new site of deployment.



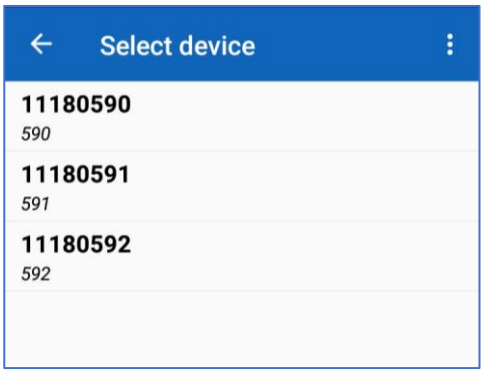
The first stage is to select the logger device.

The app must be aware of which loggers it can access, as well as their status (deployed or undeployed, etc).

Tap the sync icon (if required) to download any new logger devices from DataGate.

Tap on the “Device Serial Number” line.

The “Select Device” window will appear, listing all loggers that are available for deployment; move the list up or down and find the logger.



The logger list can be sorted by either serial-number or an “Easy-ID”.
“Easy-ID” is a user-editable field (see later) that can identify the logger (e.g. if the user labels the loggers).

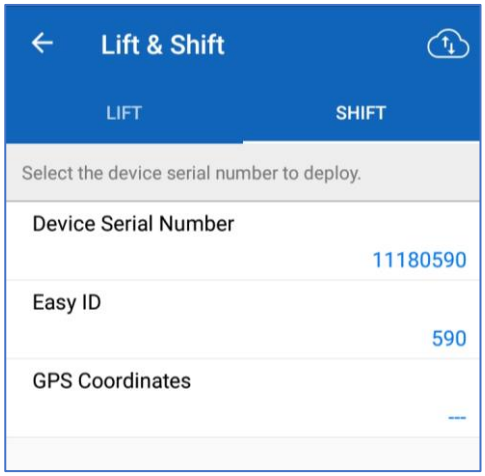
The Serial number is factory set and cannot be edited.

Tap on the line of the logger you wish to deploy.

The logger’s details are added to the display.

(If the wrong logger was chosen, tap on the “Device Serial Number” line and pick another logger).

Tapping on Easy-ID allows you to enter or edit this field.



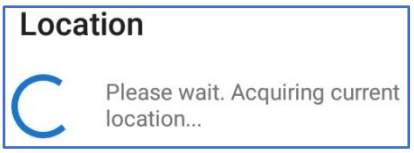
The next stage specifies the location of the site that the device is being deployed within.

Tap on the “GPS Co-ordinates” line.

The site can either be re-use of an existing one, or (when required) an entirely new one.

A local map is utilised to correctly locate the site…

The phone needs to determine where it is currently located; Then it can load a relevant map (provided by an internet map service) into the display.



The app uses the phone's location service (provided by the operating system of the phone) to obtain GPS co-ordinates of its location.

If the app is unable to get GPS coordinates from the phone (e.g. GPS signal is lost) it will instead use the GPS coordinates obtained from a recently visited location.

Note: Pay attention to the status bar of the phone (usually at the top of the screen).

Check for the geolocation symbol (see left).
If it is not visible when on the "Lift and Shift" screen, there is a temporary problem with the app using the location service.
(e.g. It may not be switched on within the phone, in use by another app, or the phone is slow to start it.)
If the icon is not displayed, leaving and then returning to the Shift tab will often clear the problem.

The "Local Map" window is loaded.

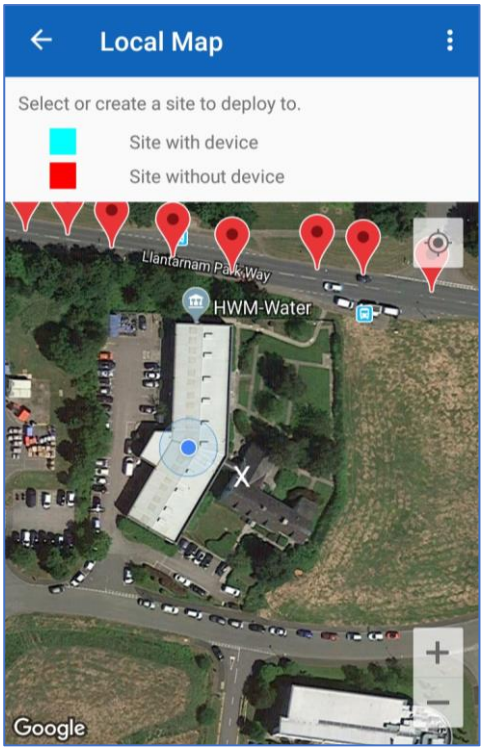
The map can be moved and zoomed to show a new area using the touchscreen and the standard methods for the phone.

The initial display shows a blue dot where the phone is located.

An "X" is used as a cursor to mark the installation location.

The location of any existing local sites can be displayed (use options to view these), together with an indication of whether the site is already occupied by a logger or not.

Moving or zooming the map can affect the "search area" of what is considered to be local.



Options for logger deployment are either:

- To deploy the logger to an existing site, or
- To create a new site for use, and then (immediately) deploy the logger to it.

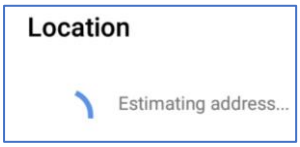
Methods for both options are described below…

The description that follows are for the creation of a new site…

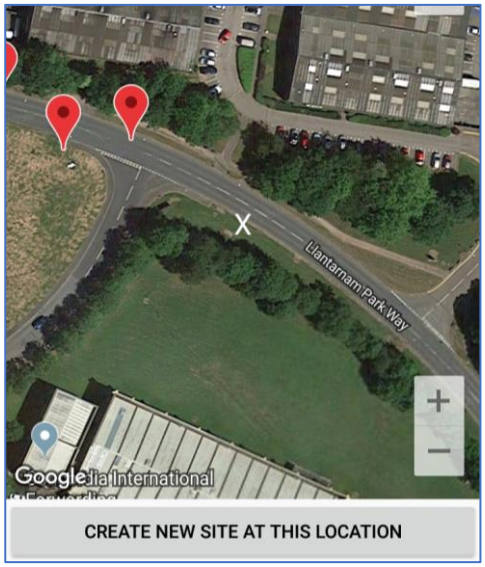
Position the "X" at the correct location of the new site (zoom in and pan the map as required to be accurate).

Then tap the button "CREATE NEW SITE AT THIS LOCATION".

The app uses the GPS co-ordinates of the position the cursor is on for the new site.



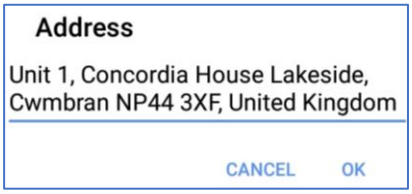
It then tries to obtain an estimated address for the new site. (This can take several seconds to complete).

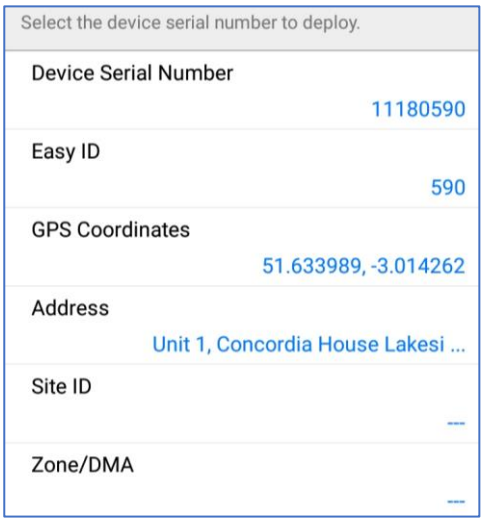


The information is obtained and loaded into the window.

An additional 2 lines also appear.

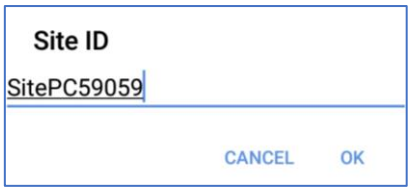
The address can be manually edited when creating a new site; Tap on the address line to edit it, if required.





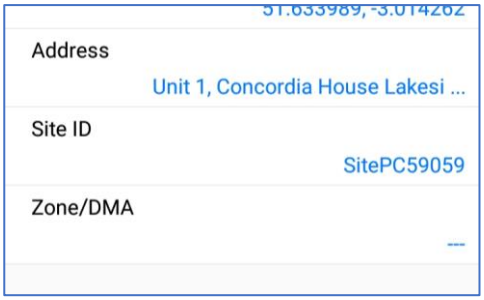
The next stage is to enter a Site ID:

- The Site ID may be left blank.
  The app will obtain an automatic (and meaningless to the user) site ID from DataGate during the next synchronisation.
- Alternatively, tap on Site ID line, and enter a user-defined site-ID, if required.



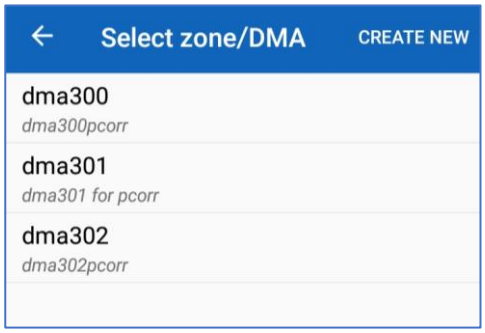
The DataGate system also requires a site to exist within a DMA. The next stage is to select a DMA.

Tap on the “Zone / DMA” line…



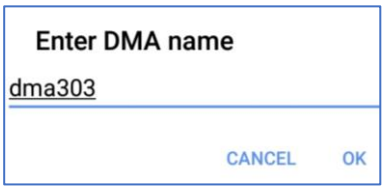
The app shows a list of any DMAs that already exist.

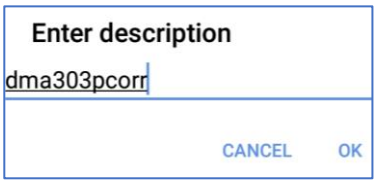
To add the site to an existing DMA, tap on the chosen one to select it.
The option also exists within the app to create a new DMA (when required).



To create a new DMA…
Tap on “Create New”.

Enter the DMA name, and later a description of the DMA.

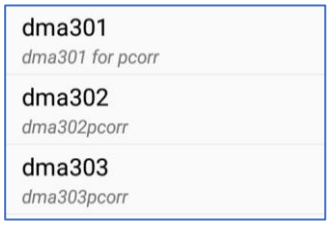




The DMA will be added to the DMAs listed.

