



## User Guide: PermaNET SU Installation and Setup (Using HWM IDT).



**Warning:**



This manual contains important safety and operating information. Please read, understand and follow the instructions in the manual and also the safety / approvals document shipped with the device.

## TABLE OF CONTENTS

1	Introduction, Background and Support of Product.....	5
1.1	Safety .....	5
1.2	Background .....	5
1.3	Logger - Unpacking.....	5
1.4	Support of Product .....	6
2	Overview and preparation for use.....	7
2.1	Logger - Device Overview .....	7
2.1.1	Measurement data types.....	7
2.1.2	Battery / life-time.....	7
2.1.3	Cellular communications and SIM-card.....	7
2.1.4	Communications with the mobile phone (or similar device).....	8
2.1.5	Logger operation - Repetitive functions .....	8
2.2	System Overview.....	9
2.3	Mobile Phone (or similar device) .....	10
2.3.1	Specification.....	10
2.3.2	Installing the HWM software (Android version).....	10
2.4	Loggers – Secure vs Insecure .....	11
2.5	DataGate.....	11
2.5.1	DataGate – Giving the App access to use Loggers.....	11
2.5.2	DataGate – Terminology and Summary .....	12
2.6	Logger Measurement Data – Destination and Use.....	12
2.7	Ways to set the Logger Configuration.....	13
2.8	IDT – Test of logger within an installation.....	13
2.9	Overview of the deployment process .....	13
3	Antenna Options and Installation Guidelines.....	16
3.1	Antenna Options.....	16
3.1.1	Monopole .....	16
3.1.2	T-Bar .....	17
3.1.3	Button.....	18
3.1.4	Cone Antenna .....	20
3.1.5	Magnetic Dipole Antenna .....	21
3.2	Installation Guidelines.....	21
3.3	Installation Process Decision Tree.....	22

4	Waking the Logger and Communications Link .....	23
5	IDT app – Logging in and use .....	24
5.1	Use of IDT without Logging in .....	24
5.2	Logging in and initial actions .....	24
5.3	IDT app - Selecting a PermaNET SU.....	26
5.3.1	Automatic Selection using barcode scan.....	26
5.3.2	Manual Selection using Bluetooth scan.....	27
5.4	IDT – Update Logger Firmware .....	28
5.5	IDT – Device Options – Configure, Test or Deploy .....	28
5.6	IDT – Configure Device menu. ....	29
5.6.1	IDT – Logger device - Device Information.....	29
5.6.2	IDT – Logger device - Call Settings.....	31
5.7	IDT – Test Device menu .....	32
5.7.1	IDT – Logger device - Sensor Test (Audio Noise Level) .....	32
6	Positioning and Installing the Antenna .....	33
6.1	IDT – Signal Test (mobile network signal strength - CSQ).....	33
6.2	IDT – Call Test (logger to server) .....	34
6.3	Troubleshooting a Call Test failure.....	35
6.3.1	Possible Issues and Checks .....	35
6.3.2	Antenna - Installation considerations.....	36
6.3.3	General Considerations .....	36
7	IDT – Deploy Device.....	38
7.1	HWM Deployment App – Logging in and initial actions.....	38
7.2	HWM Deployment App – Completing site details .....	40
7.3	HWM Deployment App – Synchronisation.....	43
8	DataGate – Setup for use & Changes made by apps .....	44
8.1	DataGate – Example Structure for use.....	44
8.2	DataGate – Required User Role permissions .....	45
8.3	DataGate – Changes made by HWM apps .....	45
9	DataGate – Remote programming of a Logger.....	50
9.1	Overview of operation.....	50
9.2	Automatic and Scheduled sound recordings .....	50
9.3	Alarms and Fault conditions .....	53
9.3.1	Channel alarms.....	53
9.3.2	System Alarms .....	54

9.3.3	Pipe Leak detected .....	54
9.3.4	Logger fails to call-in with data.....	54
10	Removal of a logger from a site .....	55
11	Service and Repair .....	57
12	Troubleshooting .....	58
12.1	The User cannot log in.....	58
12.2	The IDT app does not list the logger .....	58
12.3	The data from the logger does not appear on DataGate. ....	58

---

# 1 INTRODUCTION, BACKGROUND AND SUPPORT OF PRODUCT

---

Thank you for choosing an HWM data device. We trust it will provide you with many years of service. This user guide covers PermaNET SU models (SU/L/\*/\*).

## 1.1 SAFETY

Before continuing, carefully read and follow the information in the “**Safety Warnings and Approvals Information**” document, supplied with the product.



### IMPORTANT SAFETY WARNING:

This equipment uses a high strength magnet and should not be carried by or be placed in the proximity of anyone with a **heart pacemaker**.

The magnet can permanently corrupt magnetic storage media such as floppy discs, hard discs and tapes etc... It can also damage TV and PC monitor screens and some watches.

Retain all documents for future reference.

## 1.2 BACKGROUND

Pipeline leaks are a constant burden to water industries, which can affect the efficiency of the individual company's performance. Leakage loss reduces the amount of fluid actually being delivered, thus affecting the financial side of the business. The longer the leak is left, the larger the economic, and potentially environmental, consequences. It is therefore more beneficial and safer to detect a leak early and make repairs to the pipes before significant damage to the business is caused.

At HWM, we pride ourselves in designing the best leak detection equipment at an affordable price for the benefit of the water and gas companies.

## 1.3 LOGGER - UNPACKING

As you unpack your new logger, please confirm that you have the following parts:

- PermaNET SU data logger.
- Antenna (for direct attachment or cabled attachment).
- (Optional) Antenna extension cable.
- (Optional) Antenna mounting bracket / hook.
- (Optional) Magnet tool.
- Safety Warnings and Approvals Information.

If there are any omissions, please contact our sales team to rectify or supply the missing parts. Please dispose of your waste packaging responsibly.

## 1.4 SUPPORT OF PRODUCT

This user-guide covers the PermaNET SU product family of leak detection equipment.

The device (which will be referred to as a “logger” throughout this manual) is used in conjunction with a mobile-phone software application called “IDT”. IDT is used to assist the user to test and deploy the loggers.

This user-guide provides a brief description of the PermaNET SU functionality. It also covers the use of the IDT app. It includes the setup (registration) of the logger within DataGate, as this can be a requirement for the IDT app to correctly function with the loggers you own.

Note: The screen contents, icons and functionality may change from time to time, due to ongoing development and improvements, so may appear different in the version of the IDT you have installed. Screen resolution differences can also cause changes. IDT can run on mobile phones and other devices with an Android operating system, such as tablets. (An Apple iOS version is also being developed).

HWM also provides support of the product by means of a web-page:

<https://www.hwmglobal.com/permanet-su-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](mailto:cservice@hwm-water.com)

## 2 OVERVIEW AND PREPARATION FOR USE

---

### 2.1 LOGGER - DEVICE OVERVIEW

Note: The loggers have standard settings for operation programmed into them prior to shipping from the factory, with some variations according to customer requirements.

Your logger(s) may therefore differ slightly from the descriptions that follow.

The PermaNET SU product family are logger devices with an integrated Leak Noise Sensor, built by HWM. They are of a waterproof construction, being designed to be permanently installed around a water network, listening for leaking pipes. The devices accomplish this by means of a specialised microphone that can detect the sounds emitted from a leak. A micro-controller, built into the unit, measures the noise level once per day and performs a statistical analysis to generate data for a “noise histogram”. A leak-state judgement is made, along with two additional results called “level” and “spread”. The results are saved in memory, for upload at a later time.

#### 2.1.1 Measurement data types

The saved data could be in the form of:

- A “noise histogram”.  
This provides a detailed indication of how consistent the noise measurement is, and can be used for more advanced analysis. Histograms can also help to visualise the noise into patterns that can be identified as leaks.
- A Level / Spread indication.  
These two figures are a numeric summary of the noise histogram.  
The “Level” figure represents the sound level that occurs most often during the sample period.  
The “Spread” figure is how much the sound level varies during this time.  
(A large consistent Level and small Spread is typical of a leak, whereas a small Level and large Spread is typical of background noise within a pipe).
- A “leak / no leak” status.  
This gives a simple indication of whether results indicate a probable leak.
- Sound recording files.

#### 2.1.2 Battery / lifetime

The logger is powered by non-rechargeable Lithium batteries. The logger is designed to minimise the battery use and thus increase the life expectancy of the unit (e.g. the loggers become active when needed; most of the time they are in standby). The battery life is also affected by user-programable settings.

#### 2.1.3 Cellular communications and SIM-card

The PermaNET SU logger includes an interface to the cellular communications network, which provides access to the internet. The data stored within the loggers can be sent

automatically over internet using the mobile communications network. The normal destination of the data is the HWM DataGate server.

Communication is 2-way between the logger and server, by means of a proprietary protocol using UDP packets sent to the internet using the cellular communications network.

A SIM card is fitted within the logger.

#### **2.1.4 Communications with the mobile phone (or similar device)**

The logger includes a Bluetooth-compatible interface, used for short-range communication to other Bluetooth-compatible devices (e.g. a mobile phone). This enables the user to communicate with the logger during installation and make on-site tests.

#### **2.1.5 Logger operation - Repetitive functions**

The PermaNET SU is shipped from the factory in a minimally active state, to extend battery life whilst in storage (e.g. no measurements are made or logged). This mode is designed for periods of storage or shipping of the device, with the logger referred to as being in “shipping mode”, or “sleeping”. Once activated (see section 4), the logger no longer sleeps, but begins its repetitive daily tasks. Whenever possible it saves power by putting circuits it does not currently need into “standby” (e.g. radio circuits).

The logger will become highly active at the time it is required to make measurements, complete its leak evaluation and store the results as a set of data within its memory. The logger will then go into standby until the next programmed event.

When it is time to upload the data over the mobile network, the logger switches on its cellular radio circuits and sends its data. Once completed, it puts them back into standby mode.

The logger occasionally checks if a user wishes to communicate with it; If so, it activates its Bluetooth-compatible communications link. This link remains open for communication for 2 minutes, waiting for instructions. If there is no interaction from the user during this time, the logger puts the communications link back into standby. If the user begins using the link, the logger completes any tasks the user gives to it, and keeps the link open for 10 minutes after it was last used.

The logger’s primary task is a leak-sensing program, which runs once daily. The Leak-state evaluation program takes place between 2-4am (although it can be changed). Typically, it is made during a time of low water use to reduce the possibility of consumer water use being incorrectly judged as a leak. During this time, if the logger determines a change of leak-state, it carries out a secondary confirmation evaluation.

If the logger determines that a new leak is likely to be present near-by, it can (if so set) automatically make a sound recording when the new leak is detected. The sound recording is by default 10 seconds in duration.

Note: Making and transmitting sound recordings can use a lot of data and also drain the battery significantly if too many are made. In order to preserve battery life



and reduce data costs, the recording system is restricted to 7 recordings a month. If you have a specific requirement for more than this limit, then please contact HWM customer service for assistance.

## 2.2 SYSTEM OVERVIEW

The loggers form only a part of a functioning system. A typical system will comprise of:

- A set of PermaNET SU loggers.  
These are set to evaluate the sounds within a pipe overnight, when water use is minimal, to determine if a leak could be present nearby.
  - A mobile device (with HWM software installed).  
The mobile device provides a Graphical User Interface to the user, for access to the loggers and on-line server.
  - HWM application software (installed on the mobile device).
    - “IDT” software:  
Used to put the logger into various modes in order to test it within an installation.  
At the time of writing, IDT interacts with the “HWM deployment app” software; this must also be installed.
    - “Deployment App” software:  
Used by IDT to record the location of the site at which the logger was deployed.
  - Required for apps:
    - An internet connection (via the mobile network),
    - A User-account and password for the HWM DataGate system.  
(required for the app to function and access the HWM database).
- Note: Under certain conditions the above may not be required for the IDT app (see section 2.4).
- Note: The term “DataGate” will be used throughout this manual.  
An alternative name may be used by the server in your location.

Note: Do not use the Windows-based version of IDT as it is not compatible with PermaNET SU.

## 2.3 MOBILE PHONE (OR SIMILAR DEVICE)

### 2.3.1 Specification

The HWM IDT app used for PermaNET SU is available on Android-based mobile devices.

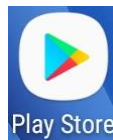
Minimum specification of device:

Android:	Android version 5 (Lollipop) minimum. Must have Bluetooth-Low-Energy (BLE) compatibility, GPS and Internet capability. Memory (for application): 60MB Memory (for data): (varies according to use).
----------	--

### 2.3.2 Installing the HWM software (Android version)

The mobile device must be prepared for use with PermaNET SU loggers by installing the HWM “IDT” mobile phone app.

On your Android device, open the “Play-Store” application.



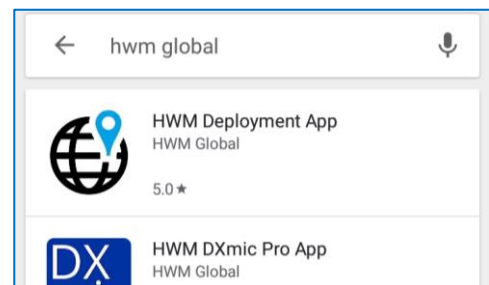
Search for “HWM global”.

A list of available HWM applications will be shown.

Select “IDT” and install it.

Once installed, an “IDT” icon will appear on the phone.

“IDT” is the “Installation and Diagnostic Tool” for PermaNET SU.



**Note:** The IDT app employs the use of the “HWM Deployment App” for deployment functions, so this must also be installed.

On your Android device, open the “Play-Store” application, as detailed above.

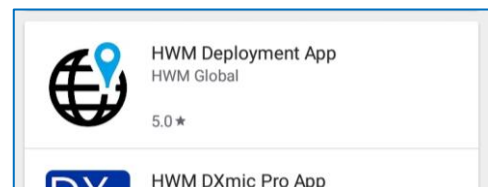
Search for “HWM global”.

