User Guide: IDT (app for mobile devices)
- Logger User Interface.

HWM IDT

Warning:	
⚠️	Please read, understand, and follow any instructions in the relevant manual for your logger or that were shipped with the equipment.

TABLE OF CONTENTS

1 PART1: ----- INTRODUCTION -----

1.1 DOCUMENTATION AND SUPPORT

IDT is available in two versions: IDT (PC version) and IDT (app for mobile devices). This user guide covers the latter. Any subsequent reference to "IDT" within this manual will refer only to the mobile app version.

IDT is currently available on mobile devices employing the Android and also iOS operating systems (from the Google and Apple corporations respectively).
Where the manual uses the phrase "mobile phone", it implies the use of any mobile / cellular device with suitable functionality.

This manual uses screenshots from an Android-based device. Some small differences in appearance or operation may exist between Android and iOS devices. The user interface uses controls that are widely used on each device; the user should find familiar.

Note: The system periodically has new features and changes released, thus you may observe slight changes in pictures from those shown in this manual.
Most users will be able to automatically download updates of the app from the usual app download servers.

HWM provides support by means of our customer support webpages:
https://www.hwmglobal.com/help-and-downloads/

Should you have any questions that are not covered by this manual or the system's online help, please contact the HWM Technical Support team on +44 (0) 1633 489479, or email   cservice@hwm-water.com

Most HWM logger devices supported by the app will have some similarities in the setup process. For the purpose of providing an explanation to accompany a description of IDT settings, the document will refer to a non-specific, typical, generic logger device. Many HWM loggers will operate in a manner similar to the descriptions provided. Other HWM equipment will have been designed for a specific purpose and will have certain IDT settings that are only relevant for that purpose.

1.2 LOGGER DEVICES SUPPORTED BY THE IDT APP

The IDT app can be used with the following logger families:

- COMLog2-IS
- ISLog
- Permanet-SU
- StopwatchGSM

1.3 SYSTEM OVERVIEW

The IDT app (Installation Diagnostic Tool) is installed onto a mobile phone, or similar device. It uses a Bluetooth-compatible radio link to communicate with compatible HWM logger devices. The app provides a graphical user interface for the purpose of Setup, Installation, Diagnostics, and Testing of a HWM logger.

HWM logger devices produce data. The logger is often deployed to a site with the intention of it interoperating with a central server for the purpose of storing data centrally; the server acts as a data receiver and data warehouse.
HWM provides software for this purpose, for example the DataGate server software. Other servers can be set up using HWM software as the front-end to act as the receiver and decoder of logger messages.

If logger data is stored on a central server it can be integrated with other server software that provides the ability to view the data. This provides the ability for the viewing platform to present the data to the user in a more meaningful way than just tables of raw data.

e.g. HWM provides the following web-based viewing platforms:

- DataGate   (includes a General-purpose graphical data view)
- PermaNETWeb (monitoring for potential water pipe leaks)
- PressView   (water Pressure Reducing Valve performance viewing website)
- SpillGuard   (monitoring system for potential water spills / floods)

A server usually has to be prepared to receive data from the logger device and can make the received data available to other users who are authorised to use the system. The central server can similarly provide an authentication service to the IDT app in order to verify that a user is registered on the system and has suitable permissions to access the settings of a logger.

Alternatively, the user can view logger data locally using app and the mobile phone display, but features are limited in comparison to use of a logger device with a server.

Logger devices are normally partially pre-configured for use within the factory, with the user occasionally having to make limited on-site adjustments. (Discuss any requirements with your HWM representative prior to ordering). IDT can provide access to many, but not all, device settings. Some settings are exclusively factory set.

The data-warehouse often operates on the principle of a logger being installed for a time period onto an installation site. i.e., It is site-based.
The links that bind a logger to a site can be manually configured (by an administrator) or partially automated by the use of another app by the installer (e.g., the HWM deployment app).