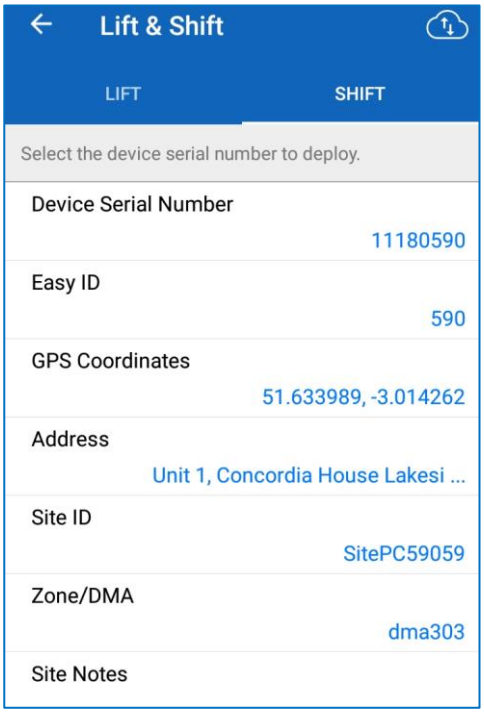
Tap on the DMA to select it.

The DMA is added to the window.



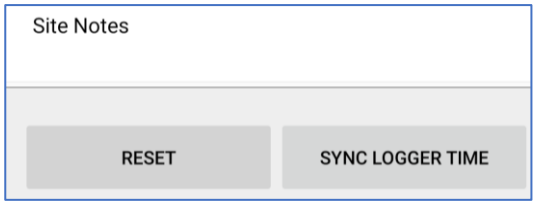
A “Site Notes” field appears, which can be used to add notes to the Datagate system (optional).

The window now has complete details of where the new site is to be created and which device is being deployed to it.



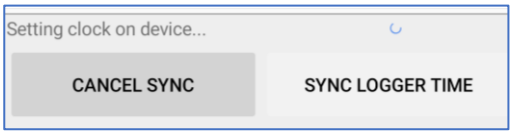
Before the logger can be deployed, the app has to be able to communicate with it in order to set its clock. This ensures the logger clock is kept accurate.

Tap on the “Sync Logger Time” button.

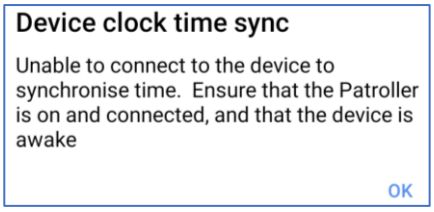


If the Patroller is not yet connected, a scan for Bluetooth-compatible devices will be made, and the user will have to select the Patroller from the list (similar to section 3).

When connected to the Patroller, the user has the option to press the “Cancel Sync” button to cancel the task of setting the logger clock; This should not normally be done. Above this button, there is a text area which shows the progress.



The process of setting the logger clock should take less than 10 seconds. If the user cancels the operation, or if it takes longer than 10 seconds, the user can try again.
Re-swipe the logger to make sure the radio-link is active before re-trying.



After the logger clock has been successfully set a “Deploy” button appears.

Tap on the “Deploy” button.

Within the local database, a new site is created, and the selected logger is deployed within it. The data items for both events are tagged as unsent to DataGate.

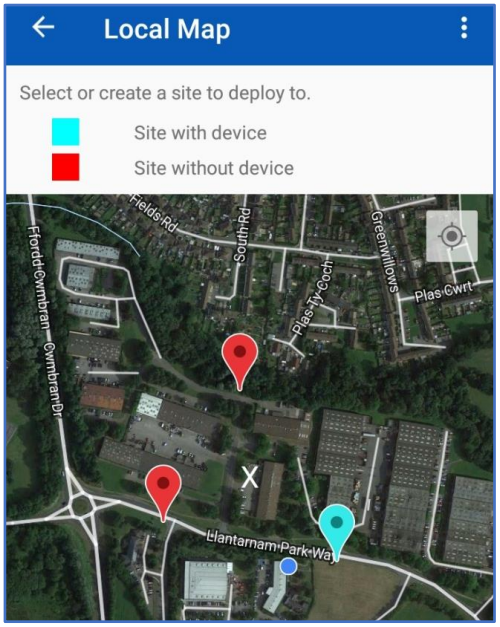
The logger device will disappear from the list of loggers available for deployment. (It has now been moved into the list of loggers that are available to lift).

Depending on the options selected in the App Settings, a synchronisation will either immediately commence, or the new data will be queued to be sent during the next synchronisation.

The description that follows are for the re-use of an existing site…

Position the “X” symbol approximately where you wish to deploy the device.

Use the “clear local sites” and “refresh local sites” options as required to update the display to show all the sites in the locality of the “X”.



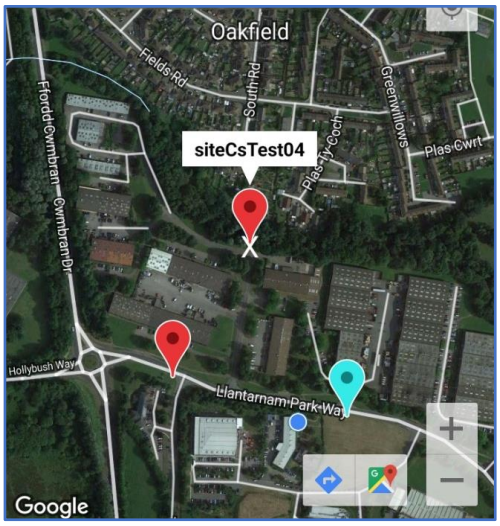
Tap on the geo-symbol of a site without a device. (Unoccupied sites are displayed as a red symbol).

This will re-locate the site to the centre of the screen.

A “text bubble” appears showing the name of the site.

(If the wrong site was chosen, tap an empty area of the map to de-select the site).

Tap once more on the “text bubble” to select the chosen site and return to the previous screen.

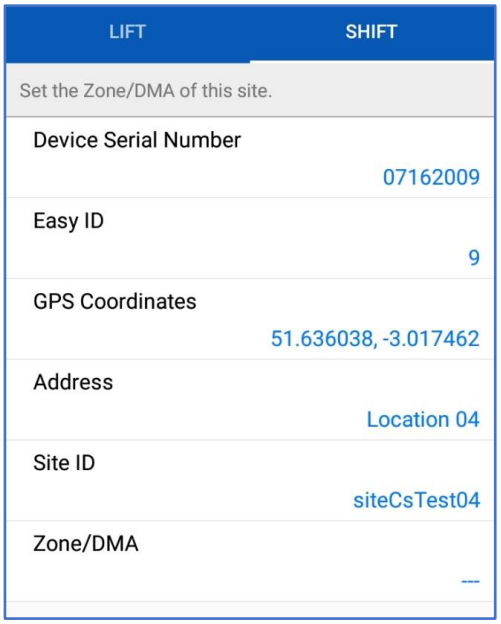


The details of the existing site are loaded into the display.

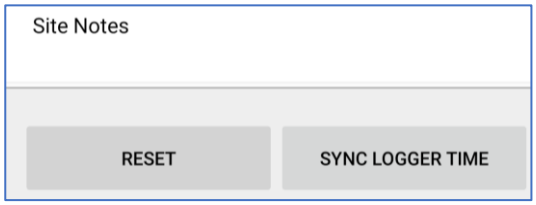
These are not editable.

Next tap on and select a Zone / DMA.

(This is editable since DMA boundaries can be re-drawn).



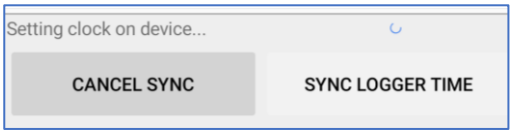
Before the logger can be deployed, the app has to be able to communicate with it in order to set its clock. This ensures the logger clock is kept accurate.



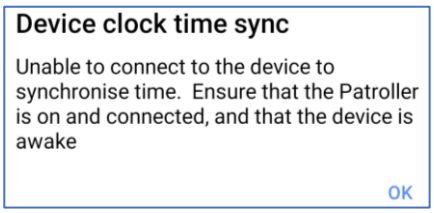
Tap on the “Sync Logger Time” button.

If the Patroller is not yet connected, a scan for Bluetooth-compatible devices will be made, and the user will have to select the Patroller from the list (similar to section 3).

When connected to the Patroller, the user has the option to press the “Cancel Sync” button to cancel the task of setting the logger clock; This should not normally be done. Above this button, there is a text area which shows the progress.



The process of setting the logger clock should take less than 10 seconds. If the user cancels the operation, or it takes longer than 10 seconds, the user can try again.
Re-swipe the logger to make sure the radio-link is active before re-trying.



After the logger clock has been successfully set a “Deploy” button appears.

Tap on the “Deploy” button.

Within the local database, the selected logger is deployed within the chosen site. The data items for this event is tagged as unsent to DataGate.

The logger device will disappear from the list of loggers available for deployment. (It has now been moved into the list of loggers that are available to lift).

The changes will be sent to DataGate during the next synchronisation.

8.2 Removal of a Logger Device from a Site (Lift)

The app provides a “Lift” function which performs 2 (or optionally more) tasks:

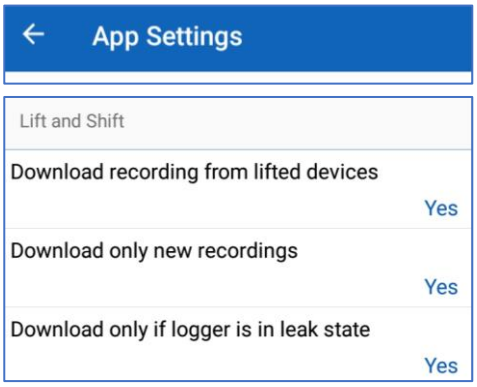
- It obtains the final leak-state information for the site.
- It records that the logger was removed from the installation site.
- (Optional) It checks for a sound recording in the logger, and (dependant on settings and other parameters) proceeds to download it.

Note: Download of a sound file can be a difficult task for several reasons (e.g. competing local radio transmissions); The app gives the user some control of how to handle the logger data if difficulties should occur.

This information is stored within the phone, pending upload to DataGate.

8.2.1 Options for automated download of a sound recording

Prior to covering the lift process, an explanation of the options associated with it will be considered. These are found under “App Settings”.



If there is a sound recording in the logger, the app has to decide whether or not to download it, using the option settings.

They are evaluated in the sequence:

1. Download recording from lifted devices.
2. Download only if logger is in leak state.
3. Download only new recordings.

They can be considered to be a set of filters that can either reject a file for download OR allow it to pass through to the next evaluation stage.
… The sound file has to get past all 3 stages for it to be downloaded.

“Download recording from lifted devices”:

When set to “No” …

- No attempt is made to download a sound file from any logger; all are rejected.

When set to “Yes” …

- The file will be accepted for further consideration for download.

“Download only if logger is in leak state”:

When set to “Yes” …

- The file will be rejected for download if the logger is NOT currently indicating a Leak condition.

When set to “No”…

- The file will be accepted for further consideration for download.