A list of available HWM applications will be shown.

Select “HWM Deployment App” and install it.

Once installed, an “HWM Deployment App” icon will appear on the phone.

**Note:** The HWM Deployment app is only briefly described in this user-guide. Further information can be found in the user-guide for the Deployment app.



## 2.4 LOGGERS – SECURE VS INSECURE

Each logger has an internal setting that can be set to either “Secure” or “Insecure” mode. “Secure” mode restricts (DataGate) unauthorised users from making changes to the logger settings and or logged data. “Insecure” mode allows a logger to be used without the (DataGate) authorisation requirement. A brief introduction to the two modes is given here.

At the time of leaving the factory, the loggers will be pre-configured to the requirements of the customer, including security settings. The loggers can communicate their security requirements to the IDT app. This manual will refer to a logger as being either a “secure” or “insecure” logger.

Secure loggers:

- Must be correctly registered on the DataGate server with appropriate ownership settings.
- Require the IDT user to successfully authenticate with the server (periodically).
- Block connections from unauthorised IDT users.

Insecure loggers:

- Do not require registration on the DataGate server to be used with IDT.
- Can be connected to and modified by anyone with the IDT app.
- Allow the use of the loggers with alternative (non-DataGate) software for data storage and display.

## 2.5 DATAGATE

Loggers set as “secure” require DataGate to operate. Loggers set as “Insecure” can (optionally) operate without DataGate, or use an alternative server.

### 2.5.1 DataGate – Giving the App access to use Loggers

All *secure* PermaNET SU loggers must be correctly registered on DataGate in order for IDT to use them. The IDT app will only allow access to *secure* loggers that the user has permission to use; it also allows access to any insecure logger. Similarly, the Deployment app will only allow access to a logger (secure or insecure) if it is correctly registered on DataGate.

DataGate must be set to give the User of the app permission to use the loggers. An example of how DataGate should be structured is given in section 8.1.

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.

### 2.5.2 DataGate – Terminology and Summary

This section *introduces the terminology* that is used by both DataGate and the apps...

The destination of all PermaNET SU logger data is the DataGate system, provided by HWM. DataGate and PermaNETWeb web-pages are the main viewing portal for logger and site data.

An overview of the scheme is summarised here...

PermaNET SU **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 District Metered Area (**DMA**). DMAs, in turn may be collected together in a group, referred to as an **account** (or Zone). 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** can be a group of multiple DMAs.
- Each **DMA** can contain multiple sites.
- Each **site** can have one logger device installed at any given time (or none).
- 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.

Details of initial setup of DataGate are provided (mainly for office staff) in section 8.

## 2.6 LOGGER MEASUREMENT DATA – DESTINATION AND USE

The loggers and the DataGate system together form a powerful leak detection system. The data produced by each logger is uploaded to DataGate. DataGate links the measurement data of each logger to the correct site.

DataGate web pages are mainly used for administration and setup. PermaNETWeb web pages are mainly used for displaying sites, along with the measurement data provided by the logger. The primary use within PermaNETWeb is to present loggers on a map display, highlighting loggers that show possible pipe leaks.

When available, sound recording files can be used to confirm whether the sound within a pipe does resemble the sound produced by a leak. Additionally, if several sites in the area have loggers that have produced sound recordings at precisely the same time, the approximate location of the suspect leak can often be found, using a process called Leak Localisation / Correlation.

**Note: Always use a ground microphone to confirm a leak location prior to commencing repair works.**

## **2.7 WAYS TO SET THE LOGGER CONFIGURATION**

The PermaNET SU holds many setting parameters that affect its operation (see 2.1).

Example settings are:

- When to make the Leak detection.
- Whether to automatically make a sound recording of a suspected leak.
- Scheduled measurements.
- When to call-in with the data.
- Mobile-network settings (e.g. telephone number, network to use).

The logger settings can be adjusted at various times...

- Initial settings are made within the factory, prior to shipping. Default settings are used, plus some settings being customer-defined. These will be suitable for most installations.
- The IDT app gives the user access to adjust some settings. The user has to be near the logger to make the changes over the Bluetooth link.
- After installation, some additional settings can be modified remotely, via the unit receiving commands from the DataGate system.

## **2.8 IDT – TEST OF LOGGER WITHIN AN INSTALLATION**

The user of the IDT app can instruct the logger to do various maintenance tasks, such as communications tests. This is particularly useful when done on-site since communications are affected by the (often below-ground) location of installation, local signal strength of the mobile network and the radio leakage properties of the chamber. ... The IDT app can help to find the best position for an antenna.

Note: IDT communicates with the logger over a Bluetooth-compatible radio link. When the lid is on the chamber, this radio link is also adversely affected. Hold the phone near the lid to improve the signal strength, or else the radio link could be dropped.

## **2.9 OVERVIEW OF THE DEPLOYMENT PROCESS**

The deployment process depends on the strategy employed by the water company. There are two approaches:

- Deploy each logger to a site, with checks of functionality being made during each installation. This confirms the logger performs OK in its installed position.
- Deploy the loggers to sites without any checks being made (i.e. skip some of the steps listed as optional). A follow-up team is then sent to selected sites to improve those that have communication problems.

Installation consists of several steps...

- Installation sites must be selected.
- Equipment must be available at the installation site to complete the installation. This will include an antenna. (A guide for the installation of the logger and antenna choices is given later – see sections 3 and 6). It is possible that several antenna configurations may need to be tried in order to get a good result. It is useful to have a variety of antenna types to try.
- The user logs into IDT and synchronises with DataGate. This downloads information regarding which loggers it has permission to use, and what sites are already in existence.
- At site, a logger is selected for installation. The surface to which it will be attached is prepared to ensure good contact. The surface must be flat so it makes good contact; Sound will be picked up and also the logger will be secure from falling off.
- The antenna is connected to the logger. The antenna location within the chamber is then determined (this may need to be adjusted later; it is a trial-and-error process).
- The logger has its Bluetooth-compatible radio temporarily activated.
- The IDT app needs to get the identity of the selected logger that is being deployed.

There are two methods available in IDT to do this:

- The user can scan the barcode on the side of the logger in order to obtain its serial number, or
- the user can manually select the logger from a list of available loggers that are being picked-up in a Bluetooth scan.

The first method is preferred as it reduces the possibility of error.

IDT will not progress with the deployment unless it can...

- Find the logger using the Bluetooth scan and
- Can verify it has permission to use it.
- (Optional). The user can test the leak-sensor if they wish. This function is provided for troubleshooting, rather than installation.
- (Optional). The user can adjust some of the settings of the logger. Alternatively, leave the logger settings in their factory-set configuration.
- (Optional). The user can (whilst the chamber lid is off) make a Call Test to DataGate to verify internet connectivity settings are OK and that data can be sent.
- (Optional). The lid of the chamber is closed (unfortunately, this degrades the signal with the mobile phone network), and the power-level received from the mobile network (CSQ level) is checked. If inadequate, adjustments need to be made to the antenna position, or the type of antenna used, to find the best CSQ level.
- (Optional). With the lid of the chamber closed (and positions finalised), a further Test Call is made to confirm the logger can send and receive data. (See section 6.2 and 6.3).
- The location of the site that the logger is deployed within is recorded by the app, including any photographs that may be required.

- The user leaves.
- The logger goes to into standby until it needs to make measurements or send in measurement data.
- The deployment data is uploaded to DataGate during an app “Sync” process.
- DataGate is automatically prepared for receiving site measurement data from the logger.

## 3 ANTENNA OPTIONS AND INSTALLATION GUIDELINES

### 3.1 ANTENNA OPTIONS

This section describes a variety of the antenna alternatives that can be supplied for use with the PermaNET SU logger. Only use HWM-provided antenna for the logger, to ensure the radio interface meets approvals requirements (i.e. safety).

#### 3.1.1 Monopole

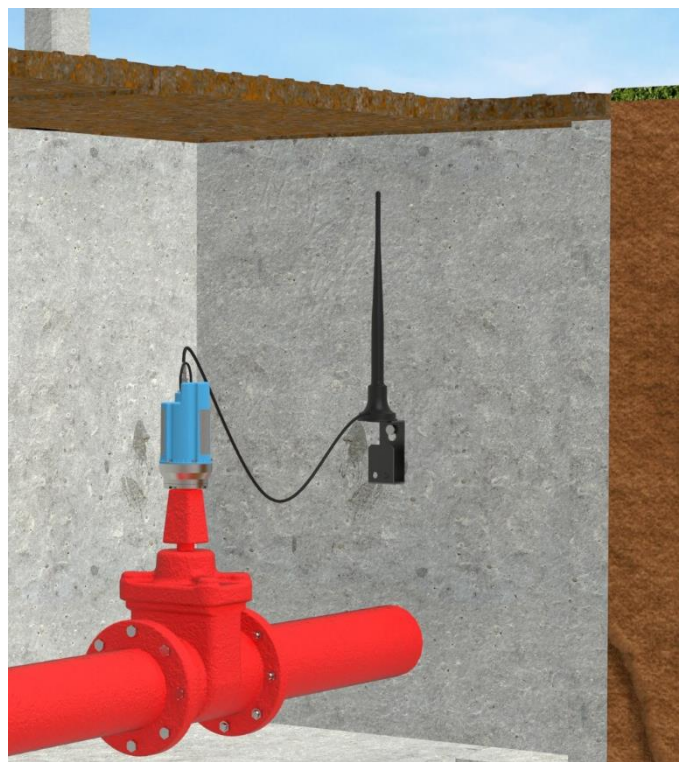
For most installations a monopole antenna will give acceptable performance.

##### Installation Considerations

- The antenna has a magnetic base to be used for mounting.
- For optimum performance the antenna requires a “ground plane” (metal surface). Consider installing a metal bracket made of a ferrous material to attach the magnetic base of the antenna, if space allows.
- Install the antenna close to the surface in large underground chambers.
- Ensure that the lid will not interfere with the antenna or cables when being opened/closed.
- This antenna is vertically polarised, it should always be installed in the vertical orientation.
- Never bend the radiating element of the antenna.
- The antenna can also be attached to an installation bracket mounted to an existing marker post.



Illustration of installed logger and a monopole antenna:





### 3.1.2 T-Bar

This antenna should be mounted at the top of the chamber. (Two examples are shown).

#### T-Bar Installation Considerations

- Mount the antenna at the top of the chamber, but spaced away from any metal lid.
- A bracket with magnetic mount is available to attach the antenna to a metal lid and also provide a gap; secure the antenna to the bracket using a tie-wrap.
- Avoid attaching the T-Bar directly to a metallic surface as this can adversely affect signal strength and performance, however it may be better than underground.
- Certain chamber lids can be replaced with a plastic version to which the T-Bar antenna can be mounted.
- Keep the antenna cable as short as possible, but allowing for installation and removal of the lid without damage or injury.

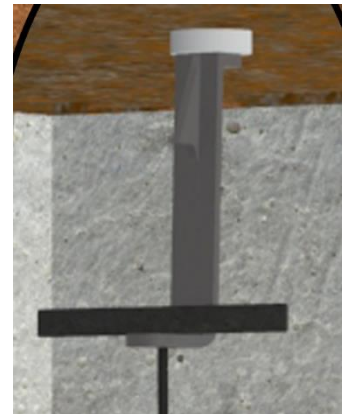
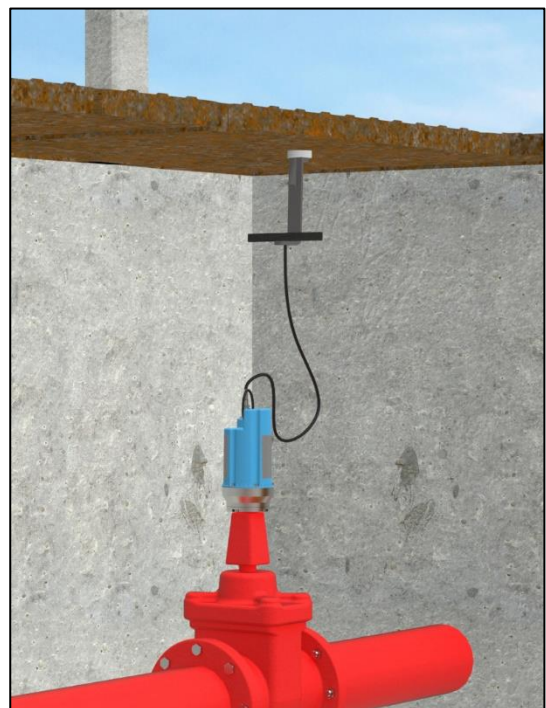
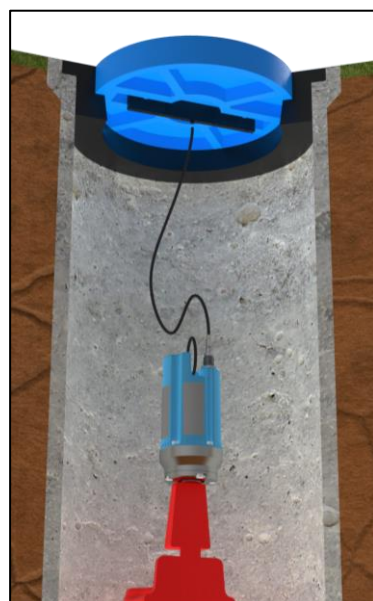
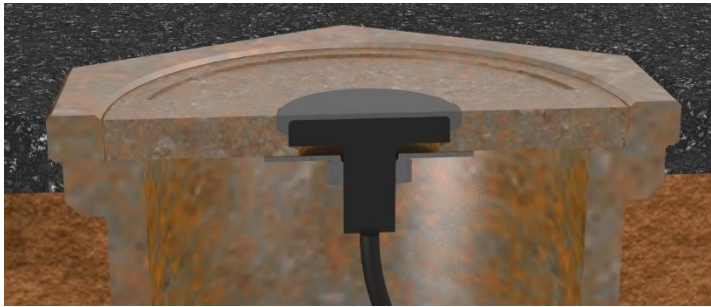