1.4 LOGGER – TYPICAL OPERATION

A typical logger device will behave as follows:

The logger's main task is to make periodic measurements and store the results. In addition, the logger will have daily tasks at set times, such as uploading its un-sent data over the internet. When sending data, the logger waits to receive confirmation from the server that the data was received without error; If confirmation is not received, it will re-send the data at the next call-in time. The task of logging does not stop during any communications.

The logger usually includes an interface (referred to as a modem) that provides access to the internet via the cellular mobile communications network. A SIM card is used to give access of the network. Setup of the logger for use with the cellular network and SIM card network provider is required, as is the availability of a suitable signal from the network.

Most loggers are powered by a non-rechargeable Lithium battery, which implies their service life is limited before the battery has to be replaced. The installer should bear this in mind when making any changes to settings; keep tasks to the minimum required in order to give best battery life.

Most logger devices are shipped from the factory in an inactive state to preserve the life of the battery and will require activation during installation. Once activated, the logger will go into the state of "Recording" and begin repetitive logging of the various sensors fitted to the unit, according to its configuration and settings.

A typical logger can operate using two periods, known as the "sample period" and also the "log period". It will periodically sample the sensors at the *sample rate* to create temporary measurement samples. After taking several measurement samples, some statistical functions can be optionally applied to produce a *datapoint* that is logged (saved) at the *log rate*; these form the recorded (logged) measurements. The log period is always a multiple of the sample period.

The datapoints are stored in the memory of the unit. At a set time, the unit calls into the cellular data network in order to contact the server; the data is then uploaded.

The logger makes measurements (as described above) which are saved into an area of memory which is referred to as the "primary recording". In addition, if the logger has the feature enabled, it can also be set to occasionally save data into a "secondary recording" memory area (e.g. data sampled at a higher frequency). This is additional data.
(Note: This is not available on all supplied units and must be arranged through your sales representative before placing an order; it also has implications concerning expected battery life of the unit).

The logger can be programmed to monitor data for certain patterns or conditions and can send a message to the server if it should detect a match. Commonly, this is used for setting a condition that can be an indication of an "alarm". Alarms can be sent to a limited set of users, but a better way of handling (and preserving battery power) is to send the message to a server only if it has the facility to fork the message and send it to multiple users.

1.5 LOGGER SECURITY: SECURE AND UNPROTECTED MODES

At the time of leaving the factory, the loggers will be pre-configured to the requirements of the customer, including any *security settings*. The logger can include a setting that determines whether it operates as either a "Secure" or "Unprotected" device. The loggers can communicate their security requirements to the IDT app. The setting will influence the cooperation of the device with the HWM IDT tool.

When required, this manual will refer to a logger as being either a "secure" or "unprotected" logger.

The "Secure" mode restricts unauthorised users from making changes to the logger settings and or accessing logged data.

Secure loggers:

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

Unprotected loggers:

- Do not require registration on the DataGate server to be used with IDT.
- Can be connected to and have settings modified by anyone with the IDT app. (The user can implement a measure of security by programming the device with a user-defined PIN number; Factory default units need no PIN to gain access).

Loggers set as "secure" therefore require DataGate (or a compatible server) for IDT to operate with them.

1.6 ACTIVATING THE COMMUNICATIONS LINK

The logger will include a Bluetooth-compatible radio interface, used for short-range communication. The IDT app similarly utilises the Bluetooth radio interface of a mobile phone for communications. No communications cable is required.

For the IDT app to communicate with logger devices, both ends of the Bluetooth-compatible communications link must be active.

Refer to section 2.4 for details regarding activating the mobile phone side of the link.

Since the radio interface uses power but is infrequently needed (it is only required when someone is attending to the logger on-site) it is normally on standby and has to be activated for temporary use. Refer your logger user-guide for specific details.
If communications is lost during the use of IDT it may be due to the logger deciding the radio link is no longer being used and putting it back into standby; Re-activate the link if required. Another explanation is that the mobile phone is out of range of the logger, and the installer should keep the two devices closer together.