“Download only new recordings”:

When set to “Yes” …

- The app will first read the timestamp for the recording.
- If the recording was made earlier than the start of the current deployment, no attempt will be made to download it.
- If the recording was made during the current deployment, the app will download the file. When sending the file to DataGate, the site and recording are linked.

When set to “No” …

- The app will download the file.
    - If the location (site) of the logger at the time of recording is known by the app, when sending the file to DataGate the site and recording are linked.

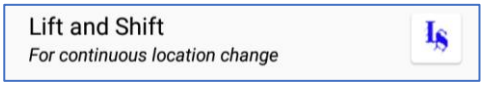
- If the logger is known by the app to be undeployed at the time of the recording (e.g. stored in a van over-night), the app cannot link the recording to a site. When sending the file to DataGate, the site and recording are not linked. The recording is sent as belonging to an anonymous site, and DataGate will be unable to use the recording.
- If the location (site) of the logger at the time of recording is NOT known by the app (e.g. It was made before the app was installed), the app cannot link the recording to a site. When sending the file to DataGate, the site and recording are not linked. The recording is sent as belonging to an anonymous site, and DataGate will attempt (using its own database) to link the recording to a site if possible.

If the sound recording already exists on the phone, it will be over-written.

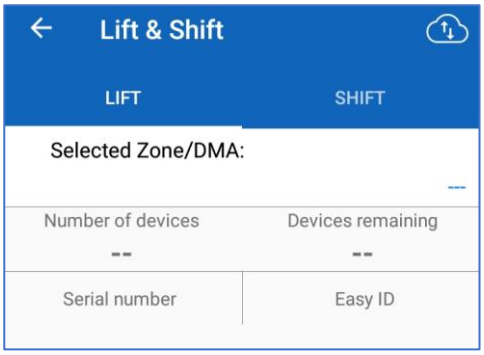
8.2.2 Removing a Logger from Site (Lift) – Without sound download

The "Lift" process is now described…
(The simplest case is given here, where the options are set to disallow any sound download). (see 8.2.1)

From the main window, tap the "Lift and Shift" line.



Select the LIFT tab.



Tap the sync control to download the latest DataGate information regarding owned loggers (if required).

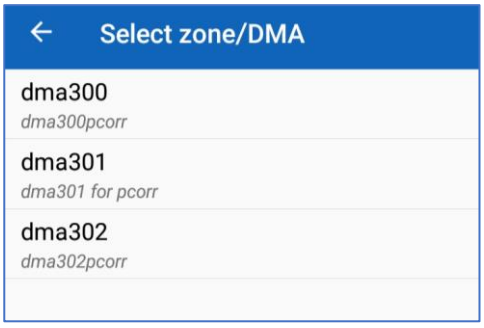
It is recommended to download latest data at least once a day.

The app needs to know which logger devices it is required to look for (i.e. which DMA contains the sites that the loggers are deployed within).

Tap the "Selected Zone / DMA" line.

A list of DMAs will be shown.

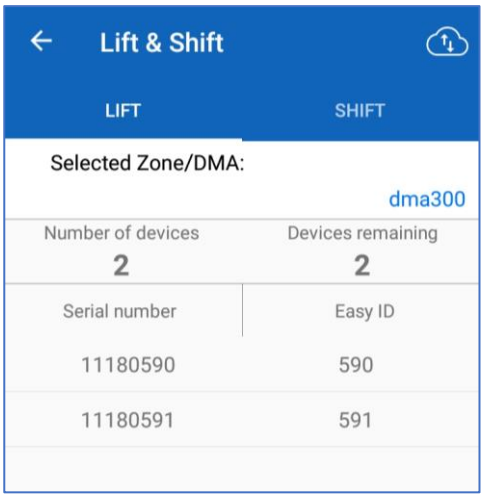
Select the DMA for the area the loggers are currently installed within.



The app will initially list all the loggers that are currently deployed in sites that are within the chosen DMA.

As loggers are picked-up over the radio link, their data will be collected, and they will be removed from the list.

Above the list, a summary shows the number of devices remaining to be found.



To start the "Lift" process, click on the "START" button.

Drive to each logger location and remove the logger from the installation site.

The radio-link of the device may be silent, since "Lift and Shift" loggers are usually set with no Patrol Window. If this is the case, the logger must be swiped to reset it and temporarily activate the radio-link (for around 2 minutes).

The Patroller 4 will pick-up the logger over the radio-link. The app will read the measurement data from the logger and save it in the local database.

The logger is moved into the "non-deployed" list within the app memory. It is removed from the displayed list of remaining devices.

Once all loggers have been found, the list displaying remaining loggers will be empty, and "Devices remaining" will be zero.

Tap "STOP" to stop the "Lift" patrol function.

The measurement data and any sound recordings are added to the local database within the phone's memory. The change of location (removal from installation sites) is stored there also. The data items are tagged as being un-sent.

The app (depending on settings) may request permission from the user to upload the data (sync) after this operation. This is recommended. Otherwise, sync manually later.

The data should be manually synchronised with DataGate at the earliest opportunity from any window containing the sync icon (e.g. The Database window).

Note: Any loggers removed from their installation site should be handled carefully to avoid damage. Refer to guidance in the "Safety Warnings and Approvals Information" document, included with the product.

8.2.3 Removing a Logger from Site (Lift) – With automated sound download

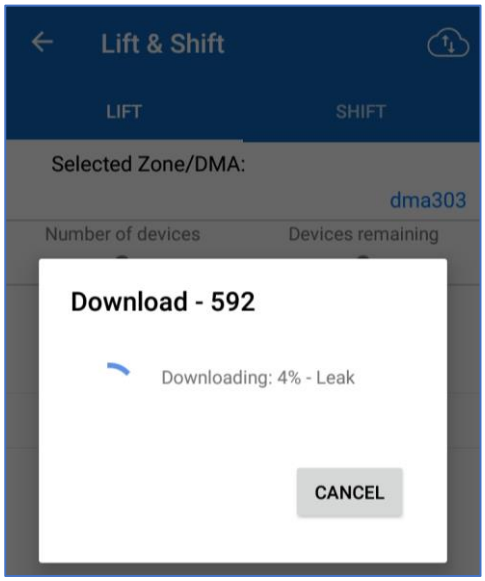
The “Lift” process is now described…
(The case given here is for when options are set that allow automated sound download). (see 8.2.1)

The process begins in a similar way to that earlier described in section 8.2.2.

Note: The evaluation of whether a sound file is to be downloaded occurs immediately after leak data is read from a logger.

- Where the app determines that no sound download is required from the logger, the process is (from the user’s point of view) identical to that described earlier.
- Where the app determines that the logger contains a sound file that it should download, *the earlier described process is* ***extended****, as follows …*

If the app determines that the logger contains a sound file that it should download, it first sets the logger so that the radio comms link is available for a minimum of 6 minutes. Then it begins to download the sound recording.



A progress box appears.

The download (when successful) progresses through each of the following stages: “Available”, “Initialising”, “Synchronising”, “Queued”, “Preparing to download”, “Downloading (x)%”, and finally “Download Finished”.

After successfully completing a sound recording download, the logger leak-state data is recorded in the database, and the deployment site database records the logger as no longer being deployed.

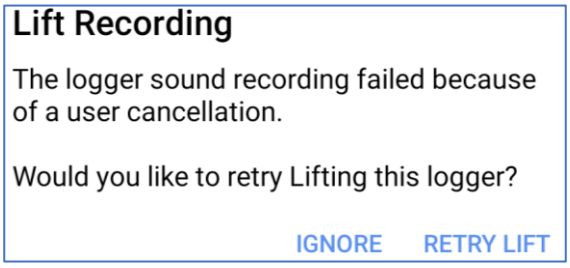
Sometimes the download of the recording does not complete. This can be for a variety of reasons (e.g. The user chose to tap the “Cancel” key, radio interference causing difficulty with the download, excessive time is being taken, the Patroller battery went flat).

For most download failure reasons, the app will try to recover or re-start the download automatically, but If the total download time exceeds 5 minutes, the app will abandon the download attempt. Likewise, the user cancelling the download will halt any attempt to re-start it.

An information (or error) message box will then be displayed.

The message boxes give the user a choice of how they wish to handle the irregularity.

Note: At this point, the logger has stored the leak-status data in the database. There is no sound file within the database.

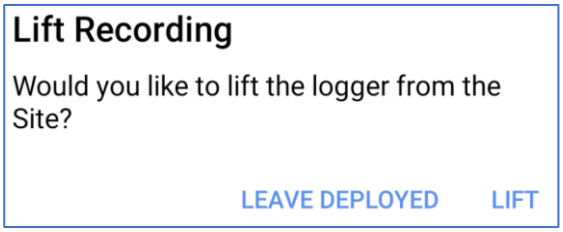


RETRY LIFT:

If the user chooses this option, then the app will clear its memory as if it has never discovered the logger.
The logger will remain on its list of loggers to find.
The app will re-start the process of looking for *any logger* it picks up over the radio link that is on its list of loggers that require to be found and lifted.

IGNORE:

This allows the user to acknowledge that the current to download a sound file from the device has failed. If the user selects this option, a new box appears with further choices required from the user.



LIFT:

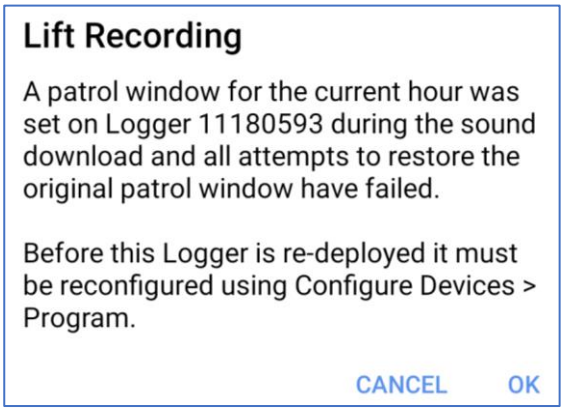
The leak-noise data of the logger is kept in the database, but no attempt is made to obtain the sound file; it is abandoned.
The logger database records the logger as no longer being deployed.

LEAVE DEPLOYED:

This allows the user to ignore this logger during the current Lift process, so the user can continue to try to find the next logger.
No changes are made to the database.
The user can re-install the logger on the site it was removed from (and lift it at a later date). OR …
An alternative is to keep the logger in the van, put to one side, and later in the day begin a second Lift process to complete the lift and data collection from any loggers that remain in the DMA.

There is one more communications failure report to consider …

The message box shown opposite may occur directly after a sound recording was downloaded.



An explanation follows:

When a sound file download option is required, the download can take several minutes to complete.
To reduce the possibility of the radio

communications link going into stand-by, the app:

- Reads the current Patrol Window settings of the logger
  (typically for Lift and Shift they will be set to no Patrol Windows being active).
- Temporarily changes the Patrol Window settings of the logger
  (to avoid the logger going into standby).
- Downloads the sound file.
- Returns the Patrol Window settings in the logger back to what they originally were.