Illustration of installed logger and a T-bar antenna:  
(2 alternatives shown: metal lid and a plastic replacement lid):

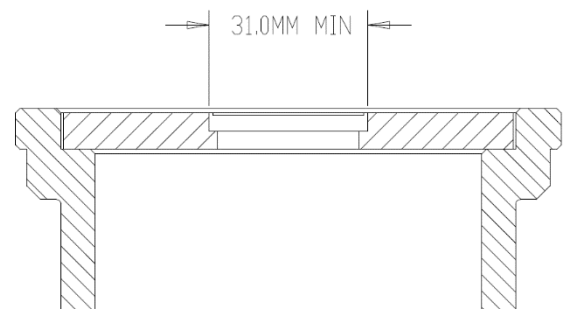


### 3.1.3 Button

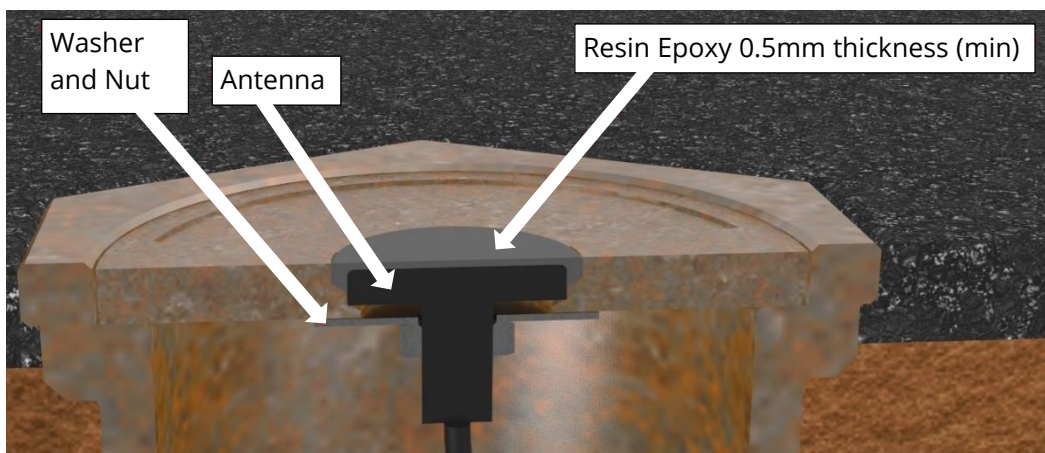
The button antenna is designed for mounting into chamber lids.



#### Button Antenna Installation Considerations



- The chamber lid is required to be drilled out to accommodate the body of the antenna.
- The top surface of the antenna needs to be a minimum of 0.5mm below the surface of the lid to prevent damage.
- Drill through the lid to make a path for the cable and connector to pass through.
- Drill partially into the lid using a wider drill to make a suitable countersink or recess that the body of the antenna can fit into. Check before drilling the recess that the size shown in the diagram still applies (the antenna supplied may be of a different size).
- Fasten the antenna using the nut supplied. A washer may be required.



- Once fitted, cover the top of the antenna with a resin epoxy such as "Marine Goop". Ensure all surfaces are clean and dry before applying the adhesive. Follow the adhesive manufacturer's instructions.
- Ensure the antenna cable does not become damaged (e.g. by the lid) during installation and use.

Installation pictures:

Drill hole in lid to provide a recess for the antenna body.



Thread antenna cable through hole, washer and nut.

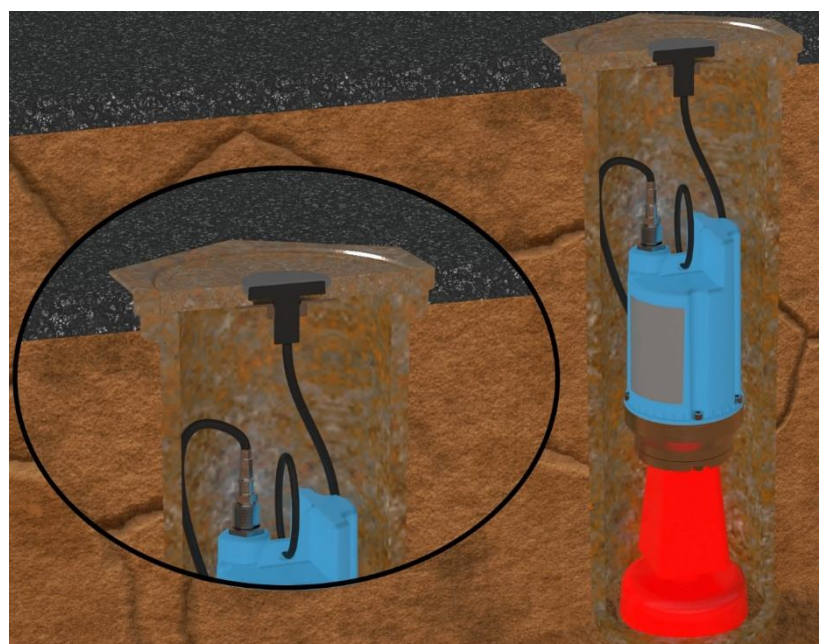
Secure antenna to the lid using the washer and nut.



Apply a resin epoxy such as Marine "Goop", covering the antenna to protect it.



Illustration of installed logger and button antenna:





### 3.1.4 Cone Antenna

This antenna should be mounted at the top of the chamber.

#### Cone Antenna Installation Considerations

- Mount the antenna at the top of the chamber, but spaced away from any metal lid.
- A magnetic mounting hook is available to provide a gap. The antenna must be attached to the hook and suspended as shown.
- Keep the antenna cable as short as possible, but allowing for installation and removal of the lid without damage or injury.

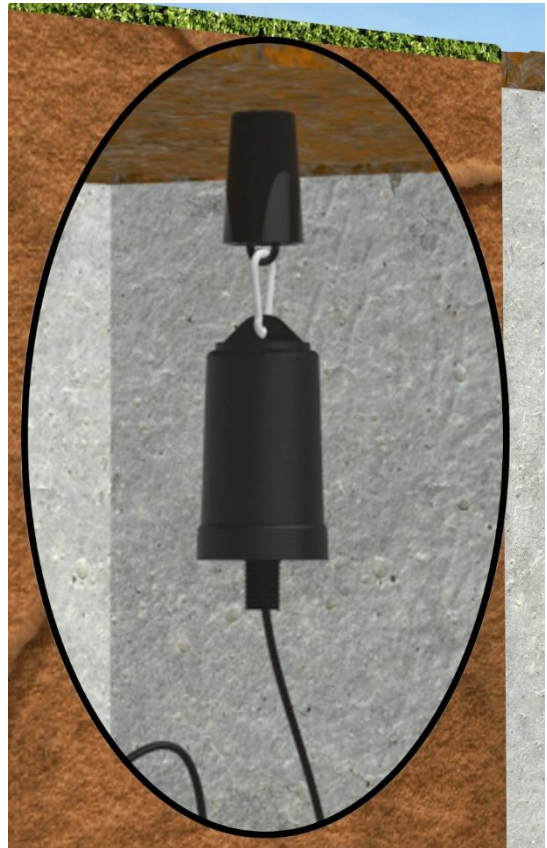


Illustration of installed logger and cone antenna:



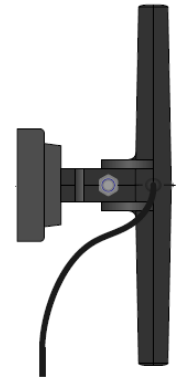
### 3.1.5 Magnetic Dipole Antenna

This antenna is similar to the T-bar.

The magnetic mounting of this antenna makes it ideal for attaching to metal structures inside larger chambers.

#### Magnetic Dipole Antenna Installation Considerations

- Antenna can be attached to the side wall of a chamber or to the underside side of the chamber lid.
- Best installation is usually with the antenna vertically polarised.

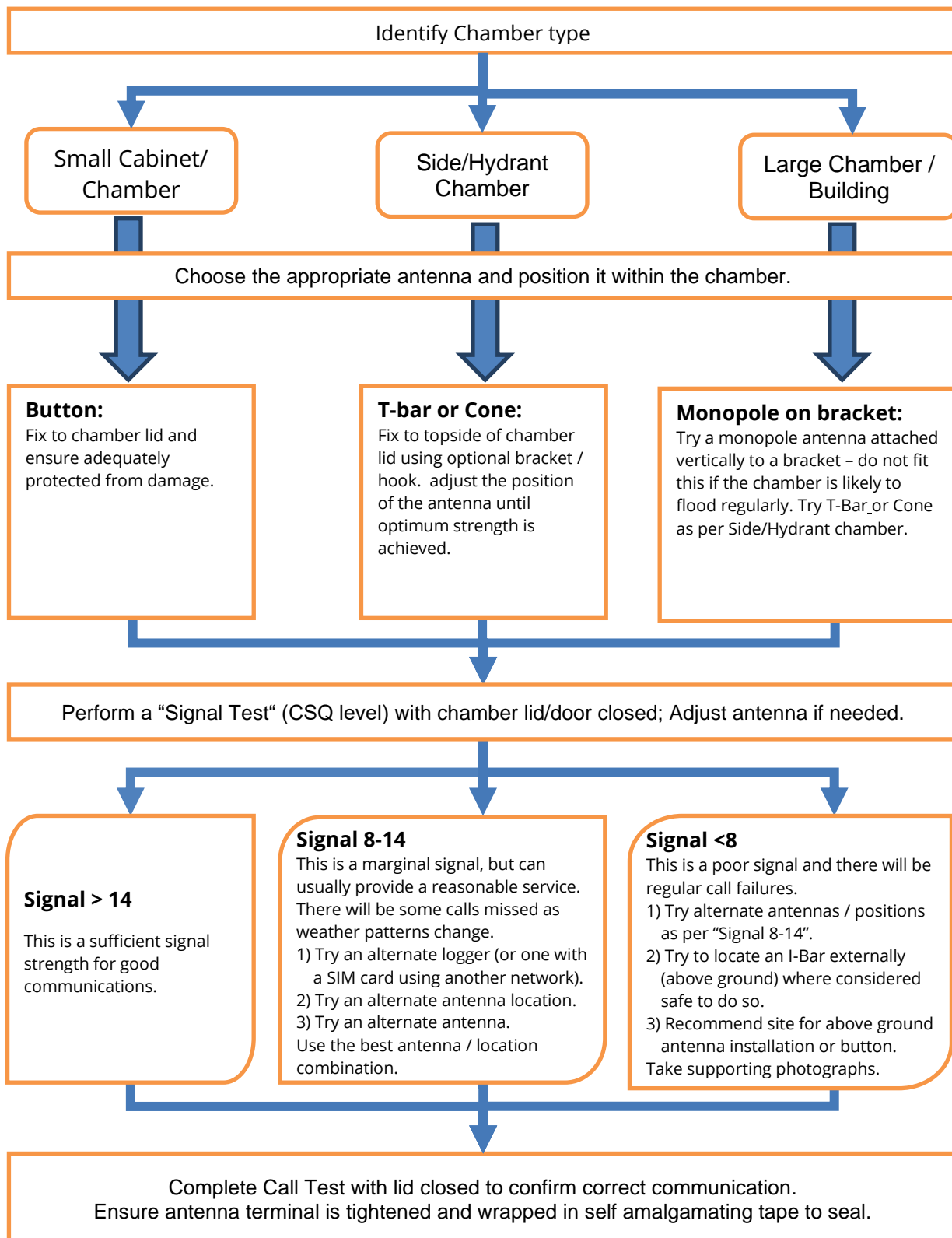


## 3.2 INSTALLATION GUIDELINES

Every site installation is unique with various types of connections, positioning or environmental conditions possible, the following recommendations will assist in a reliable installation.

- Keep the equipment neatly arranged in chambers so that cables are not crushed.
- The logger and antenna are held in place by magnets. Ensure the weight of any cables does not excessively load any magnet so as to detach it from the installed location.
- Do not allow any equipment to rest on the antenna connector as crush damage to the connector or antenna cable can result.
- Position loggers away from sources of electrical interference such as motors or pumps.
- Carefully locate the logger onto the pipe (or tap) to avoid shock damage to the sensor. Always grasp the main body of the logger when placing or retrieving it from the pipe fitting. Do not pull the logger by any cable as this can cause damage.
- Always ensure that the contact point is free from dirt, so that the magnet makes a good contact.
- Maximum operating temperature of the Logger should be below 60°C, therefore if fitting to a hot water pipe, ensure a suitable insulation is used.
- Use the IDT program to check for the best location of the antenna before finalising its position. Refer to section 6 for details of how to do this.

### 3.3 INSTALLATION PROCESS DECISION TREE



## 4 WAKING THE LOGGER AND COMMUNICATIONS LINK

At the time it is shipped from the factory, the logger is in a very low-power mode, often referred to as being in “shipping mode” or as being “asleep”. In this mode, designed for storage and shipping, the logger has not yet begun any of its daily tasks for making and saving measurements. This begins at the time of deployment, when the logger is activated, waking it from its “sleep”. Activating the logger is done by using a magnet. The same action with a magnet also used to temporarily activate the Bluetooth-compatible communications link.

Communications with the IDT app is over a Bluetooth-compatible radio interface. In order to preserve the life of its battery, the communications circuit is normally in standby. It only needs to be activated when a user is nearby and wishes to communicate with the logger. The user places a strong magnet near the logger. This activates the Bluetooth-compatible communications link, and allows user interaction using IDT. (It will also wake the logger from sleep if it was previously in storage, and required activating).

A magnet symbol can be observed near the antenna. A magnetic field sensor is near this symbol.

A strong magnet must be constantly held near the sensor for **12 seconds** (see diagram below). There is *no visual indication* on the logger that it is now active. The user must use IDT to confirm the logger and radio-link are active.