Where several loggers are within radio range, the user will need to select one using IDT.

1.7 PREPARING A MOBILE PHONE (OR SIMILAR DEVICE) FOR USE WITH IDT

The HWM IDT app is available for both Android and iOS-based mobile devices.

The examples used in this guide will show an Android device, but similar methods, views and behaviour will exist using an iOS (Apple) device.

The mobile phone must have Bluetooth-Low-Energy (BLE) compatibility, GPS, and Internet capability.

1.7.1 Installing the HWM software (IDT and HWM Deployment App)

The mobile device must be prepared for use with ISLog loggers by installing the HWM "IDT" mobile phone app.

On an Android device, open the "Play-Store" application.
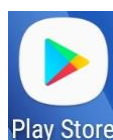
Search for "HWM global".

A list of available HWM applications will be shown.
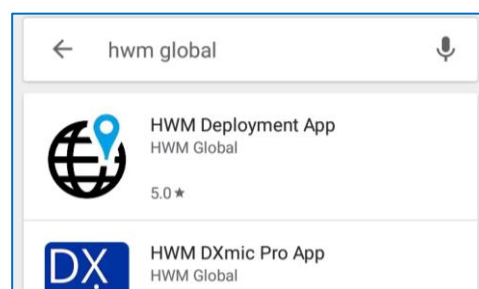
Select "IDT" and install it.

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

"IDT" is the "**I**nstallation and **D**iagnostic **T**ool" for various HWM loggers.

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

On an 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.
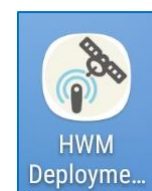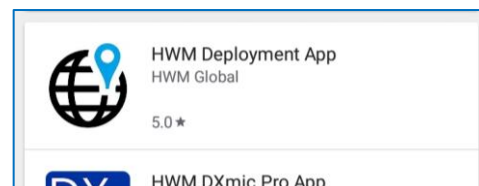
Note: Further information can be found in the user-guide for the Deployment app.

For iOS-based devices, use the Apple App store to obtain the above two apps.

1.8 LOGGER CHANNEL TYPES AND DATA INTERPRETATION

The IDT app has an *adaptive user interface*. For example, although it can be used with several types of logger, it recognises the type that it is communicating with and adapts the content of its screens so that it presents only relevant options to the user. Similarly, it presents only options that make sense based on any previous setup selections.

A typical logger model family may have many possible configuration options, but only certain options will be fitted for a customer order. These will have the appropriate electronic interfaces, including any connector options built into it during manufacture of the device.

Some electronic interfaces are multi-purpose in nature. The logger has to use an appropriate software driver to make an interface work. The combination of both an electrical interface and a software driver put together form a "channel type". During manufacture, the logger will include (factory-only) settings that define what channel-types are built into the unit. IDT uses this information to adapt its display to show only relevant and sensible options to the user.

Sometimes an electronics interface can support one of a several types of channel (each requiring a different driver). The user can make one selection from the set and IDT will subsequently exclude the other options from being available; the interface use has been already committed.

When the logger makes readings from an interface, it obtains data. Data is simply a numeric value. The logger can have one or several interfaces producing data. IDT provides a means to identify a specific stream of measurement data; this is done by assigning a "channel number" to each data stream.

The installer (as part of channel setup) also has to set the logger to interpret the data into its real significance (i.e., what each measurement represents).

Steps for channel setup to measure from an interface and save data will include:
(IDT can be used to make or check the required settings).

- Assigning a channel number and channel type for an interface.
- Setup the logger to be able to interpret raw data from a channel into its real-world significance (including any calibration requirements).
- Determining how often to make the measurement, and if any mathematical operations should be applied to the raw measurement data
  (e.g. averaging several samples).
  This will create "data-points" (the values saved as logged data).

Note: The logger will usually have settings pre-programmed by the factory prior to shipping. However, the installer has responsibility for confirming the settings are appropriate for use at the installed site.