(The process is normally invisible to the user but is only apparent if a fault condition occurs, where the app could not re-store the original Patrol Window settings).

If the problem should occur, it is not a major issue, but the logger will be wasting some battery power. Simply put the logger to one side for manually re-programming its Patrol Window later in the day (see section 10.2).

The above message does not affect any storage of the sound recording or leak-status data; these are still saved to the database.

8.2.4 Caution Point: Trying to simultaneously download multiple loggers.

The app and Patroller only talk with one logger at a time. Downloading a sound file takes over a minute, but the radio-link of a swiped logger is only active for around 2 minutes. It is therefore not possible to download sound files from more than one logger at a time. Additional loggers that are swiped will probably go into standby whilst the first logger is still downloading.

It is recommended that the user downloads data (and any sound file) from one logger whilst driving to site and un-installing the next logger. When the user returns to the vehicle with a newly collected logger, they can check if the previous logger finished download, tap OK, and then reset the new logger to start the next download.

This limitation only applies when download of recordings is enabled in the options.

8.3 LIFT AND SHIFT – SOUND RECORDING DOWNLOAD ISSUES

In case of difficulty in obtaining sound recordings, please be aware of the following…

Logger device issues:

- Only PCorr devices support sound recordings.
  (Check the device is a PCorr, not a Permalog).
- PCorr devices only make automatic sound recordings when they have been programmed to do this.
  (Check the logger settings and re-program if required).
- PCorr devices only make automatic sound recordings when either:
  - They have been recently swiped (to reset them) and they detect (at next evaluation) the site is considered to have a leak near-by.

    - They have been on site for a few days and have detected a new leak.
- PCorr devices do not make new recordings if a protected sound recording exists in the device that has not yet been downloaded. Scheduled sound recordings (see section 11.4) are protected for 24 hours against being over-written by an automatic recording.

9 APP – PATROL

"Patrolling" is the process of collecting the latest leak-status results from loggers.

Where the loggers are to remain installed within their existing sites, a drive-by of each of the installation sites is appropriate, at a modest speed. The app implements collection of the Leak-state data using a window called "Patrol".

Measurements are not meaningful to DataGate unless they were made at a known site. The logger devices must therefore already be deployed at sites (e.g. by using the app "Shift" function for deployment, as described earlier).

If the devices were not already setup by the factory for a patrolled data collection, they should be setup (prior to installing) in a suitable mode of operation using the app (see section 10.2).

They require:

- A suitable radio-link patrol window, to match the time of data collection.
- Measurements are set to be made during a quiet (low usage) period.
- The setting for the automatic sound recording feature of the logger (PCorr only) should be set to the requirements of the user.
    - Enable (set to "yes") if it is required to collect any sound recordings following the drive-by patrol.
    - Disable (set to "no") if this is not required (to save battery power).

In addition:

- The devices being patrolled must exist on DataGate, with permission for the app user to collect data from them.
- The app must have synchronised to DataGate to become aware of its permission to collect data from the logger devices.

Although a logger that is broadcasting its data may be picked-up by a patrol several times, the repeated data is discarded by the app. The app only permits one result (the first obtained) for a logger per site per day.

If the app considers a logger is not installed during a patrol, its measurement data will still be sent to DataGate (but since it is not on a site, DataGate will discard it).

9.1 COLLECTING DATA (PATROL)

From the main window, tap the “Patrol” line.

Tap on “START”.

Initially an empty list is seen.

A summary shows the number of devices picked-up over the radio-link that it has permission to collect data from. It also shows the number of “chirps” (data broadcasts from a logger) that have been picked-up since the patrol was started.

Drive past the installed loggers.

Loggers picked-up as they come into range and are added to the list on the screen.

The Leak status, Level and Spread results are presented in the list, along with time that the logger signal was last picked-up.

Loggers with a status of “leak” are shown in a faint red colour.

Once all the loggers have been found, the user should tap “STOP” to end the patrol activity.

Data is collected from any device (provided the user has permission to use the logger device); It does not matter which DMA contains the site in which the logger is installed.

Synchronisation of the new data with DataGate has to be manually triggered (e.g. from within the “Database” window).

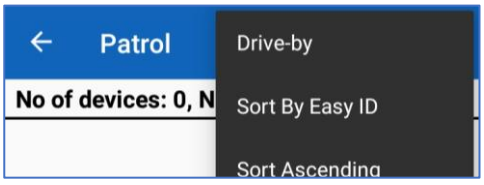
No sound files are downloaded. If they are required, they can be collected by re-visiting the sites in a leak-state and using the “Sound Recording” window (see 11.1).

9.2 COLLECTING DATA (DRIVE-BY PATROL)

An option within the “Patrol” function (described earlier) is to do a “drive-by” patrol.

The option is similar to the regular patrol.

Select “Drive-by” from the local option list.



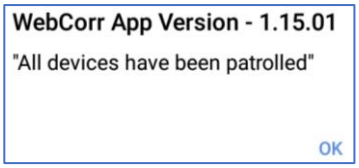
The user is required to select a DMA and then to drive through a route that will pick-up all devices in the DMA.

Select the DMA to patrol.
The Patrol is automatically started.

A list of all the loggers that are on sites within the selected DMA is shown.
The list is divided into 2 sections:

- The top part of the list shows loggers that have not yet been picked-up over the radio-link.
- The bottom part of the list shows loggers that have been picked up, along with the results. Loggers showing a state of leak are highlighted with a coloured background.

When all deployed devices within the DMA have been picked-up on the radio-link, the patrol is stopped automatically, and the user is informed.



The leak-status data from all the devices are stored.

The user can (if desired) select a different DMA and move on to a different patrol route.

9.3 Upload of Patrol Results to DataGate

Patrol data is stored by the app in the phone's memory. After collecting data, the phone must be manually synchronised with DataGate, which uploads all the collected data as part of the synchronisation process.
The synchronisation can be initiated from within the "Database" window.

When DataGate receives the data, it routes it to the correct site, where it appears as follows:

Channel 1 = Leak Status.

Channel 2 = Level.

Channel 3 = Spread.

10 App – Configure Devices (Logger repetitive function)

10.1 Logger Device configuration – Reading

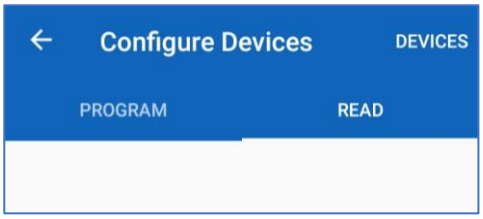
The logger makes daily repetitive measurements of noises within the pipe it is attached to. It activates its radio-link during any patrol windows, and broadcasts short messages (referred to as a “chirp”). Once the app finds a logger that is within radio range, it can obtain other information from it. If the radio-link of the logger is not currently active it can be temporarily activated.

The settings that the logger has can be read as follows:

From the main window, tap on the “Configure Devices” line.

Select the “Read” tab.

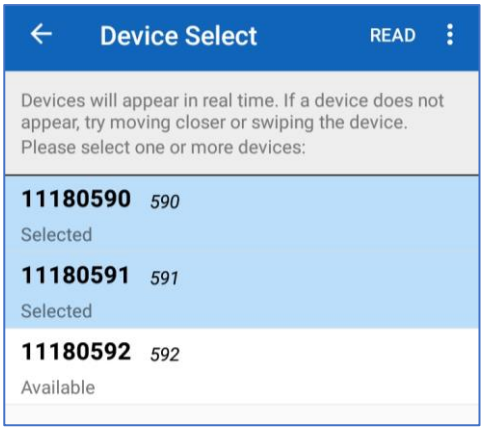
Then tap on the “Devices” button. DEVICES



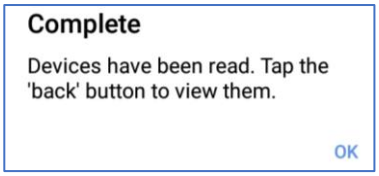
(If the required loggers do not appear in the list, they may be sleeping; Swipe them to cause a reset to wake them up. The radio-link activates for around 2 minutes.)

Select the logger(s) to be read.

Then tap on the “Read” button. READ



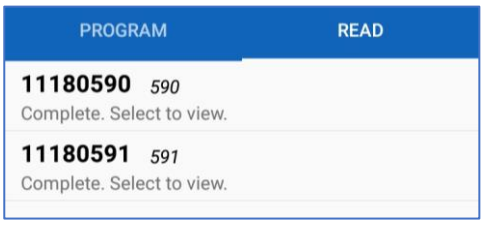
Wait for the logger configuration(s) to be read.



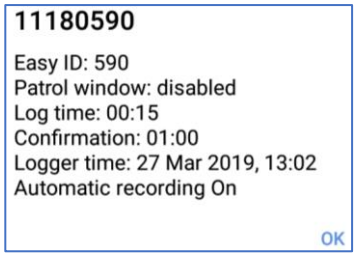
Tap the “back button” (top-left arrow).

A list of loggers that have had their configuration read is shown.

Tap the line of a specific logger to display its setup configuration.



The configuration shows:



- Availability times of the radio-link (Patrol window).
- The time of the day that the leak-detection begins (Log time).
- The time the logger waits before re-running the leak-detection, if it needs to confirm that the leak-state has changed since the previous day (Confirmation).
- The date and time of the clock inside the logger (Logger time).
- The "Automatic Recording" setting.
    - "On" = Make automatic recordings (limited quantity).
    - "Off" = Automatic recordings are never to be made.

10.2 Logger Device configuration – Setting

Note: This step may not be required as the loggers can be set to customer requirements within the factory.

Skip this section if the loggers are already set up.

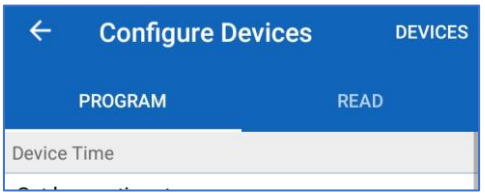
The logger makes daily repetitive measurements of noises within the pipe it is attached to. It then sleeps until it next needs to do some activity. It activates its radio-link during any daily patrol window times, and repeatedly broadcasts the latest data over the radio-link so that it may be picked up during a drive-by patrol.

The logger settings for its daily repetitive program can be re-configured as follows:

From the main window, tap on the "Configure Devices" line.

The "Configure Devices window opens.