The diagram opposite shows alternative faces for applying the magnet to activate the logger and the Bluetooth-compatible communications.

Communication remains active for 2 minutes, but this period is extended to 10 minutes if the logger is paired with the phone using the IDT app, and the app is being used by the user.



Use a strong magnet, or the magnetic base of another logger.



Note: This action is sometimes called “swiping the logger”, due to earlier logger versions that only required a momentary presence of a magnet.

## 5 IDT APP – LOGGING IN AND USE

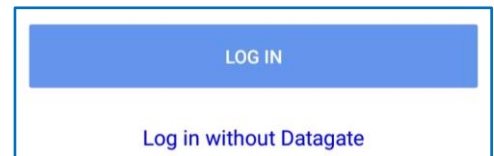
Apart from the magnetic sensor, the logger has no controls or display. The user is required to use the IDT app as the local user-interface to the logger.

Logging in enables IDT to be used with your owned loggers for up to 48 hours, after which the user is required to log in again. Login is required to use “secured loggers”.

### 5.1 USE OF IDT WITHOUT LOGGING IN

It is possible to use IDT without going through the login process, but restrictions will exist.

It will not be possible to see any secure logger, only insecure ones. It will not be possible to go through the deployment process using an app without logging into DataGate.



### 5.2 LOGGING IN AND INITIAL ACTIONS

Locate the IDT icon on the phone.

Tap the icon to launch the app.

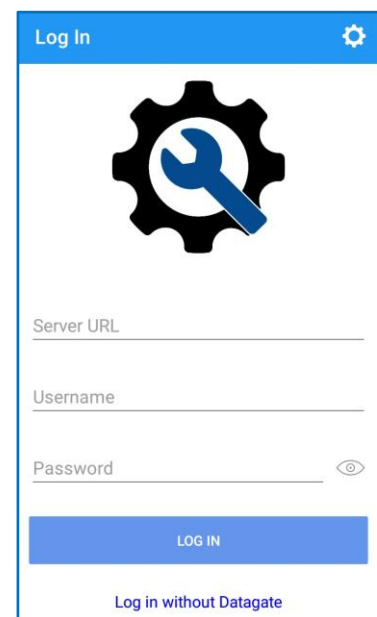


The initial screen is shown.

After several seconds, the “Log In” screen appears.

After launching the app for the first time, it has to be configured to point to the correct server.

Tap the settings control.





Type the URL of the DataGate server being used.  
(The URL, Username and password will be provided by your system administrator).

To verify the server details are valid, tap on "TEST CONNECTION".

This tests the URL, to verify it is valid and that a server is reachable using the entered details. It does not authenticate the app or its user for using the system.

Ensure the "Connection test successful" appears.

Note: This screen also shows the IDT software version.



Tap the back-arrow to return to the "Log In" window.

Enter your DataGate username and password for your mobile phone app.



The password visibility can be turned on and off with the view control.

Tap the "LOG IN" button, and the app will attempt to log into DataGate as an authenticated user.

If authentication was successful, the app will show the "Devices" window.  
("Device", as used by the app, means "logger device").

Following a successful login, DataGate downloads some information to the IDT app.

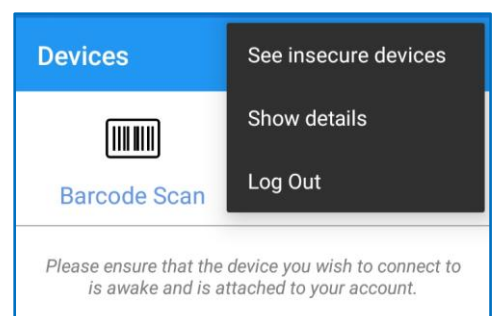
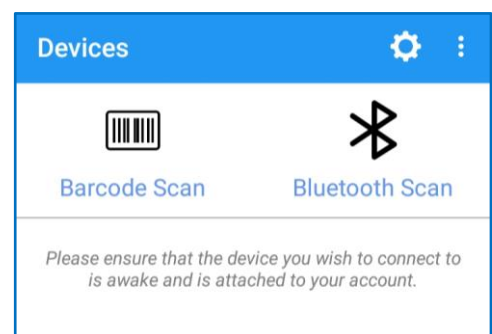
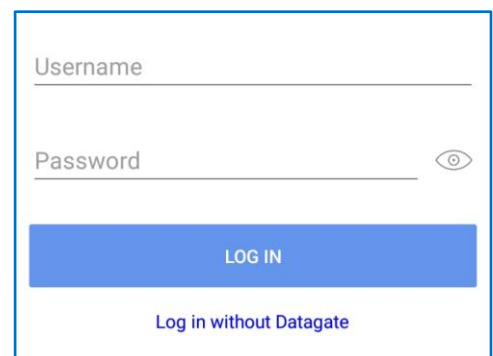
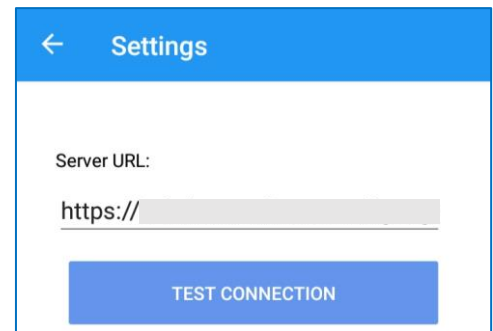
This includes a list of logger devices it is authorised to use.

(i.e. All loggers must be previously entered into the DataGate system. This task should be done by the system administrator, before installation begins, so that the app performs smoothly for the installer).

Note: Tap on the options control to access a menu.



You can log-out to prevent unauthorised use, include insecure devices in the lists (see 2.4), and change the details listed by using this menu.



## 5.3 IDT APP - SELECTING A PERMANET SU

Choose the logger to be installed. The app only communicates with one logger at a time.

Ensure the communications link of the logger has been activated (see section 4).

Two methods exist to select the logger that IDT should communicate with:

- Bar-code scan (automatic selection) ... see section 5.3.1.
- Bluetooth scan (manual selection) ... see section 5.3.2.

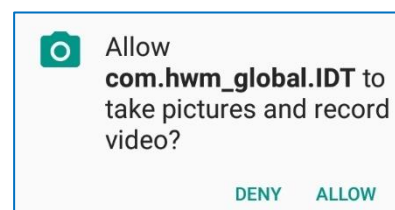
### 5.3.1 Automatic Selection using barcode scan

From the Devices window...

Tap the "Barcode Scan" icon.



The app may request permission to use the camera for photos and video. Tap on ALLOW.



The phone's camera will activate and the phone will display what is within its view.

The PermaNET SU has a barcode, as shown (or on a similar label).

Move the phone so that the red line in the displayed image is positioned over the barcode.

The app will continuously attempt to read the bar-code, changing focus settings until it comes into clear view.

When the phone reads the barcode successfully, it will check that it has permission (a serial-number match) to use the logger. If it has no permission, it will not move from the barcode scan window.



IDT next confirms the logger is physically present by trying to detect it. It therefore begins a Bluetooth scan, and looks for Bluetooth-compatible devices in the area.

If it finds the logger signal, it pairs with it.

#### Connecting to device



Please wait while we acquire the device details

If the logger device is not discovered, or the radio-link has disappeared, an error message is displayed.

#### IDT App Version - 1.0

Could not connect to device

#### Could not connect to device

Please try re-swiping device and check that you have been granted premission to use it.

OK

Re-activate the Bluetooth-compatible link and try again.

When successful, the barcode of the logger is shown, along with controls to access various options.

← SU-000050

(Skip to section 5.4)

### 5.3.2 Manual Selection using Bluetooth scan

From the Devices window... Tap the "Bluetooth Scan" icon.









A scan will commence and list some of the Bluetooth-compatible devices found.

If your logger is not listed, re-tap the Bluetooth icon. Re-activate the Bluetooth-compatible link, if required.

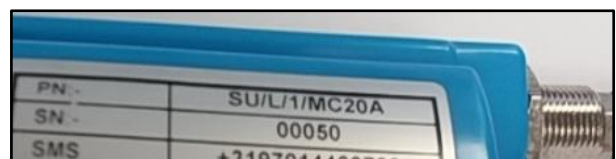
Note: Use of the options control gives the ability to see insecure loggers (shown with a red serial number).



Also, details can be shown or hidden.

Barcode Scan		Bluetooth Scan	
		MAC Address	Signal (dBm)
	SU-002627	00:80:25:D2:0A:43	 -67
	SU-080985		
	SU-002627		

The PermaNET SU will have a label which includes the serial-number.



When you find the correct logger device on IDT, tap on the line to select it. IDT will pair with it.

#### Connecting to device



Please wait while we aquire the device details

If the logger radio link disappears, you may get an error message ... re-activate the Bluetooth-compatible link and try again.

#### IDT App Version - 1.0

Could not connect to device

When successful, the barcode of the logger is shown, along with controls to access various options.

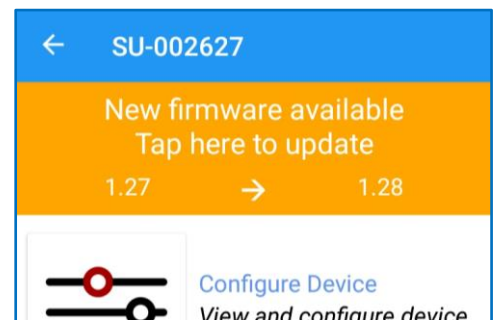
← SU-002627

## 5.4 IDT – UPDATE LOGGER FIRMWARE

The PermaNET SU logger occasionally has new software releases (called firmware) from HWM. IDT automatically checks for new logger firmware from time-to-time. If available, IDT saves the required files.

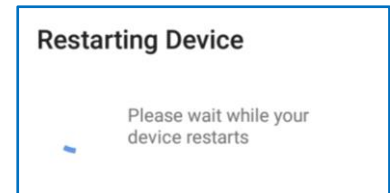
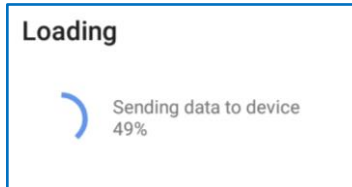
When communicating with a logger, IDT checks its current firmware version. If a newer one is available, the user has the option to update the logger using the file saved in the phone. This is recommended.

Tap the “New firmware available” line to start the upgrade, which takes approximately one minute.



Progress is shown.

The logger then has to re-start itself to run the new version.



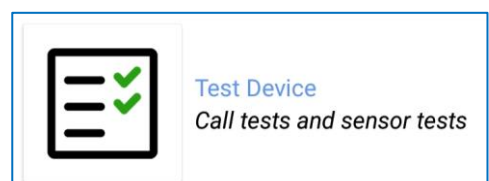
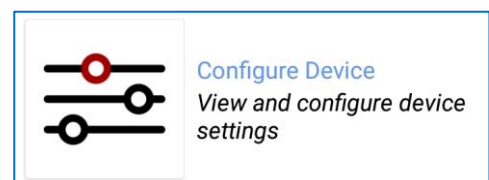
## 5.5 IDT – DEVICE OPTIONS – CONFIGURE, TEST OR DEPLOY

Following selection of a logger, controls are displayed for the user to select how they wish to use IDT app:

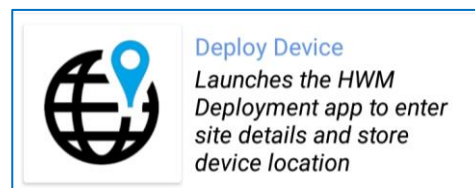
The user has access to a selection of the PermaNET SU settings, to be able to re-configure the device.

Further options are available via DataGate configuration tools.

The user has access to some tests, to be able to confirm the logger device is operational within its installed environment.



The user is able to record the installation location of the device. Tapping the Deploy Device option launches the HWM Deployment app and passes details of the logger to it.



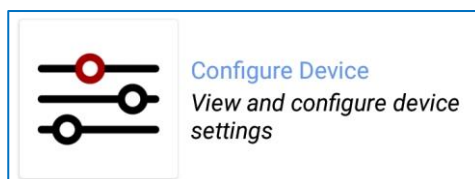
(The user will then use the HWM Deployment app to complete the task of selecting the site of deployment and update of the DataGate system).

*Pre-configured loggers* are those where the customer placing the order has agreed the required logger settings will be entered by the factory, prior to packing the device. For *pre-configured loggers*, the installer is not required to adjust any settings.

For users that are **deploying** pre-configured loggers **without any further configuration or tests** ... go to section 7.

## 5.6 IDT – CONFIGURE DEVICE MENU.

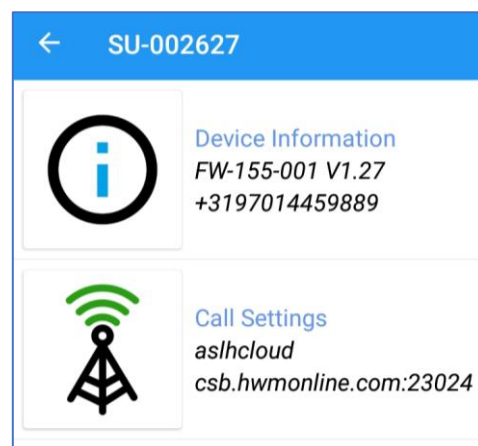
To access the PermaNET SU configuration menu, tap on the “Configure Device” control.



A new view will open with various configuration options.

**Caution:** Factory settings are usually acceptable and deviating from these can reduce the battery life.

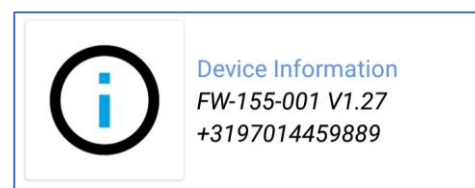
Note: The settings of your logger may be different to the illustrations in this manual.



### 5.6.1 IDT – Logger device - Device Information

Tap the “Device Information” control.