If you have specific requirements this can be discussed with your HWM sales representative at the time of ordering the loggers.

2 USING THE IDT APP / MODES OF USE

2.1 IDT – USER-LEVELS

IDT can be set to various user-level "views" including:

- "Basic" (no user-level is shown on the display).
  … This gives basic details and is sufficient for most uses.
- "Advanced" ("User level: Advanced" appears on the display).
  … Additional options are available for advanced users.
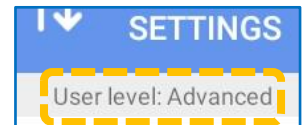
Both user-levels are available and can be selected within the app from the Settings screen.

To change, navigate to the settings screen and tap the line.
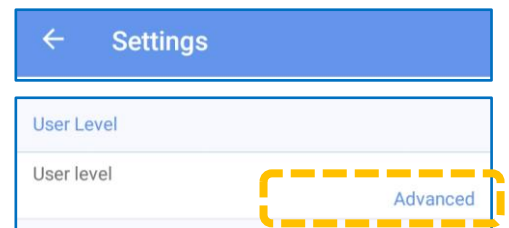
2.2 IDT - MODES OF USE

IDT may be used in two modes of operation:

- Operated in conjunction *with* the use of the DataGate server.
- Operated *without* the use of the DataGate server.

Using IDT *in conjunction with the DataGate server* adds certain requirements for use and gives the user access to the comprehensive functionality of IDT, including:

- The user is required to authenticate themselves with a username and password.
- An internet connection is required initially for the authentication process and also at other times for communication to the server.
- The user is given the ability to manage secure loggers (as well as unprotected loggers).
  (Also requires that the User and loggers have been setup on DataGate correctly to give the required permissions, such as logger ownership).

Logging in gives the app a token which enables IDT to be used for up to 48 hours, after which the user is required to log in again.

A list of the loggers you have permission to access to is also transferred at login time; this is also required for the HWM Deployment app, in order for it to record changes in the logger location into the DataGate database.

Using IDT *without the DataGate server* removes access to some of the capabilities of IDT:

- The user is not required to authenticate themselves with a username and password.
- A regular internet connection is not needed since there is no communications from IDT to any server during use.

(IDT requires occasional internet connection for obtaining any updates, including obtaining updates for the logger firmware).

- The user will be unable to manage or access the data of secure loggers.

2.2.1 Use of IDT without Logging in

It is possible to use IDT without going through the login process, but restrictions will exist, (see also section 2.2). It will not be possible to see any secure logger, only unprotected ones. It will not be possible to go through the deployment process using an app without logging into DataGate.

After the initial splash-screen (which shows the IDT logo), the user will have the option to either log in or select to use the app without DataGate. This can be done by clicking on the link to "Log in without DataGate". Once this link is activated, the app will, in future, bypass the "Log In" page.
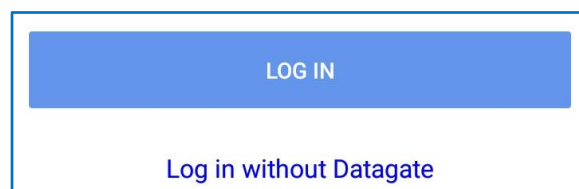
Note: Bypassing the log-in page still allows app communication with unprotected loggers. These can be set to communicate with DataGate if so desired.
It is simply *the app* that does not communicate with DataGate.

If you have selected this option, skip to section 2.3.

2.2.2 Logging in and initial actions

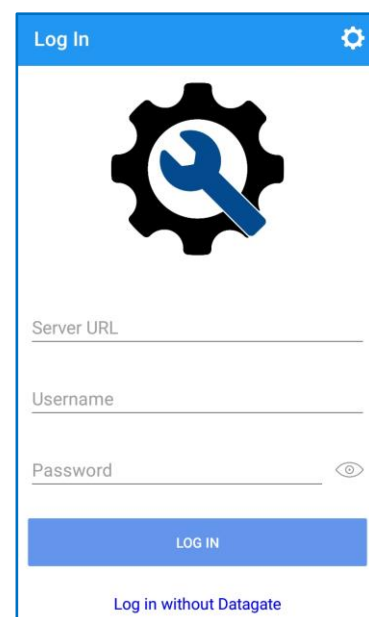Locate the IDT icon on the phone and launch the app.