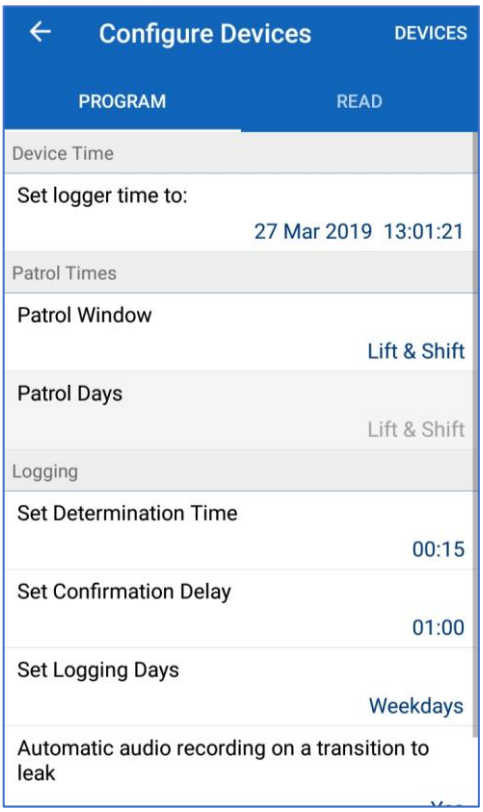
Select the "Program" tab.



Note: This screen **builds a configuration in the phone's memory** that can later be sent to the loggers (when programming them).
When the logger is programmed, all of the listed settings are transferred to the logger. Check each setting before programming the loggers.

The “Set logger time to:” line is automatically set using the phone’s time; It cannot be adjusted by the user.

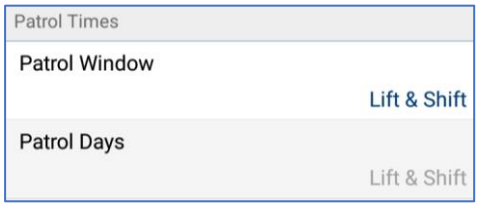
Note: Setting loggers using this screen does not set the clock sufficiently accurately to use any of the sound recordings for correlation purposes; The clock on the mobile phone is not sufficiently precise.



All other settings can be adjusted by the user.

The user can adjust each line to the required setting by tapping on the line and editing the values.

Each setting is discussed briefly…



“Patrol Window” controls the availability of the radio-link.

It can be either set to “Lift & Shift”, a pre-set time window, or a custom time window.

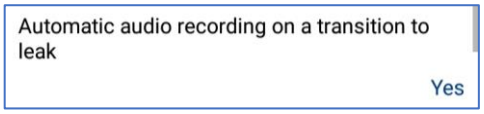
“Lift & Shift” de-activates the patrol window. Other settings are restricted to a maximum of 8 hours per day, to limit battery use. It is also possible to set which days the patrol window is active on. Set the time to the minimum needed (to maximise battery life), but also consider any changes made annually to local time (the logger does not automatically adjust its time for any changes between winter and summer).

“Set Determination Time” controls the start time of the daily leak evaluation; It should be set to a time of low water use to help accurately identify leaks.

The confirmation delay can be set on the following line, which is in case the first assessment is in error due to ambient noise, etc. This is the delay the logger waits before confirming the result whenever it appears that the leak status has changed.

Extend battery life by only evaluating on the days that the data will be collected.

The logger (PCorr+ only) can be programmed to automatically make a sound recording whenever the logger detects a new leak.



Set to “Yes” to enable this feature.

Note: There are some circumstances where the logger will not make an automatic recording... If it has previously made a recording and it has not been collected by the user, the logger will not make any further recordings (making fresh recordings has no merit but uses additional energy). After the user collects the recording, the process of making an automatic recording when next required will resume.

After changing a setting, the new value can be accepted by tapping on the “Set” button.
The new setting will then be copied into the main “Program” screen. Alternatively, the change can be cancelled.

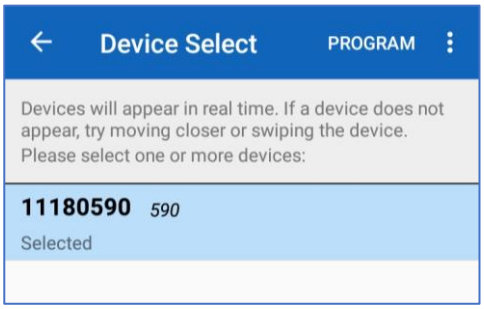
After the “Program” screen has been completed, confirm each listing setting is correct.

Then tap on the “Devices” button. DEVICES

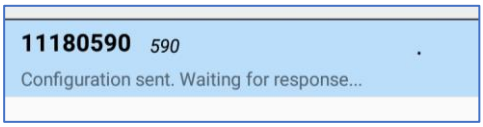
(If the required loggers do not appear in the list, they may be sleeping. Swipe them to cause a reset to wake them up. The radio-link activates for around 2 minutes.)

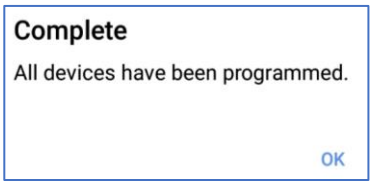
Select the logger(s) to be programmed.

Then tap on the “Program” button. PROGRAM



Wait for the logger(s) to be programmed.





The re-program of the repetitive logging task of the selected loggers is now complete.

*** The logger devices are now ready for installation and use. ***

11 Logger Sound Recordings

PCorr+ Logger devices can contain a sound recording file. This can either be generated:

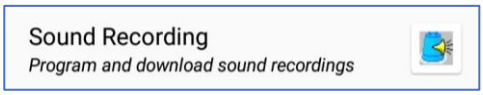
- Automatically when a new leak is detected (depends on logger settings), or
- As a result of a (higher priority) one-time scheduled recording.

The sound file can be manually downloaded by the user.

Note: The app does not distinguish between PCorr+ and Permalog+ devices.
Any programming of sound recordings will be dismissed by Permalog+ devices.

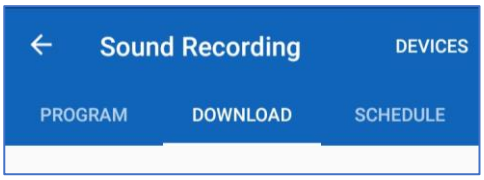
11.1 Manual Download of Sound File

From the main window, tap the “Sound Recording” line.



Select the “DOWNLOAD” tab.

Then tap on the “Devices” button. DEVICES

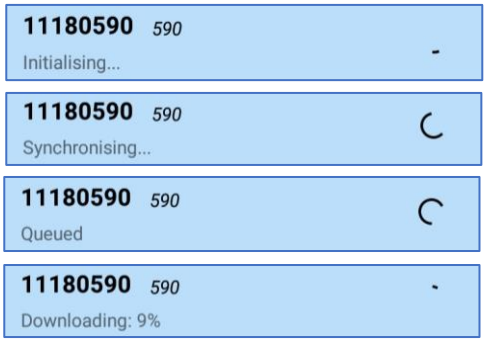


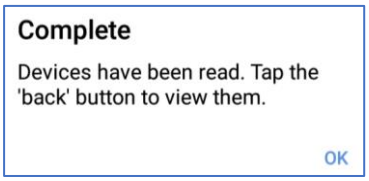
(If the required loggers do not appear in the list, they may be sleeping. Swipe them to cause a reset to wake them up. The radio-link activates for around 2 minutes.)

Select the logger that you wish to download the sound file from.

Then tap on the “Download” button. DOWNLOAD

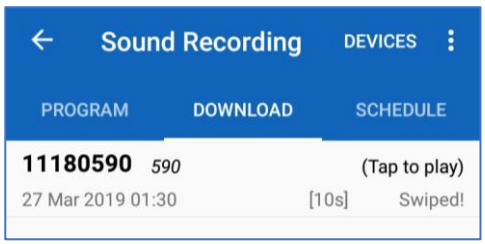
The progress is shown, until the download is complete.





After downloading sound file, the user can listen to it by tapping on the relevant line. Sound is played through the phone’s speaker or headphones (recommended).

The time and length of the recording is shown.



The “Swiped” indicator implies the logger has been reset since it was last configured.

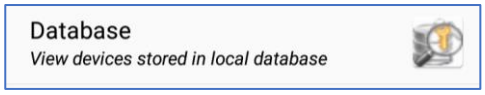
11.2 Automated Download of Sound File (Lift & Shift option)

(Please refer to section 8.2).

11.3 Playing a Sound Recording

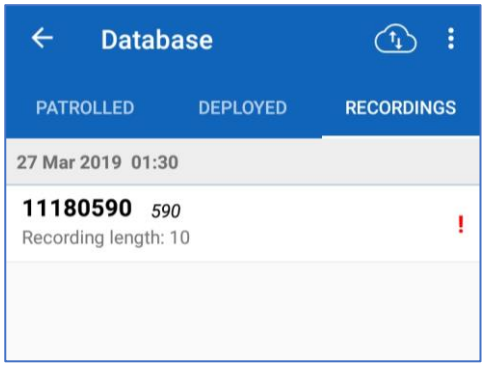
Recordings can be viewed and selected for play-back from the Database view.

From the main screen, select “Database”.



Then select the Recordings tab.

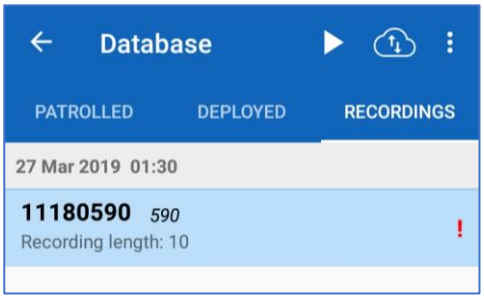
Sound files will be listed along with the date and time at which the sound recording was made.



Tap the line of the recording you wish to listen to.

The line will highlight as selected.

A triangular “playback” control will appear at the top of the screen.
Tap the control to play the audio from the phone.
(The use of headphones is recommended).

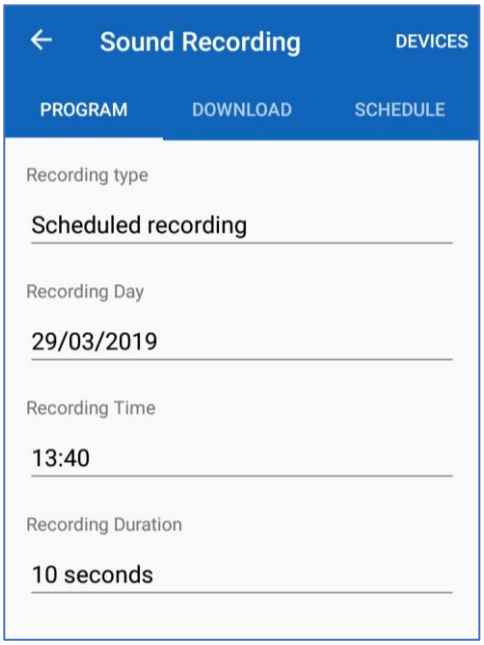


11.4 Manual (Scheduled) Sound Recording

To program a logger to make a sound recording at a set time…

From the main window, tap on the “Sound Recording” line.