Various logger parameters are shown, including the firmware version, serial-number, and its current time.



The “Editable settings” section allows the user to (optionally) input a unique identifier in the Logger-ID field, up to 7 characters.

Another editable field is the “Telephone Number”. This number is not read from the SIM card, but has to be programmed into the logger memory.

Note: This acts as an identifier to the DataGate system, so caution should be taken when modifying this field.

The telephone number field is usually programmed into the logger by HWM prior to shipping. It is normally set to match the number of the SIM fitted, or a HWM-provided number.

On occasions where the customer fits their own SIM card, the SIM telephone number may be entered in the format shown (i.e. international format).

There is also a “UTC offset” time setting which is adjustable by the user. This is explained below:

The “Logger Time” shown in the top half of the screen may not match the time in your local time-zone. If this is inconvenient for the user, who may need to set up events using IDT (e.g. Call-in times) using the local time-zone, the user can improve operation by setting the “UTC offset” to reflect the difference between local time and UTC time (or Greenwich Mean Time, GMT). Adjusting this setting does not immediately change the displayed “Logger Time”. The update does not come into effect until after the logger next successfully calls into DataGate, which then changes the logger’s time. This allows DataGate to be able to correctly interpret logger time-stamps.

e.g. If your local time is 4 hours behind UTC / GMT then set this field to “-04.00”.

Tap the “GET” button to

If required, tap the “GET” button to display further information regarding the type of mobile network modem fitted and SIM information.



These can be forwarded to expert users for assistance by tapping on the share control.

A screenshot of a mobile application screen titled "Device Information". At the top, there is a blue header bar with a back arrow, the title "Device Information", and a share icon. Below the header, the screen is divided into sections. The first section, "Device Information", displays: Type: FW-155-001 V1.28, Serial Number: 002627, and Logger Time: 19/06/2019 16:07:47. The second section, "Modem Information", has a blue "GET" button next to it. Below these is a section titled "Editable settings" which contains three fields: "ID" with the value "ABCDEFGH", "Telephone Number" with the value "+3197014459889", and "UTC offset (30m intervals)" with the value "00:00".

Device Information	
Type:	FW-155-001 V1.28
Serial Number:	002627
Logger Time:	19/06/2019 16:07:47
<b>Modem Information</b> <span>GET</span>	
Editable settings	
ID	ABCDEFGH
Telephone Number	+3197014459889
UTC offset (30m intervals)	00:00

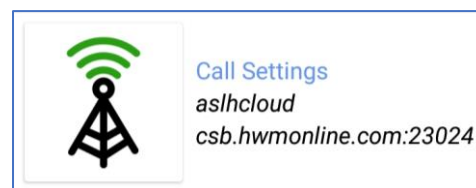
A screenshot of the same "Device Information" screen, but with the "Modem Information" section expanded. It shows: Modem: GE866-QUAD, Firmware: 16.01.204, IMEI: 356850083033546, IMSI: 204047930992764, ICCID: 8910390000016974636, CSCA: "+316540998300",145, and MSISDN: "",129. The "GET" button is still present.

Device Information	
Type:	FW-155-001 V1.28
Serial Number:	002627
Logger Time:	19/06/2019 16:07:47
<b>Modem Information</b> <span>GET</span>	
Modem: GE866-QUAD	
Firmware: 16.01.204	
IMEI: 356850083033546	
IMSI: 204047930992764	
ICCID: 8910390000016974636	
CSCA: "+316540998300",145	
MSISDN: "",129	
Editable settings	



## 5.6.2 IDT - Logger device - Call Settings

Tap the “Call Settings” control.



The current settings of the logger are displayed...

- Confirm the settings match those of your mobile-network data service provider.
- Edit any that are incorrect.  
... Tap on any line to change the setting; the change is made to the logger immediately without having to confirm it.

The APN (Access Point Name) is the name of the gateway being used by the mobile service provider to access the internet.

If required, enter a username and password... (Confirm the settings required with your system administrator).

← Call Settings	
APN Settings	
APN	aslhcloud
APN Username	
APN Password	
Settings	

In the Settings section, the first 3 items determine where logger should send its data, and what type of internet connection is to be used.

The “Call-mode” setting determines the logger call-in with data. It can either be set to “Time” or “Frequency”. The PermaNET SU should always be set to “Time”, as only one leak evaluation is made per day.

Multiple call-times can be set, but it is wasteful of the battery to send data if it was already successfully sent. Therefore, set “Continue to call when there is no data” to “No”.

Settings	
Server Address	csb.hwmonline.com
Server Port	23024
Call Type	UDP
Call Mode	Time
Continue to call when there is no data	No
Call Times	06:00, 09:30, -:-

“Call Times” lists all times the logger will attempt to call in. If it is unsuccessful at the first attempt (e.g. the network is busy), it will re-try at the next earliest call time. If all call-times for today are exhausted, it will queue the data to be sent on the following day. (A logger can send in data for more than one day, if it needs to).

It is advisable to have only a few call-times as the logger battery life could be affected when it is not possible to communicate for several days (e.g. if the chamber is flooded).

Delay call times <input checked="" type="checkbox"/> by up to 10 mins	
1	06:00
2	09:30

Call times can be added



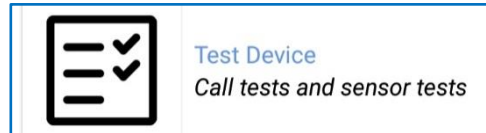
or deleted.



There is also a control available to delay the call-in time by a random time. This control reduces the peak loading on the HWM server (a large number of loggers sending data in at the same time will slow-up the response time for users of the system, until the data is processed).

## 5.7 IDT – TEST DEVICE MENU

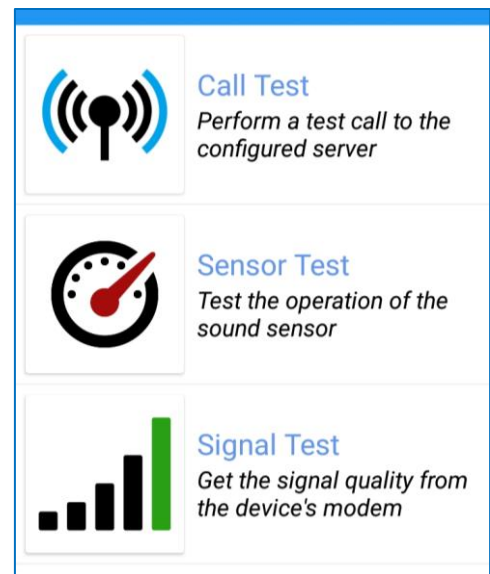
To access the PermaNET SU test menu, tap on the “Test Device” line.



A new view will open with various test options.



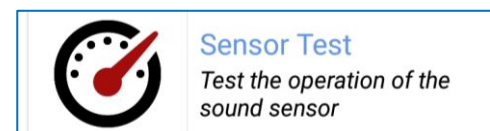
Signal Test and Call Test are covered in section 6.



### 5.7.1 IDT – Logger device - Sensor Test (Audio Noise Level)

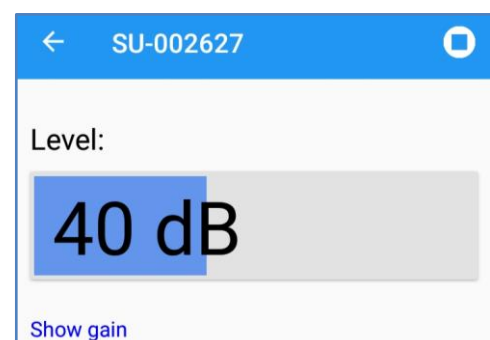
This is mainly used for troubleshooting... If there is some doubt whether the sound sensor is working.

Tap on the “Sensor Test” control.



The sound level will be displayed. This will change above ambient if you gently scratch or tap the magnetic attachment point of the logger.

(A “show gain” option is available for experienced users, which shows the loggers internal amplifier gain).





## 6 POSITIONING AND INSTALLING THE ANTENNA

See section 3 for a discussion of the various types of antenna available and guidelines of how to install. This section deals with using the IDT app to check that the logger can connect to the mobile network and that the antenna is in the optimal position for the site.

Initially, perform the “Signal Test” to confirm the logger connects to the mobile network and find the best location of the antenna.

Next, perform a “Call Test” to confirm the logger can communicate with the DataGate server.

### 6.1 IDT – SIGNAL TEST (MOBILE NETWORK SIGNAL STRENGTH - CSQ)

Access the “Test Device” menu and then tap on “Signal Test”.



This test measures the **signal strength** (CSQ) of the received mobile network signal.

Once connected to the mobile network, the provider details and signal strength indicator (CSQ) are displayed.

Initially, this test should be done with an open chamber. This is to verify that the connection to the mobile network works, and to determine what the local signal strength is.

Then, with the test still running, close the chamber. The CSQ will drop due to the lid of the chamber reducing the strength of the received signal. Re-position the antenna within the chamber to find the best signal strength (CSQ). The antenna should finally be installed in the best signal-strength position.

Network: vodafone UK 2G  
Modem: GE866-QUAD  
Firmware: 16.01.204

19

History (tap to highlight)

10:09:40	Not registered
10:09:41	Not registered
10:09:42	Not registered
10:09:43	Not registered
10:09:44	Not registered
10:09:45	Not registered
10:09:46	Not registered
10:09:47	Not registered
10:09:48	Not registered, searching
10:09:49	Not registered, searching
10:09:50	Not registered, searching
10:09:51	Not registered, searching
10:09:52	Not registered, searching
10:09:53	Not registered, searching
10:09:54	Not registered, searching
10:09:55	Registered (roaming)
10:09:58	Signal Strength (CSQ): 18
10:09:59	Signal Strength (CSQ): 18
10:10:00	Signal Strength (CSQ): 19

The following guidelines are given for the cellular network signal strength (as measured by CSQ result, with the chamber closed):

- 0-7      Poor.  
(The logger may be able to register with network but will not be able to send or receive data reliably).
- 8-14    Acceptable.  
(Depending upon the ambient conditions data transmission may be possible. It is important to select the correct antenna and install it in the most suitable location).
- 15+     Good.  
(Data transmission should be reliable).

## 6.2 IDT – CALL TEST (LOGGER TO SERVER)

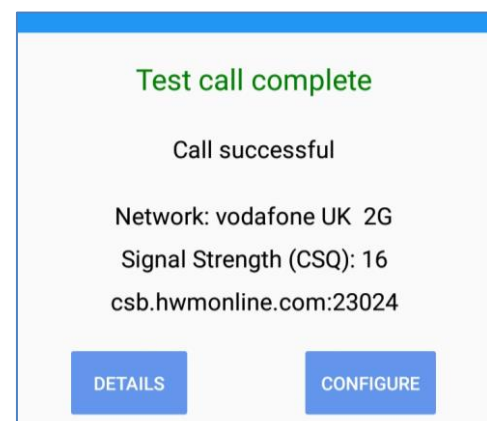
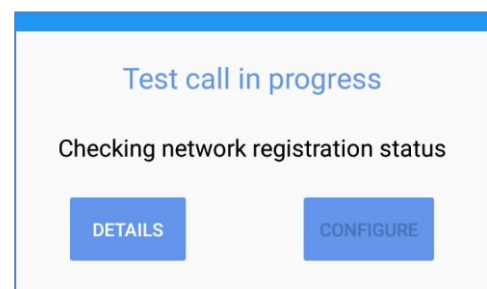
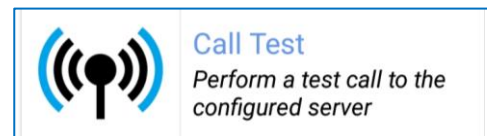
This test confirms the logger can **communicate with the DataGate server**.

Access the “Test Device” menu and then tap “Call Test”.

The logger makes a test-call to the data-server over the mobile network.

The call will progress through various stages.

Check if it is successful.



If there is some problem with the test-call, some details are available to assist in finding where the problem exists.

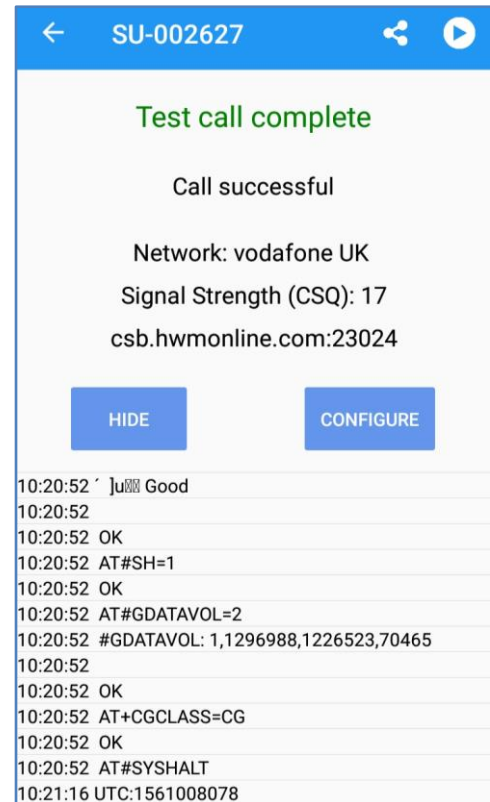
If required, Tap the “Details” button to show the modem commands and responses (for debug).



These can be forwarded to expert users for assistance by tapping on the share control.

**Note:** The Call Test can be made initially with the chamber open, to prove it is possible to communicate with DataGate using an unimpaired mobile phone signal.

Repeat the test later with the lid closed to confirm the signal is not degraded to an unusable level by the chamber lid.



## 6.3 TROUBLESHOOTING A CALL TEST FAILURE

### 6.3.1 Possible Issues and Checks

There are a number of reasons why a Call test may fail.