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. (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 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.

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 have to be previously entered into the DataGate system).

2.3 DEVICES (INITIAL SELECTION SCREEN)

If login and authentication was successful, the app will show the "Devices" window.

(This will also be shown if you have previously selected to use the app without DataGate, as in section 2.2.1).

("Device", as used by the app, means "logger device").

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

(The menu contents can vary).

13

2.4 SELECTING A LOGGER DEVICE

Select a logger and ensure its communications link has been activated (see section 1.6). The logger broadcasts its presence over the Bluetooth compatible radio link.

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

- Bar-code scan (automatic selection) … see section 2.4.1.
- Bluetooth scan (manual selection) … see section 2.4.2.

2.4.1 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.
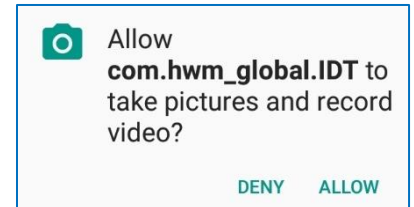
The phone's camera will activate, and the phone will display what is within its view.

Locate and view the logger barcode using the camera. The red line in the displayed image should be 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 starts a scan and looks for Bluetooth-compatible devices in the area.

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

If the logger device is not discovered, an error message is displayed. (The phrase "re-swiping device" means to re-activate the logger's communications link).

Follow the guidance message and then tap OK.

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

When successful, the identity of the logger is shown, along with controls to access various options.
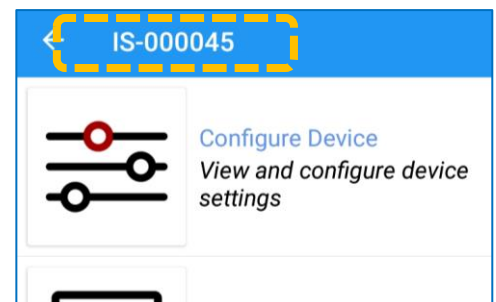
This is the main options page.

Could not connect to device

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

OK

Could not connect to device

IS-000045

Configure Device
View and configure device settings

The IDT app automatically communicates with the logger and obtains its configuration and settings.

(Skip to section 2.5)

2.4.2 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 logger devices found. The scan can pick up several types of logger, as long as they are within communications range.

Your logger can usually be identified by comparing with information on its label (e.g., serial number).
If your logger is not listed, try re-activating the logger communications link.

Devices ⚙ ⋮

▯▮▯▮ Barcode Scan   ✳ Bluetooth Scan

Please ensure that the device you wish to connect to is awake.

Barcode Scan   Bluetooth Scan

IS-000045   ▪▫▫▫

If you are not using DataGate:

- All loggers you have access to appear in black text.

If you are logged into DataGate:

- Secure loggers that you own are listed with black text.
- Unprotected loggers that you "own" (on DataGate) are listed with red text (providing "show unprotected devices" is selected from the local menu).
- Loggers that you do not own are not listed.

15
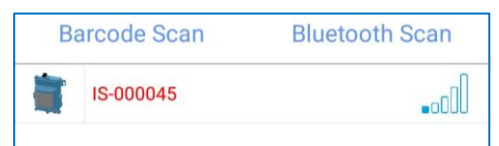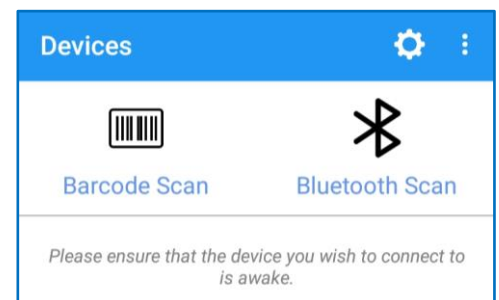
Note: Use of the options control gives the ability to *show details*: MAC address (Android only) and dBm.