Select the “Program” tab.

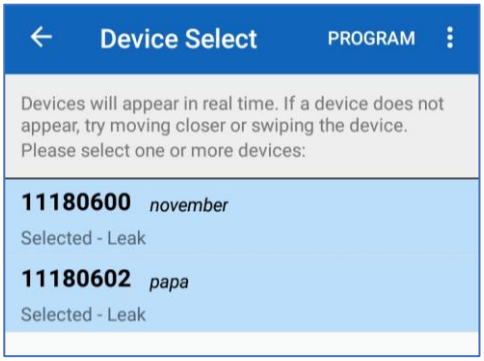


The app supports 2 modes of recordings:

- A “test recording”.
  This is simply a recording to be made several minutes in the future.
  The clock is not adjusted during the setup of this function.
- A “Scheduled recording”.
  This schedules a recording to be made at a fixed time.
  Multiple loggers can be set to record at the same time.
  The clock of each logger is adjusted during the setup of this function.

Set the required logger program by tapping any line that requires change and selecting a new value.

When the program is correctly set, tap the “Devices” control.



Select the loggers that are to be programmed.

Then tap the “Program” control.

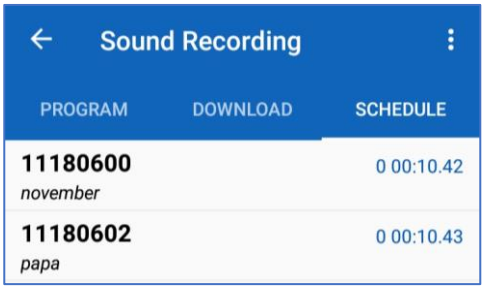
The loggers will be set to make a one-time recording at the specified time.

Note: Whilst the programming is waiting to be run, the regular repetitive logger program is suspended. It resumes after the program is completed.

It is important to download the sound files from the device, as the logger will not over-write the file until it is collected. Failure to do so will prevent the logger from making any automatic recordings.

Selecting the “Schedule” tab displays a count-down of the approximate time left before each sound recording begins.

The sound recording takes around 1 minute to make.



Note: Prior to set-up of a scheduled sound recording, consider whether any changes to the patrol window of the logger(s) are required. If clock accuracy is to be maintained, the sound file of a logger must be collected without a swipe (reset) of the logger. This is particularly important when sound files are being made for Leak Localisation (correlation) purposes.

Note: (At the time of writing, the setting of loggers to produce sound files for correlation purposes is not yet supported by WebCorr app).

11.5 Uploading Sound Recordings to DataGate

All downloaded sound recordings are tagged as unsent data.

Downloaded sound files can be uploaded to DataGate. Due to the size of the files the user may prefer to set the app to wait until the phone is using a wi-fi connection.

Use the “Database” window and tap the control that will start the synchronisation process.

Sound files are time-stamped, so DataGate is able to route the file to the correct site on which they were made.

12 PCorr+ – Leak Localisation / Correlation

(Please contact your sales representative or HWM Customer Support for enquiries or latest information regarding this function).

13 DATAGATE – SETUP FOR USE WITH WEBCORR AND LOGGERS

DataGate must be set to give the User of the WebCorr app permission to use the loggers. An example of how DataGate should be structured is given in section 13.2.

Note: If a logger does not appear on the app it does not imply that the logger is not functioning correctly. Check with your system administrator that the logger is correctly setup on DataGate for use with your user-account.

The initial destination of the logger data is usually the database within the WebCorr app. (Variants of PCorr that are hard-wired to the input of a customer's Automatic Meter Reading system, "AMR" models are a possible exception to this). Whilst it is possible to manage the data exclusively within the phone, as the size of the database grows it becomes more difficult to do so. The data is better managed by uploading it to the DataGate server, where multiple users can access it using a standard web-browser.

13.1 DATAGATE – TERMINOLOGY AND SUMMARY

The DataGate system is provided by HWM. DataGate and PermaNETWeb web-pages are the main viewing portal for logger and site data.

The terminology and an overview of the scheme is summarised here…

PCorr+ and Permalog+ **logger devices** produce several forms of measurement **data**, each of which can be considered as a data **channel**. The data represents a measurement made by a logger deployed on the pipe network. Access to the pipe network is often available through various chambers that house valves or hydrants, connected to the pipes. A chamber can be used as an installation **site** for a logger. A site may be one of many in an area or suburb, with the pipe network interconnecting them. Sites may therefore be collected together in a group, often referred to as a **DMA**. DMAs, in turn may be collected together in a group, referred to as an **account**. Each of these separate entities may be represented on a database, such as one used by the **DataGate** system, which links some of them to a **User** of the system.

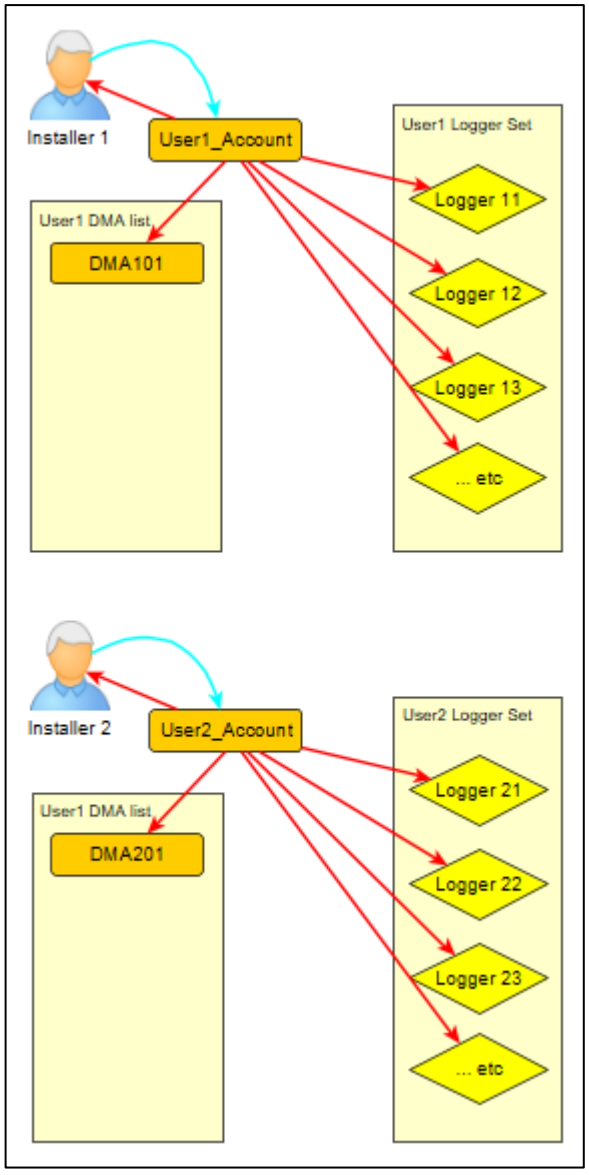
Or, put in reverse order…

- **DataGate** contains a database.
- A **User** of Datagate can be linked with an account.
- An **account** in Datagate can be a group of multiple DMAs.
- Each **DMA** can contain multiple sites.
- Each **site** can have one logger device installed (maximum, at any given time).
- Each **logger device** can produce multiple **channels** of measurement data.
- The **data** of a channel may consist of multiple samples that are obtained at different times.

13.2 DataGate – Example Structure for use

The initial registration of PCorr+ and Permalog+ loggers is normally made by HWM at the time the loggers are shipped from the factory, with guidance of the account manager, who liaises with the customer to find their requirements. The customer will typically have a few installers for the loggers. The loggers are effectively divided into sets, each set being pre-allocated for use by a particular installer.

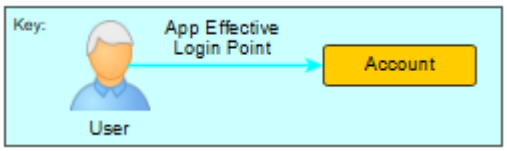
The DataGate system should be set up initially as shown in the following example…



Two users of the WebCorr app are shown opposite.

Each of the system users must have their own account for use. The user must be "owned by" this account (which will, in turn, be owned by a higher-level account in the organisation).

The apps will log-in at this level.



The account is often referred to as the "install account", but here it also doubles as the "owner account".

After log-in, the app can access any DMA immediately below this account level, as long as it is "owned". The illustration shows a DMA (optionally) already created on DataGate, but the WebCorr app can create new ones, as required.

There are several different ways within DataGate to link entities together:

- "Owned by".
  Used to give permission to modify.
- "Deployment".
  Used to pair a logger and a site.

- "Associated".
  Used to give visibility of a site from an account (or, by using multiple associations, from many accounts).

It can be seen from the illustration (above) that each of the loggers allocated for a user are owned by the user's account.

The WebCorr app, when it logs in, has information transferred to it as to which loggers, DMAs, and sites are owned by the user-account. It then, during its operation, keeps track of the logger's installation location. A "sync" with DataGate causes updates to the data-structure shown above. The process is described in section 13.4.

13.3 DataGate – Required User Role permissions

The WebCorr app User must be of a User-type that includes the following DataGate permissions:

- Can Access DataGate.
- Can Create Sites.
- Can Edit Sites.

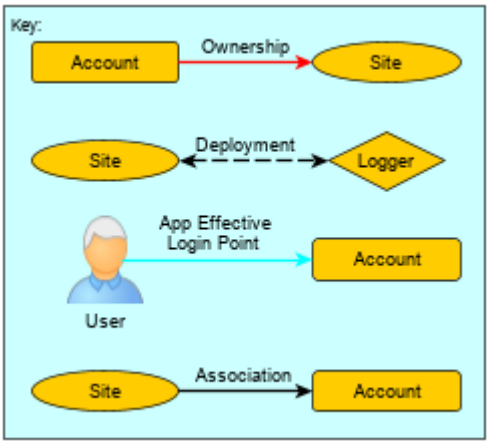
This can be confirmed by your system administrator.

13.4 DataGate – Changes made by the WebCorr app

Note: This information is not required by installers but may be informative for office staff.

This section describes graphically the changes apps make to DataGate.

See opposite for a key of various types of links.



An ownership link can be used to form a tree structure on DataGate. It gives permission to make changes. Sites can be owned by accounts. Accounts can be owned by other accounts (although WebCorr does not support this). Logger devices can be owned by accounts.

A deployment link attaches a logger to a site. (Any data the logger generates and uploads whilst deployed at a site belongs to the site).