The following points should be checked before calling HWM support for assistance: -

Possible Problem	Solution
Network Busy due to excessive traffic. Commonly occurs around schools and at peak travel times.	Retry the test after a few minutes.
Network signal not available at your location. Not all Cell masts carry data traffic	Relocate the logger to an area that has a data service or change to a different network provider.
Network signal not strong enough. You need a CSQ (reported by the Call test) of at least 8 for reliable communications.	Relocate the antenna if possible or try alternative antenna configurations. Ensure antennas are vertically orientated where possible. See section 6.3.2 and 6.3.3.
APN settings incorrect.	Check with your network operator that you have the correct settings for your SIM.

If you continue to experience problems with communication, you may need to check the network coverage in your location.

### **6.3.2 Antenna - Installation considerations**

The method of installation of the antenna at the site should be carefully selected.

Signal strength within a cellular network can vary dramatically even within the same cell; proximity to the transceiver, type of antenna used, position, angular orientation of the antenna, time of day, all have a significant effect on the ability of a logger to reliably communicate with the cellular network.

Also consider that network operators can change the operating power during the day / night, so this can lead to times of the day when communication is not possible.

To ensure reliable data communications it is essential that the most suitable antenna is selected and it is mounted in the most appropriate location.

Installing a logger without considering the type of antenna and its installation constraints can lead to disrupted and unreliable data communications and accelerated battery consumption.

If the logger has a poor mobile network service it can also result in the failure to send sound files, since these are much larger files and will be more vulnerable to transmission failure.

The following gives practical advice on how to minimise potential problems:

### **6.3.3 General Considerations**

- Always perform a signal strength test using the IDT "Signal Test" function. Try moving the antenna to different positions and comparing the CSQ value (please see section 6 for description of signal strength test results).
- When checking and comparing signal strength (CSQ) with various antennae and positions, ensure that the chamber lid/cabinet door is in the normally closed position to ensure an accurate comparison and result.
- Try to avoid moving the logger and/or cables after performing the "Signal Test" and "Call Test" as this can change the result. The final call test should be performed with the antenna cables and logger in the final positions.
- If the logger is installed in an underground chamber consider, where possible, locating the antenna in a secure position outside the chamber. (e.g. Inside a hollow marker post or attached to the back of a concrete one). A steel post can also work to get the antenna above the snow level, but always make sure the antenna is not shielded within the metal; fit it inside a plastic cap.
- When positioning the antenna in an underground chamber, be aware that the best signal is not always at the very top of the chamber. A few cm below the metal lid can improve signal reception. Use a bracket if required to provide the gap between antenna and lid.
- Always try both antenna polarities (Horizontal and Vertical), most antennas work best when the long side is positioned vertically, but sometimes the horizontal position can be better.
- Ensure the logger and antenna connectors are dry before connecting them.

- Ensure that the antenna connector is in good condition and correctly tightened, using fingertips only. DO NOT overtighten. Adequate tightening of the connector reduces the risk of water ingress.
- Consider using secondary environmental protection for the antenna connector such as silicon grease and / or self-amalgamating tape.
- Use the shortest possible antenna lead and ensure that there are no kinks or tight radius bends in the cable. A kinked cable can cause signal loss.
- Where long antenna leads are required, consider using a low-loss cable.
- Any antenna submerged under water will not work; place the antenna in a location where it will not become submerged.

## 7 IDT – DEPLOY DEVICE

To begin the process of **recording the location of deployment** of the PermaNET SU, tap on the “Deploy Device” line.

At the time of writing, this action launches (and passes logger details into) the HWM Deployment app.



### Deploy Device

Launches the HWM Deployment app to enter site details and store device location

### 7.1 HWM DEPLOYMENT APP – LOGGING IN AND INITIAL ACTIONS

The HWM Deployment App is launched by the IDT app (rather than the screen icon), simultaneously passing some logger parameters.

The initial splash-screen is shown.

After several seconds, the “Log In” screen appears.  
... Do not attempt to log in yet.

After launching for the first time, the app must be configured to point to the correct server.

If the server settings are empty, the app will shortly take you to the required screen. If it does not, tap the line:

“Configure server URL and install account name”



Username

Password

LOGIN

[Configure server URL and install account name](#)

v2.15rr

Enter the Install Account, and (optional) any Storage Account being used. (See section **Error! Reference source not found.**).

(These will be provided by your system administrator).

e.g. Install Account = Fleet 1

Storage Account = Van 1

... in the example given.

Enter the URL of the DataGate server being used.  
(This will be provided by your system administrator).

To verify the server details are valid, tap on “TEST CONNECTION”.

This tests the URL, to verify it is valid and that a server is reachable using the entered details.  
It does not authenticate the app or its user for using

### Installation Setup

Install Account Name:

Mysuinstall

Storage Account (optional):

Mysuinventory

Server URL:

TEST CONNECTION

NOTE: Connection Test does not test Install Account Name or the Storage Account name. This is checked when you are logging in.

the system. A tick appears if the URL can successfully reach a server.



Tap the back-arrow to return to the "Log In" window.

Enter the DataGate user-name and password that has been allocated for your mobile phone app.

Note: This should be the same username and password as used by the IDT app.

Tap the "LOGIN" button, and the app will attempt to log into DataGate as an authenticated user.

If authentication was successful, the app will show the "HWM Deployment App" main window.

When the "INSTALL" tab is selected, it will show the SMS (telephone) number of the logger, which was passed to it by the IDT app.

If this is the first time the Deployment app has been run, the logger will not be known to it. A sync is required.

To sync:

Select the Options tab. Tap on “Last sync with server”.

Sync should complete.

### Synchronisation

Synchronisation completed successfully.

OK

Last sync time is updated.

Last sync with server

25 Apr 2019  
10:37

Failure to sync regularly can lead to errors later on as the logger is deployed.

e.g.

### Error

Could not retrieve site information for this SMS number. Check your internet connection, or try synchronising your database (found in the Options menu).

OK

The screenshot shows the 'HWM Deployment App' interface with the 'OPTIONS' tab selected. The screen is divided into sections: 'Site Details' with toggle switches for 'Automatically estimate address' (on) and 'Add an auto-generated site ID' (off); input fields for 'Prefix address with:' and 'Prefix site ID with:' both set to '[No prefix]'; an 'Other' section with 'Last sync with server' set to 'Never'; and links for 'View help document', 'App Information', and 'View privacy policy'. A red 'Log out' button is at the bottom.

Note: The user can set various options from this screen and also log-out.

Log-out when you have finished using the apps, to prevent unauthorised use.

## 7.2 HWM DEPLOYMENT APP – COMPLETING SITE DETAILS

Select the “Install” tab.

Next select the installation type, which should be set to “New Install”.

### Installation type

New install

Lift & Shift

(A new installation overwrites the details of the site the logger is on. It therefore completes the information for the site the logger is linked to when shipped by the factory).

(Optional).

To confirm the Deployment App has permission to deploy the logger...

### SMS Number

3197014459889

CANCEL

OK

Tap on the SMS Number line. Then tap OK. If the logger is found, there will be no error message.

The screenshot shows the 'HWM Deployment App' interface with the 'INSTALL' tab selected. The 'Site Details' section is active, showing 'Installation type' set to 'New install'. Below this are fields for 'SMS Number' (3197014459889), 'GPS Coordinates', 'Site Address', 'Site ID', 'Zone/DMA', and 'Site Notes', each with a corresponding icon and a text input area.



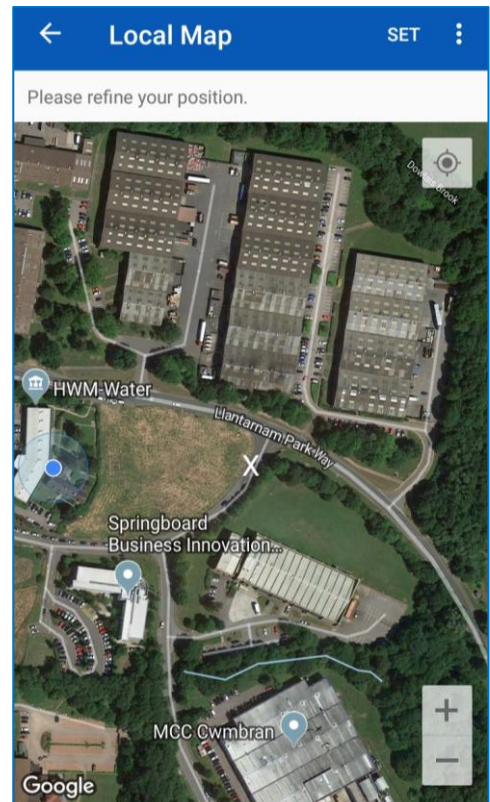
The location (GPS coordinates) of the installation site of the logger should now be entered...

Tap on the "GPS Coordinates" line.

Wait for the map page to load.

Locate the "X" cursor onto the position of the installed logger. Then tap on "SET".

(You can use regular phone screen control methods to zoom or move the map).



The GPS coordinates are completed.

An *estimate* of the address of the site is obtained from the internet. (This can be manually adjusted if required – Tap on the address to edit it).

Tap on "Site ID" and enter a Site ID.

<b>Site ID</b>
mySUsite0001
<span>CANCEL</span> <span>OK</span>

HWM Deployment App	
INSTALL	SWAP DATABASE OPTIONS
Site Details	
Installation type	New install
SMS Number	3197014459889
GPS Coordinates	51.6339625343405, -3.01483478397131
Site Address	Unit 1, Concordia House Lakesi ...
Site ID	
Zone/DMA	
Site Notes	
SAVE	

Tap on “Zone / DMA” and select a DMA from the list of available DMAs (the list is obtained by the app after DataGate login and sync).



To enter additional information, move the list upwards.

Complete details for the pipe and chamber type (pick from lists).

A minimum number of photos of the installation is needed by the app, however additional ones can be made.

(The minimum number of photos is a DataGate setting).

Ideally, the photos should show the logger, the antenna, the closed chamber and its location.

Tap on “New photos”. To add photos, select the camera icon and take some photos of the installation.

Photos are listed.

When finished, tap on “DONE”.

	GPS Coordinates 51.6339625343405, -3.01483478397131
Site Address	Unit 1, Concordia House Lakesi ...
Site ID	mySUsite0001
Zone/DMA	mySuDMA001 (my SU DMA001)
Site Notes	
<div>SAVE</div>	

Site Notes
Pipe and Chamber
Pipe Material
Pipe Diameter
Chamber Type

Pipe and Chamber
Pipe Material Cast Iron
Pipe Diameter 2" (50mm)
Chamber Type FH (Fire Hydrant)
Photos
New photos No photos selected
<div>SAVE</div>

<div>← Photos DONE</div>	
Photo selection Add photos either from your photo library, or take pictures directly.	
Add from camera	Add from saved
 mySUsite0001_1555340271_0	

When all the data for the installation has been completed, tap on “SAVE”.

The deployment details will be listed within the “Database” tab, which shows all deployments made by the app. If an exclamation mark is displayed on the line, it indicates the data is waiting for upload (or a sync) to DataGate.



Upload the deployment data to Datagate using the Upload icon (shown). This uploads location details and also any photographs.

The screenshot shows the 'HWM Deployment App' interface. At the top is a blue header with the app name, a cloud icon, and a menu icon. Below the header are four tabs: 'INSTALL', 'SWAP', 'DATABASE', and 'OPTIONS'. The 'DATABASE' tab is selected. The main content area displays deployment details for a specific site. The details are as follows:

Field	Value
Zone/DMA	mySuDMA001 (my SU DMA001)
Site Notes	
Pipe and Chamber	
Pipe Material	Cast Iron
Pipe Diameter	2" (50mm)
Chamber Type	FH (Fire Hydrant)
Photos	
New photos	1 photos selected.

At the bottom right of the form is a blue 'SAVE' button.

You have now completed your site installation and (optionally) confirmed that the logger is operating and transmitting its data to DataGate™ (or your local data server).

### 7.3 HWM DEPLOYMENT APP – SYNCHRONISATION

The IDT app / HWM Deployment app and DataGate manage the location of the loggers so that their data can be routed to the correct site in the database. This process requires the exchange of data between the IDT app / HWM Deployment app and DataGate.

As the app is put into use, information (e.g. new location of deployment of a logger) is stored by the phone. Each item of new information is tagged as an unsent data item.

DataGate must be brought up-to-date with this new information. This is done as part of a process called synchronisation.

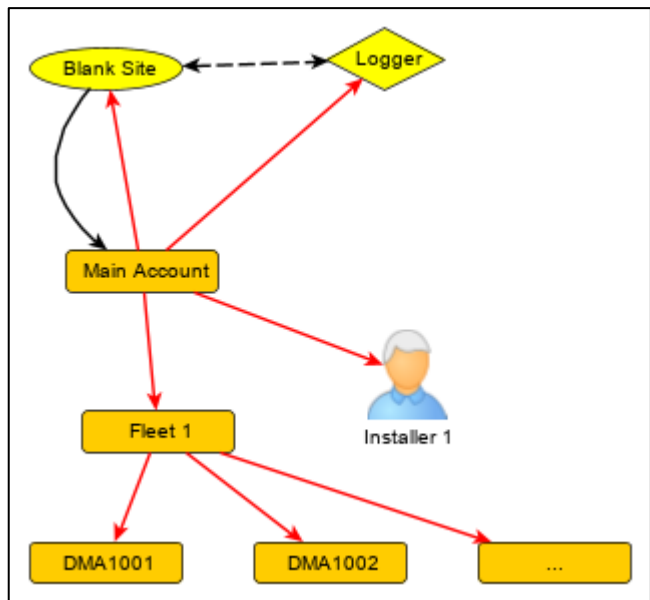
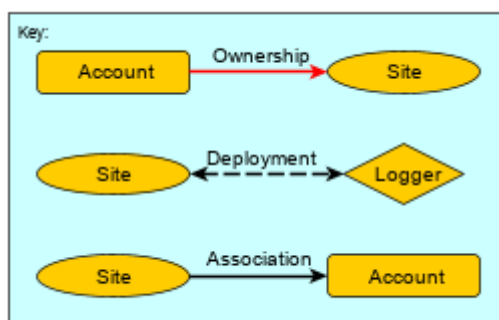
**Note:** It is important to synchronise frequently to avoid loss of data. Deployment data held within a phone that becomes mis-placed (without it being synchronised) cannot be recovered. A visit to the site of deployment of each logger will be required, to recover the devices and then re-deploy them using the IDT app once more.

## 8 DATAGATE – SETUP FOR USE & CHANGES MADE BY APPS

Note: This information is not required by installers, but may be informative for office staff. It should be read in conjunction with section 2.5, which describes the terminology used by DataGate and the apps.

### 8.1 DATAGATE – EXAMPLE STRUCTURE FOR USE

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



The Users of the system (here, the user of IDT and HWM Deployment app) must be “owned by” the “Main Account”. The apps log-in at this level, but have permission to access any account below this level. If the app is required to work at a lower-level account, the details of lower-level account can be entered into the app (as the “Install Account”) during its setup and use.

When the logger devices leave the HWM factory, they are also registered (by HWM) on the DataGate system and linked to a “blank site” (one site per logger). Both the blank site and the logger are initially owned by the Main Account.

All accounts are linked together hierarchically by the concept of ownership. Thus, the “Fleet 1” account has the “Main Account” as its owner.

Note: The “Fleet 1” account in the diagram is shown as a single account, but could be sub-divided into many accounts if required.

DMAs are very similar to accounts in that they are linked together hierarchically by the concept of ownership. Thus, “DMA1001” has the “Fleet 1” account as its owner.

The app, during the operation of deployment, makes updates to the initial site data, causing the logger to be linked to a “real site” (by completing the data for the “blank site”). The site is then linked to the chosen DMA. The process is described in section 8.

Note: The scheme described in section 2.5.2 is slightly modified, for ownership of sites. The DMA does not take direct ownership of the site. The site remains owned by the main account. It is connected to both the selected DMA and also other accounts (acting as larger DMAs) by means of another type of database link, referred to as an “association”. Association links permit the site to *appear to* belong within multiple DMAs (or accounts).

There are 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).

## 8.2 DATAGATE – REQUIRED USER ROLE PERMISSIONS

The 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.

## 8.3 DATAGATE – CHANGES MADE BY HWM APPS

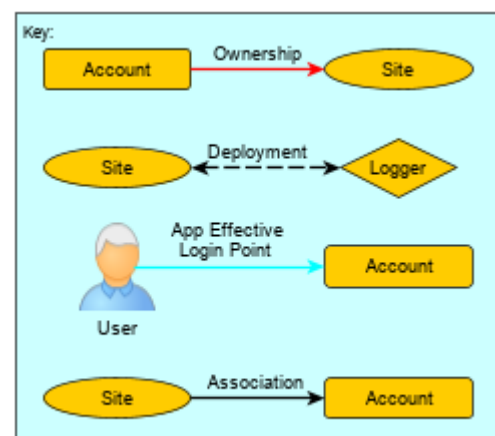
This section describes graphically the changes apps make to DataGate.

See opposite for a key of various types of links.

An ownership link can be used to form a tree structure. It gives permission to make changes. Sites can be owned by accounts. Accounts can be owned by other accounts. 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.



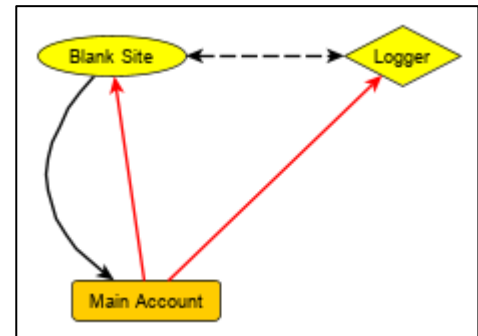
A User (person or app) logs into DataGate at the level of the account that owns the user. However, the app can change to an “effective login point” to below this level for its operations. The Deployment app makes use of two “effective login points”, the “Install Account” and also the (optional) “Storage Account”. (A storage account is required if HWM PRISM app was used by goods-in or stores).

### Initial State (HWM):

At the time the logger device leaves the HWM factory, it is registered on DataGate by **HWM** and attached to a newly created “blank site”.

Both logger and blank site are owned by the main account of the water company (or whatever the company has nominated as being the main account).

The site also has an association link to the main account (to give visibility of the site).



### Initial State (Water Company):

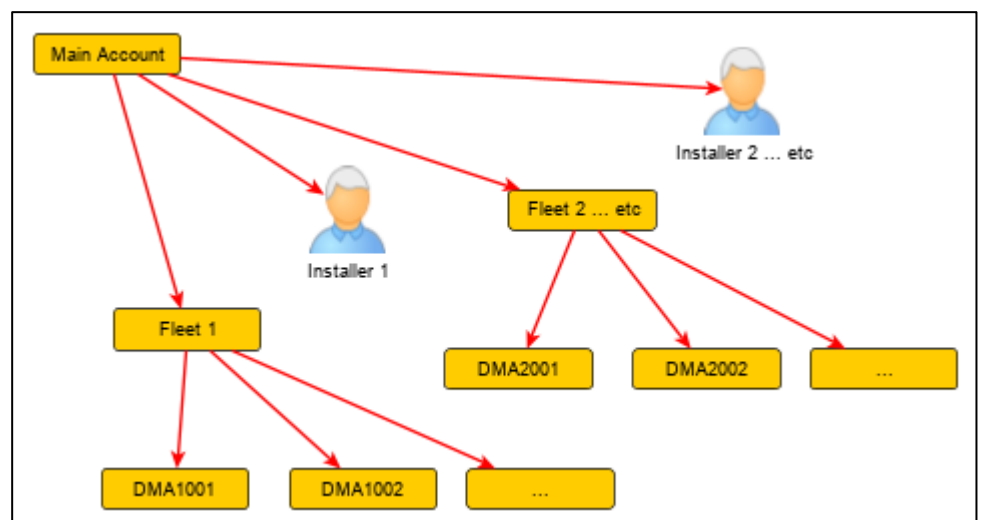
The **Water Company** is responsible for any structures connected to or below the main account. Each installer requires their own phone. For each installer, a User has to be created on DataGate for the app to use. Each User is owned by the main account.

Each installer (User) also requires an account to be set up to hold all the DMAs that the installer will be deploying the loggers within. This account (referred to as the Install Account by the app) is also to be owned by the Main Account. However, it does not have to be directly owned ... it can alternatively be owned by a sub-account of the main account).

Below the Install account, multiple DMAs will be created, each representing a geographical area of the pipe network to which loggers are to be deployed.

The DMAs are owned by the Install Account.

Refer to the picture opposite.



The water company may (optionally) have set up a similar structure within DataGate to manage the location of the loggers *whilst in storage*.

Note: This manual does not cover the use of the HWM PRISM app. Details are given here to demonstrate how the scheme works.

Refer to the picture opposite.

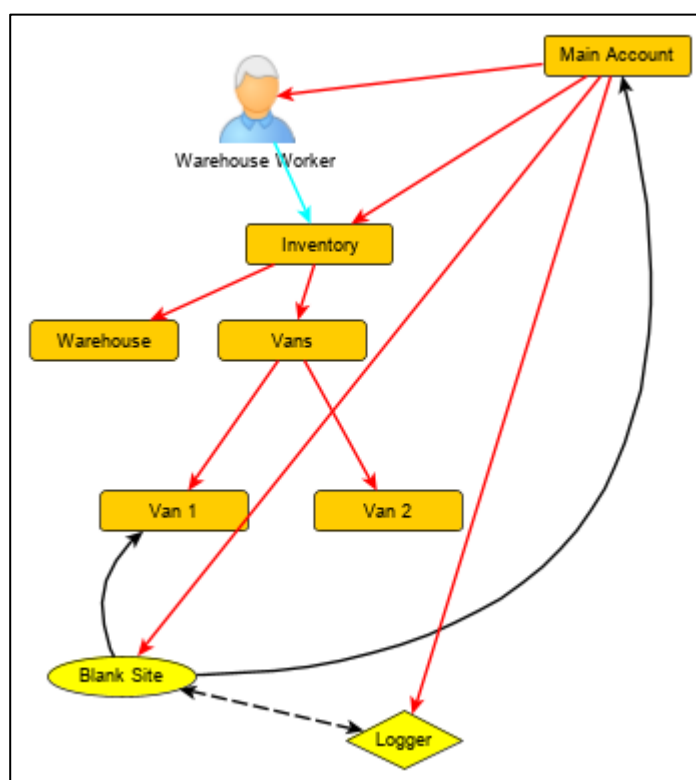
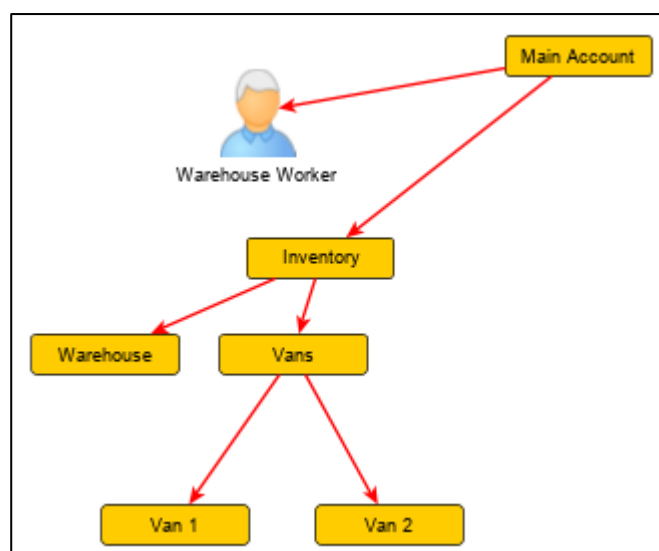
Each account represents a physical storage location, or collection of storage locations.

### Changes using PRISM:

Upon arrival at the water company, the **water company** may use an app (e.g. HWM PRISM) to link the logger (within DataGate) with a storage location.

This is not an ownership move, but a visibility move, using the site to which the logger is attached.  
(i.e. An additional association is made between the blank site and the account representing the storage location).

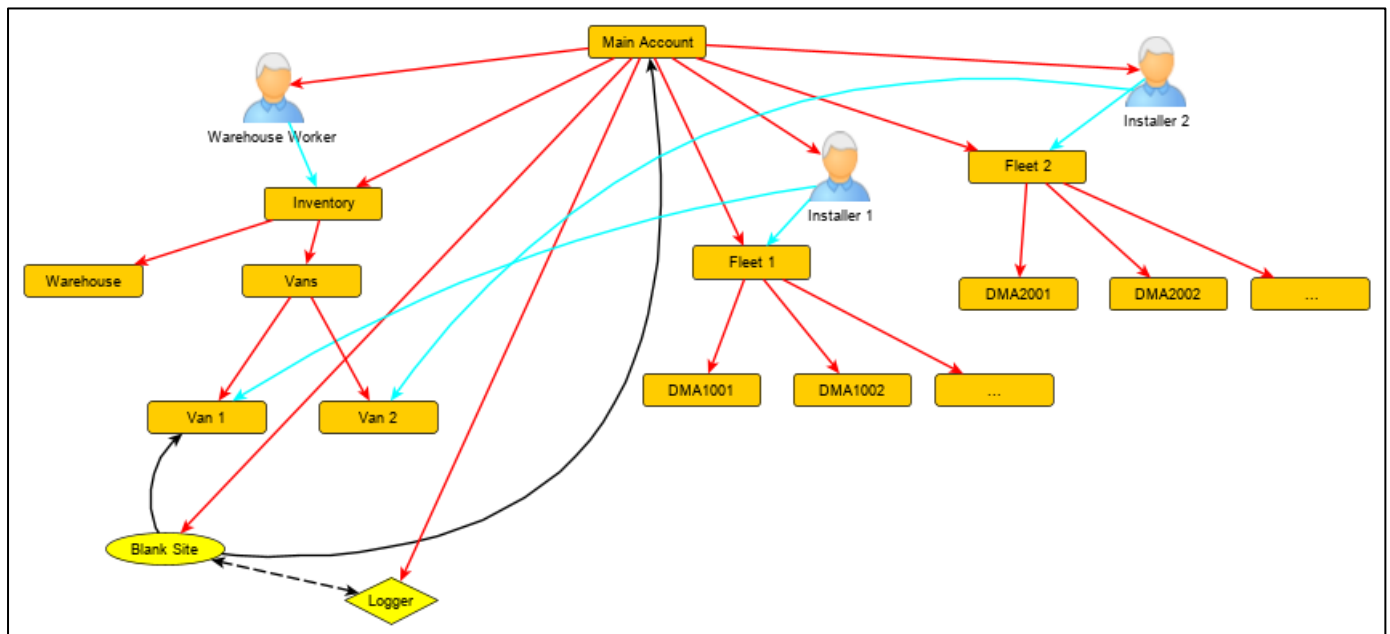
In the diagram opposite, the warehouse worker has put the logger into "Van 1" using the HWM PRISM app and thus there is a new association link between the blank site and Van 1.





### Changes using IDT / Deployment app:

The diagram below shows the use of the IDT / Deployment app by the **water company**.