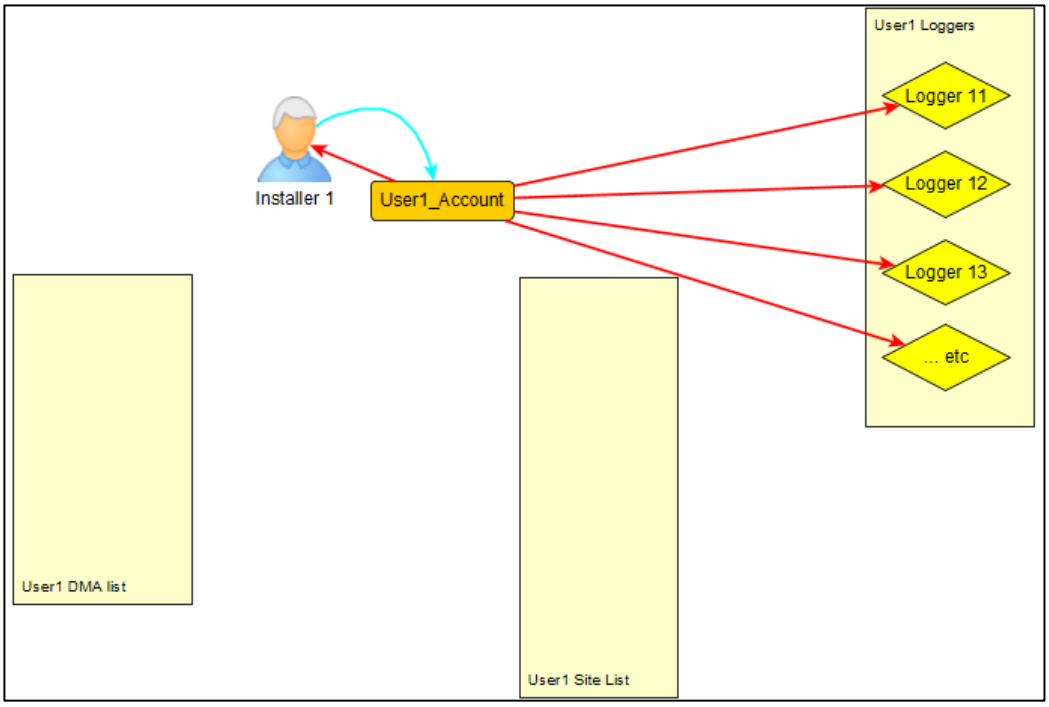
An association link exists between a site and an account. Multiple association links are possible. It is used to give visibility of a site from an account.

A WebCorr user logs into DataGate at the level of the account that owns the user.

Initial State (HWM):

At the time the logger device leaves the HWM factory, it is registered on DataGate by **HWM**, but is not attached to any site.

(Note:
The boxes for DMAs, sites, and loggers are for illustration only. They do not require entry into Datagate).



The app user logs in at this level and has permission to modify everything that is linked by an ownership link.

Initial State (Water Company):

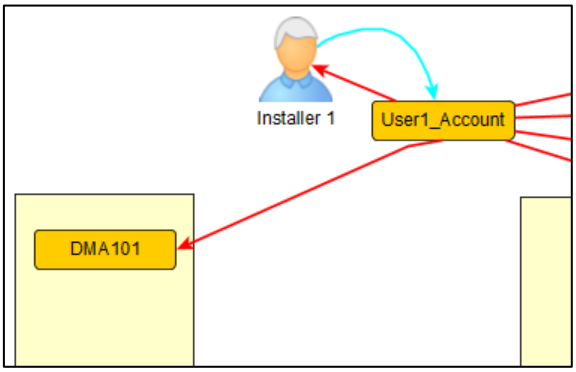
The **Water Company** can optionally accept the structure, above, or add DMAs into the data-structure for the app to use (as shown previously). It is optional, since the WebCorr app can create these, if required.

Irrespective of how they are created, the user's account will "own" all the DMAs that the installer will be deploying the loggers within. Each DMA represents a geographical area of the pipe network to which loggers are to be deployed.

Deployment (Shift) of a logger:

The installer, using the “Shift” functions within the app, chooses a logger for deployment and installs it at a location (site) that gives access to the pipe network. As the app guides the user through the process, details of the site (address, GPS coordinates, etc) are entered. In addition, the site is allocated to a DMA.

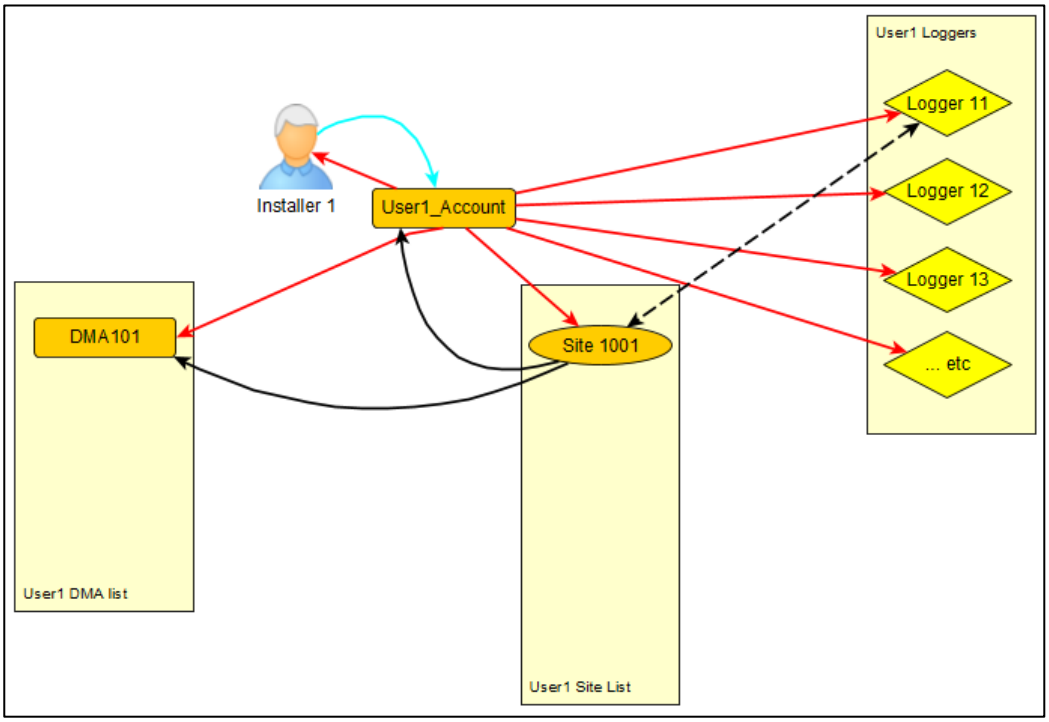
Once the details have been saved, and the location data has synced to DataGate, the following changes are made…



The user may have chosen to create a new DMA. This DMA is stored on DataGate and linked to the owner account by an ownership link.

The new DMA is then added to the list of available DMAs within the app.

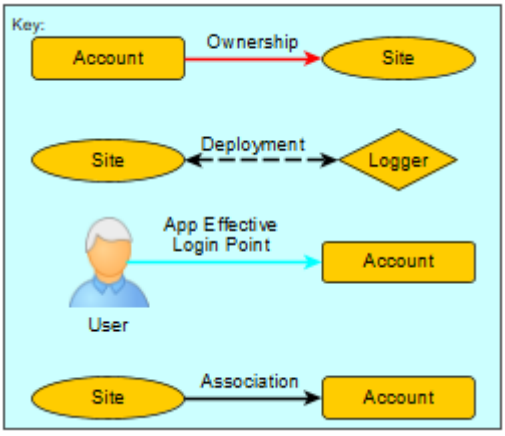
The app creates a new site (unless re-use of an existing site is chosen)



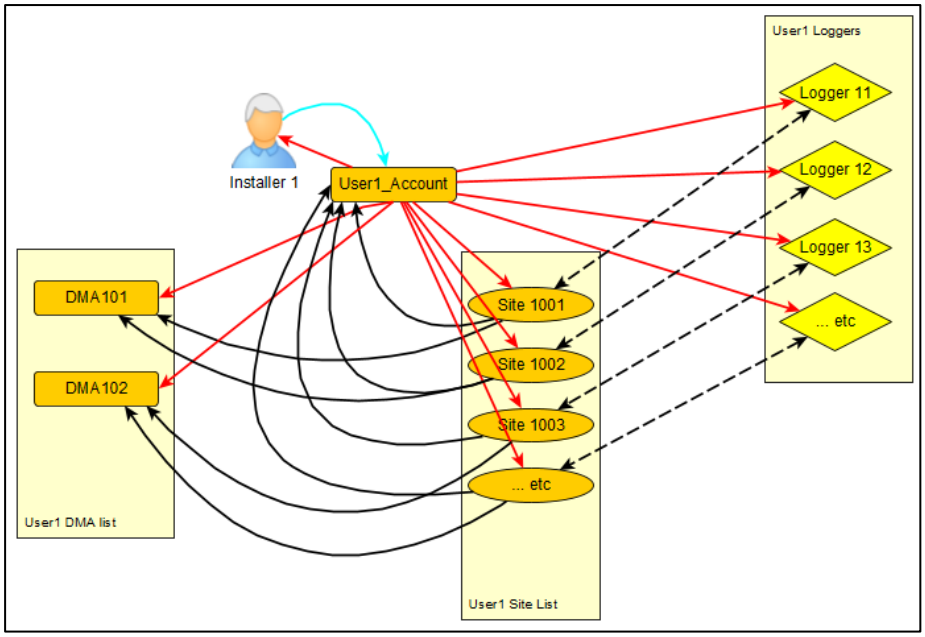
It uses a deployment link to join the logger to the site.

It uses an “associate” link to connect the site to the chosen DMA. It also uses an “associate” link to connect the site to the owner account.

The association links are required to give visibility of the site (and its data) from both accounts.