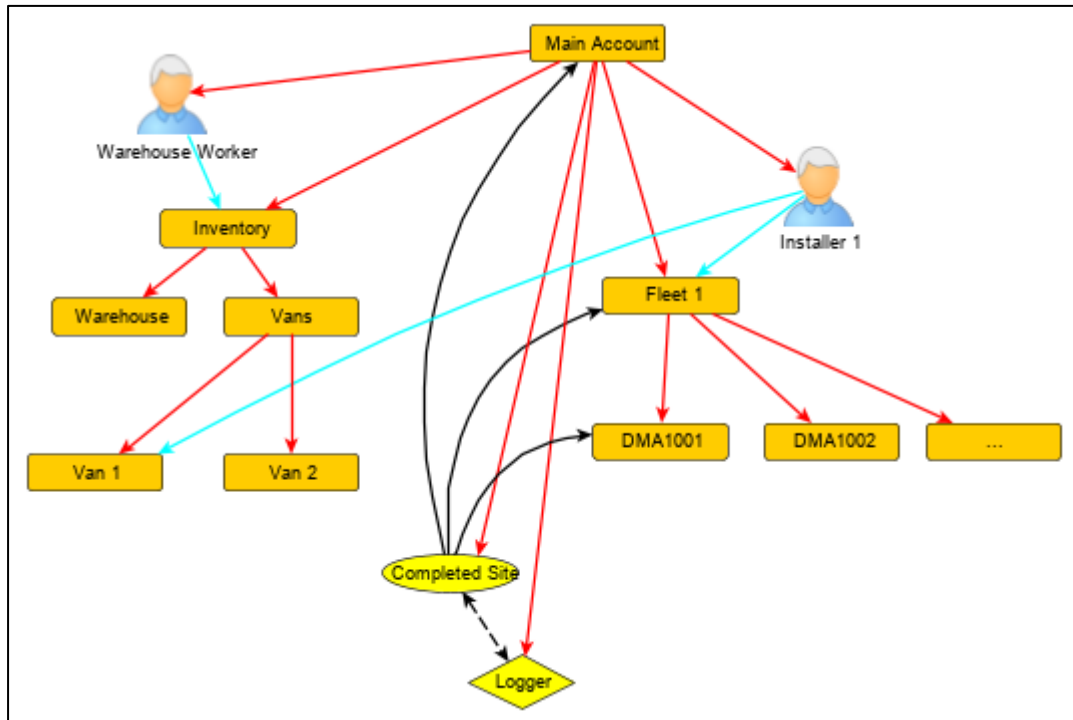
In the diagram, two Users ("Installer 1" and "Installer 2") are both using their own phone with the app installed. Each user has set the app to point to their individual install account and their (optional) individual storage account. Both users are owned by the main account, as are all the loggers and sites. Both users therefore have permission to use any of the loggers owned by the main account.

Note: At the time of writing, there is no check and restriction within the app to only give access to loggers that are also in a user's (optional) storage account. There is however a physical constraint ... the user must confirm they have the logger in their possession by first waking it and then talking to it via Bluetooth).

After the user has selected the logger and gone through the deployment process within the app, they must upload the deployment details to DataGate.

The following changes then occur on DataGate:





- The details for the site of deployment are over-written onto the (partially completed) “blank site” that the logger was attached to when it left the factory. This includes, for example, a new site-ID and GPS coordinates. (The blank site becomes a fully completed site).
- The ownership of the logger and site do not change, but the associations of the site change. (see diagram above).
  - The site is disassociated (association link removed) from the account pointed to as a storage account; effectively this removes the logger from being connected to any storage location represented on DataGate.
  - The site keeps the existing association (to the owner account) and adds associations to the DMA selected and also the Install account. Effectively, this makes the site (in which the logger is deployed) now visible from DMA and also the Install-account when navigating through the levels of the DataGate account hierarchy. It is also still visible at the Owner-account level.
- Photos of the logger installation are linked to the site.
- The DataGate has been set to expect the receipt of measurement data for the site from the installed logger.
- DataGate monitors the site to ensure the installed logger is communicating its measurement data regularly.

## 9 DATAGATE – REMOTE PROGRAMMING OF A LOGGER

---

### 9.1 OVERVIEW OF OPERATION

Once the PermaNET SU has been installed and is successfully communicating with DataGate, the logger has the ability to have some of its settings adjusted remotely using the DataGate system. This is done by the use of queued commands. Queued commands are needed because the logger is normally in standby (to conserve battery use), so it is not available for DataGate to send the command(s) immediately.

When the logger calls into DataGate, it first sends its measurement data. Following this it enquires if any commands are waiting. If there are, it collects them and processes them before ending the call. Thus, changes to the logger's settings do not usually come into effect until the day after the command is entered into DataGate. It also is dependent on the data connection (provided by the mobile network) being sufficiently good at this time to exchange messages with the installed logger.

The command is stored within the DataGate database as if it were a command for *the site*. The logger can therefore only be re-programmed when it is installed on a site. Likewise, *the site* will not accept any commands to be stored unless it has a logger installed.

The remote programming facility is typically used to:

- Switch automatic sound recording generation on or off.
- To setup a scheduled sound recording.

The delay for the pick-up of commands should be considered when remotely re-programming loggers, especially when programming scheduled sound recordings; the logger could otherwise pick-up the command after the recording start-time, and so cannot process it.

Note: Remote programming of the logger can only be made by a user *with sufficient privileges* to access the various web pages in DataGate / PermaNETWeb.

Note: Additional settings can be adjusted remotely by HWM Customer support staff. Including: Leak evaluation time, call-in times, leak determination thresholds. Please seek advice if an issue is found with a site which has a logger using the factory default settings.

### 9.2 AUTOMATIC AND SCHEDULED SOUND RECORDINGS

The PermaNET SU can be considered to have two (user-accessible) internal controls relating to sound recordings:

- Automatic sound recordings required flag (On / Off).
- Scheduled sound recordings required flag (Pending / Off).  
(Additional settings are required, for example the time to make the sound recordings).

"Automatic recordings" occur when the logger changes from a no-leak to a leak state.

“Scheduled recordings” are a *1-off program* that can be given to the logger in order to make *additional recordings* at fixed times.

To remotely program the sound recording settings:

Use PermaNETWeb and navigate to the site which contains the logger.  
e.g. Find the site in the List View, shown below.

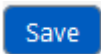
Access the site “pop-up” by clicking on the line listing the site.

The details of the logger and latest measurements will initially be displayed, within the “Info” tab.

Select the “Program” tab.

The drop-down control (shown) will list the condition options under which the logger will make sound recordings.

- No Sound Recordings.
  - Sets the production of automatic sound recordings = **OFF**.
  - No additional scheduled sound recordings are programmed into the logger.
- Record sound when leak detected.
  - Sets the production of automatic sound recordings = **ON**.
  - No additional scheduled sound recordings are programmed into the logger.
- Record sound at pre-set time.
  - Sets the production of automatic sound recordings = **OFF**.
  - Additional scheduled sound recordings are programmed into the logger; The logger evaluates the start-time of the scheduled recordings, and if in the future it sets the scheduled recordings flag = **Pending**.
- Record sound when leak detected or pre-set time.
  - Sets the production of automatic sound recordings = **ON**.
  - Additional scheduled sound recordings are programmed into the logger; The logger evaluates the start-time of the scheduled recordings, and if in the future it sets the scheduled recordings flag = **Pending**.

 Additional settings may be required ... see below. Once the settings are complete, click the “Save” button, which creates and stores the command.

When programming a scheduled sound recording, multiple sound recording events can be programmed within the one schedule. The logger can only store one schedule.

Set the start-date of the schedule, making sure sufficient time exists to pick-up the command.

Select the daily start-time of the recordings

Set the number of days you want to make the recordings on (starting from the first day).

Set the number of recordings to be made each day (beginning at the start-time), and (if 2 or more) the time-gap you want between the sound recordings.

Set the length of the sound recording (in seconds).  
The duration can be between 1 and 20 seconds.

Then click on the Save button to generate and store the command.

Note: Once a scheduled recording program is finished, the flag changes within the logger from “pending” to “off”.

## 9.3 ALARMS AND FAULT CONDITIONS

Alarms from HWM loggers can generally be categorised into one of two groups:

- Logger generated “channel alarm”  
(alarms when channels measurements go outside of a desired range. These are under user-control ... the user has to set them up).
- Logger internal “system alarm”  
(generated by the logger software; no user-control).

### 9.3.1 Channel alarms

Some HWM loggers with leak-noise sensors support the sending of a “channel alarm” type of alarm from the logger when the logger detects a new leak, although it is rarely used.

This is activated or de-activated using the Alarm Settings tab of the site pop-up box.

Note: **The PermaNET SU does not support channel alarms.**

Any use of this tab in the pop-up box will generate and store a command, but it will be ignored by the logger.

New leaks must be handled using the PermaNETWeb web-pages (e.g. map display).

### **9.3.2 System Alarms**

The PermaNET SU supports the generation of internal system alarms (e.g. logger sensor fault detected, logger battery low). The logger sends any system alarm conditions in as part of its communication when it calls in to Datagate.

### **9.3.3 Pipe Leak detected**

Suspected pipe leaks are handled as channel data rather than an alarm. The leak-state of sites can be displayed on various PermaNETWeb pages including a map of sites, where the site icon is colour-coded to show leak / no-leak conditions.

Suspected leaks should be investigated.

### **9.3.4 Logger fails to call-in with data**

A logger can fail to communicate with Datagate for a variety of reasons:

- The battery is dead.
- The site has been tampered with and the logger antenna has been removed.
- The site is flooded.
- Maintenance is being done on the mobile network.
- The SIM card has no credit left.
- An object has been placed on top of the chamber.
- Water has got into the logger or antenna.
- Vermin have entered the chamber and changed the installation positions.

A logger that does not contact DataGate can give no indication of what the fault is. DataGate however can monitor the site and indicate if there is an issue with data arrival. A site that has a logger that is failing to call-in is known as a “quiet site”.

Quiet sites can be displayed on various PermaNETWeb pages including a map showing where the sites are. Also it can show when a logger of a site last called-in.

Quiet sites should be investigated if they persist.

## 10 REMOVAL OF A LOGGER FROM A SITE

An activated and deployed logger will continuously send in measurement data for a site. Later there will be a requirement to remove the logger from the site. This could be for a variety of reasons:

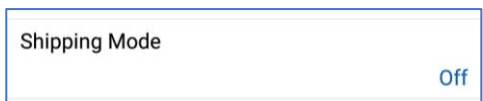
- Use of the logger at that site is no longer required
- The logger requires maintenance
- The logger is being swapped with another unit.

The logger cannot be simply physically removed from the site, as it will still continue to make measurements and attempt to send in data. It has to be properly “shut-down”. This will prevent possible damage to the logger and also prevents excessive draining of the battery.

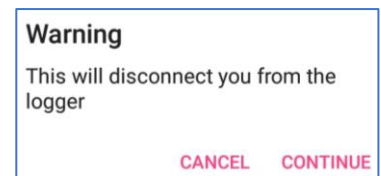
Use the following procedure:

1. Log into IDT (See section 5.2).
2. Activate the Bluetooth-compatible link and connect to the logger (See sections 4 and 5.3).
3. Navigate to: Configure Device → Device Information.

4. Find the “Shipping Mode” setting.  
This will currently be “ Off ”, since the logger has been activated.



5. Tap the Shipping Mode line.  
A warning box will appear. Tap “Continue”.  
This action instructs the logger to go into shipping mode.



Shipping Mode stops the logger from making measurements and also the calling-in functions.

The logger will use minimal power until it is re-activated. This is ideal for storage.

6. The antenna can now be disconnected from the logger, if required.

The Permanet SU logger contains sensitive transducers that can become damaged if incorrectly handled. Store the loggers in the original packaging or in a manner that does not risk damage. Refer to the “Safety Warnings and Approvals Information” document supplied with the logger for guidance of storage conditions.

### Re-Deploying previously used loggers:

Following the above process will leave the logger unchanged in the DataGate system, with the logger still deployed on site. The logger will show as a “quiet device” on any map views. These loggers may either be un-linked from the sites by office staff, or left.

When re-deploying the logger, follow the same process as normal, except that when choosing the “Installation type” select “Lift & shift”. This will remove the logger from the existing site (without modifying its location) and deploy the logger to a different site.

#### Installation type

New install

Lift & Shift



## 11 SERVICE AND REPAIR

---

### **Antenna.**

- Only use antenna recommended and provided by HWM.
- For details of antenna options and part-numbers to order, refer to the following link:  
<https://www.hwmglobal.com/antennas-support/>

### **Battery.**

- Only use battery and parts recommended and provided by HWM.
- Batteries are replaceable by a HWM approved service centre or relevantly trained technician.

### **SIM-card.**

- SIM-cards are replaceable by a HWM approved service centre or relevantly trained technician.
- Only use consumable parts recommended and provided by HWM.

When returning product for investigation or repair, be sure to follow the instructions of your distributor to document why the product is being returned.

If returning to HWM, this can be done by completing the on-line RMA form:

<https://www.hwmglobal.com/hwm-rma/>

Refer to the Safety Warnings and Approvals Information for guidelines of the packing requirements.

## **12 TROUBLESHOOTING**

---

### **12.1 THE USER CANNOT LOG IN**

- Ensure the correct server URL exists (Test connection).
- Ensure the correct user-name and password are being used.
- Ensure the user is correctly set-up on DataGate.

### **12.2 THE IDT APP DOES NOT LIST THE LOGGER**

- The logger is sleeping (or has not been activated), or the Bluetooth-compatible link is in standby.
  - Wake the logger or re-activate the link using a magnet.
- The logger is not correctly registered on DataGate
  - Refer to sections 2.5.1 and 8.1.
- The user is not logged into the app, or the initial synchronisation is incomplete
  - Refer to sections 5, 7.1 and 7.3.
- The user does not have the appropriate DataGate permissions
  - Refer to section 8.2.
- Try selecting “show insecure devices”. If the logger appears listed in red it is functioning correctly in “insecure mode”.
- Try re-starting the phone and the app.
  - Confirm the app Bluetooth connection is working correctly by waking and trying another logger.
- The battery may be flat or the logger may be defective.

### **12.3 THE DATA FROM THE LOGGER DOES NOT APPEAR ON DATAGATE.**

- Ensure the logger uses the correct data destination URL and port-number for your server.
- Make a Call Test and confirm OK.

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



©HWM-Water Limited. This document is the property of HWM-Water Ltd. and must not be copied or disclosed to a third party without the permission of the company. Copyright reserved.