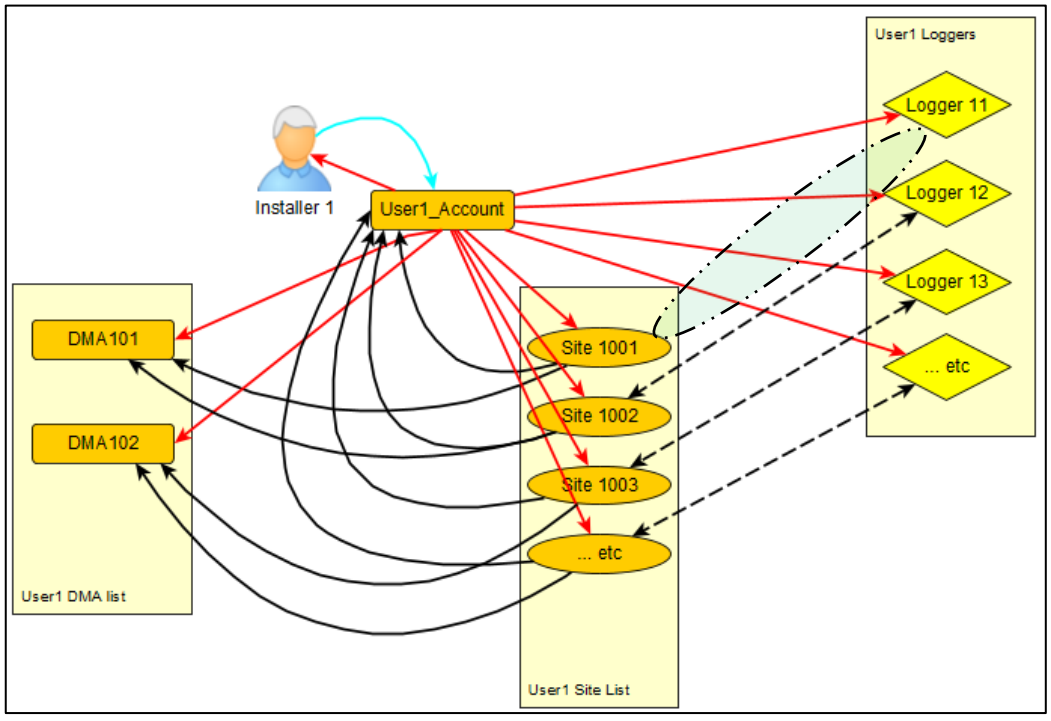
As deployments continue, loggers are linked to sites; sites are allocated to DMAs (according to their general location), and the geographical information is uploaded to DataGate.



DataGate uses this information to link logger measurement data to the correct site, each time the logger sends a new set of measurements, sound recordings, etc. Normally this data is collected using the WebCorr app and is uploaded as part of the sync process.

Removal (Lift) of a logger:

The installer, using the "Lift" functions within the app, visits a site to remove the logger from it. The installer must select a DMA that contains the group of sites that are having the loggers removed. The installer wakes the logger after it has been collected. The app recognises it as one of the loggers being looked for and downloads its final data. Once download has finished, it timestamps the change of location (now no longer on any site).



During a sync, measurement data is initially transferred, then the change of location. Once DataGate has processed the location change, any subsequent measurement data received is not linked to any site since the logger is no longer

deployed. The only link that is removed in the lift process is the deployment link; sites remain associated to (visible from) the accounts to which they were first associated.

Note: At the time of writing, although a logger can be deployed to an existing site, the app will not support a clean transfer of the site to another DMA; the site will exist in both old and new DMAs.

14 TROUBLESHOOTING

Many potential problems can be avoided by the app user following two simple rules:

- Synchronise with DataGate frequently.
- Do not swap from one phone to another.

14.1 LOGGER DEVICE DOES NOT GET LISTED IN THE APP

Check for:

- Ensure you are logged into the WebCorr app.
- Sync to confirm the app has latest data from DataGate.
- Contact your system administrator and confirm your user-account has ownership of the logger. Details are given in section 13.
- The logger may be out of range of the radio.
- Confirm the battery of the logger device is not dead: The LED should give a short flash every few seconds (a visual indication of leak state).
- Confirm the logger and Patroller are using the same frequency (check label details).
- Confirm the logger has the radio link active – Swipe the logger with a magnet to cause the communications link to temporarily re-activate.
- Check logger patrol-window settings are set to the required time of making patrols.

14.2 ERROR MESSAGE DURING LIFT OR SHIFT

The app may display an error message during lift and shift…
“Error during Transmission. User does not have permission to edit accounts”.

DataGate allows creation of users with different roles. The above error can be caused by the app user logging into the account with a username that has a role (user-type) without the correct permissions. Refer to section 13.3.

14.3 Sound file will not upload to DataGate, and displays "E".

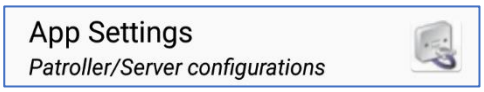
This issue is caused by a sound recording timestamp indicates it was made at a time which DataGate does not consider the PCorr+ was actually deployed to a site.
(e.g. A sound recording made whilst the logger was being stored).

- If the user agrees that the logger was not deployed to a site when the recording was made, they can regard the indication as being for information only.
- If the user considers that the logger was deployed at a site when the recording was made, the deployment of the logger to that site should be repeated.

14.4 App – Deletion of Database

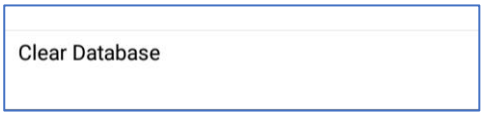
If it is ever required to delete the app database (e.g. At the request of HWM due to some technical problem), use the following steps:

Tap on "App Settings".



Tap on "Clear Database".

Confirm the request to clear.



14.5 Phone – Memory Full (*Android phone*)

The phone database contains measurement and logger location data. Measurement and logger location data that are more than 3 months old are automatically deleted by the app. The app checks whether it needs to purge any data every time it starts.

Sound recordings are never purged and must be deleted manually by the user, by the following process:

- This process requires someone who is competent at using File Manager on a PC. If in doubt about the process, ask your supervisor or a computer specialist.
- The phone should be synchronised with DataGate before considering removing any sound data manually. Then close the WebCorr app.
- Plug your phone into a PC (running on Microsoft Windows10).
- Activate the phone (e.g. enter your PIN) and allow the PC to have access to its contents.
- Launch Windows "File Explorer" and find your phone device, listed under "This PC\". Navigate to the following folder:
  This PC\[YourAndroidPhone] \Phone\HWM_WebCorr_App
- Sound recordings are stored in both *.wav and *.ssr formats.
- Order the files according to date.
- Delete any *.wav and *.ssr files that are more than 3 months old.

14.6 PHONE – MEMORY FULL (*APPLE IPHONE*)

The phone database contains measurement and logger location data. Measurement and logger location data which are more than 3 months old are automatically deleted by the app. The app checks whether it needs to purge any data every time it starts.

Sound recordings are never purged, and no facility exists to remove them (they are not user-accessible), except for the process of deleting the app and its data from the phone and re-installing.

- Ideally: Lift all logger devices from their sites.
- Ensure the phone is Synced to Datagate.
- Confirm all measurements, recordings and deployment details have been sent by the phone, and that none are pending.
- Delete the WebCorr app and its data from the phone (see section 14.8.4).
- Re-install the app.
- Expect some data-loss during the first lift and shift of each logger as the app and DataGate re-sync.
- Data loss may occur when collecting data from any deployed logger (the app does not know when the deployment was started). It is recommended that any deployed loggers be lifted from and shifted back to the same site in order to repeat the measurement. Non-deployed loggers should not have any issues.

14.7 HOW SHOULD I HANDLE A PHONE UPGRADE?

It is important that only one phone is driving the update of DataGate with logger deployment and measurement information.

When upgrading to a newer phone:

- Ideally: Lift all logger devices from their sites.
- Sync the old phone prior to the upgrade.
- Confirm all measurements, recordings and deployment details have been sent by the phone, and that none are pending.
- Delete the app and all of its data from the old phone (see section 14.8.3 for Android phones or 14.8.4 for iPhones).
- Install the app on the new phone.
- Start the app on the new phone and proceed until a synchronisation has been completed. The new phone is now ready for use.
- Due to the disruption of synchronisation, it may be required to lift and shift each logger from and to its current site in order to complete the re-synchronisation process.

14.8 HOW SHOULD I HANDLE A LOST PHONE?

It is important that only one phone is driving the update of DataGate with logger deployment and measurement information. Each time the user changes to a new phone, there is the potential to lose data or produce garbage data (e.g. data being

linked to the wrong site). The most effective solution is usually to spend time to locate the missing phone.

There are several possible scenarios regarding the lost phone:

- The phone was synchronised prior to being lost.
- The phone was not synchronised prior to being lost.

14.8.1 Old phone was synchronised

If the phone was lost after it was synchronised, the replacement phone can be handled similar to a phone upgrade (see section 14.7). Data loss may occur when collecting data from any deployed logger (the app does not know when the deployment was started). It is recommended that any deployed loggers be lifted from and shifted back to the same site using the new phone to repeat the measurement. Non-deployed loggers should not have any issues.

If the old phone is found:

- The app should not be re-activated (synchronisation with DataGate could cause issues within the app and also DataGate).
- Delete the app and all of its data from the old phone (see section 14.8.3 for Android phones or 14.8.4 for iPhones).

14.8.2 Old phone was not synchronised

If a misplaced phone becomes lost with unsynchronised data, the data should be treated as lost forever. Expect loss of data as DataGate and the phone go through the re-synchronisation process. The replacement phone will be obtaining its starting position from DataGate. DataGate will initially give a misleading picture of where the devices are deployed. Initial data from the app may therefore be routed to the wrong site. Following the first lift and shift cycle with the new phone things will settle down and be OK going forwards, since the new phone is now driving any deployments. It is recommended to re-deploy the loggers to the sites they were physically on soon after the new phone is employed and obtain fresh data. Similarly, re-deploy them to the sites that DataGate considered that they were located at the time the new phone was deployed and obtain fresh data.

If the old phone is found:

- The app should not be re-activated (synchronisation with DataGate could cause issues within the app and also DataGate).
- Delete the app and all of its data from the old phone (see section 14.8.3 for Android phones or 14.8.4 for iPhones).

14.8.3 Deleting the app and logger data from an android phone

- Go to Play store and find the WebCorr app.
- Select the “Uninstall” option.
- The app (and user inaccessible data) will be deleted from the phone.

- User-accessible data (e.g. sound recordings) must be deleted manually by the user, by the following process:
    - This process requires someone who is competent at using File Manager on a PC. If in doubt about the process, ask your supervisor or computer specialist.
    - Plug your phone into a PC (running on Microsoft Windows10)
    - Activate the phone (e.g. enter your PIN) and allow the PC to have access to its contents.
    - Launch "File Explorer" and find your phone device listed under "This PC\". Navigate to the following folder:
    - This PC\[YourAndroidPhone]\Phone\HWM_WebCorr_App
    - Delete all files within this folder.
    - Delete the HWM_WebCorr_App folder.

14.8.4 Deleting the app and logger data from an Apple iOS phone

- Hold your finger for 3 seconds over the WebCorr app icon on the home screen. After a few seconds the icons of deleteable apps will begin to "shake" (small left and right rotations), and an "X" will appear in the corner of each icon.
- Tap the "X" on the WebCorr app.
- A box will pop-up asking if you wish to delete the app (with Cancel or Delete option buttons).
- Select "Delete". The WebCorr App, its database and all sound files will be deleted.

14.9 FIRMWARE UPGRADE

(At the time of writing, upload of new firmware to the Patroller and logger devices is not yet supported by the HWM WebCorr app. Please contact your sales representative or HWM Customer Support for latest information or to obtain guidance as to how the upgrade can be done).

HWM-Water Ltd
Ty Coch House
Llantarnam Park Way
Cwmbran
NP44 3AW
United Kingdom
+44 (0)1633 489479
www.hwmglobal.com