Confirm (using the serial number) the correct logger device is listed on IDT.

Tap on the line to select it. IDT will connect with it.

The identity of the logger is shown, and IDT displays some graphical controls that give access to the various options.

This is the main options screen.

The IDT app automatically communicates with the logger and obtains its configuration and settings.
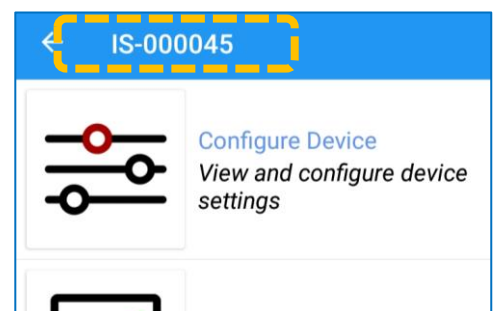
2.5 LOGGER FIRMWARE UPDATE

New software releases (firmware) for loggers are occasionally released from HWM.

Before reaching the main options page, IDT automatically checks the existing logger 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.
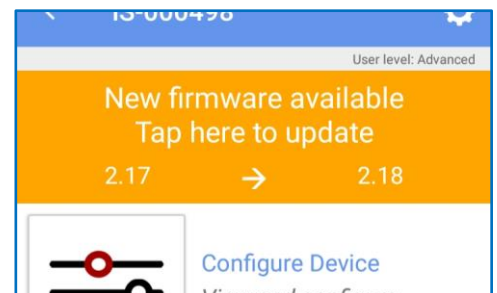
Progress is shown.
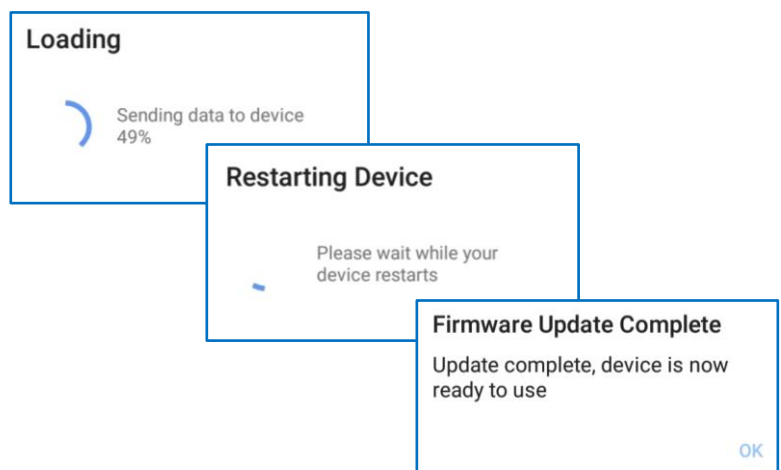
... Until the upgrade is completed.

The main options screen is then shown.

16

3 IDT – MAIN OPTIONS PAGE

The main options page is shown below.

This page functions as a menu. Selecting an option on this page will open up a new sub-page with further options.

Controls are displayed for the user to select how they wish to use IDT app:

Configure Device:
The user can use the app to check the device configuration (settings) or re-configure the device.

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

Logged Data:
The user can access measurement data held within the logger device.
(Access is temporary; data is not stored by the app).

Firmware Selection:
The user can modify the device firmware.
(Roll-back is rarely used, only if advised by HWM)

Deploy Device:

Note: This option is only available when IDT is used with DataGate.
Tapping the Deploy Device option will launch the HWM Deployment app and passes details of the logger to it. The user is able to record the installation location of the device.
(The HWM Deployment app is used to complete the task of selecting the site of deployment and an administrative update of the DataGate system).

.

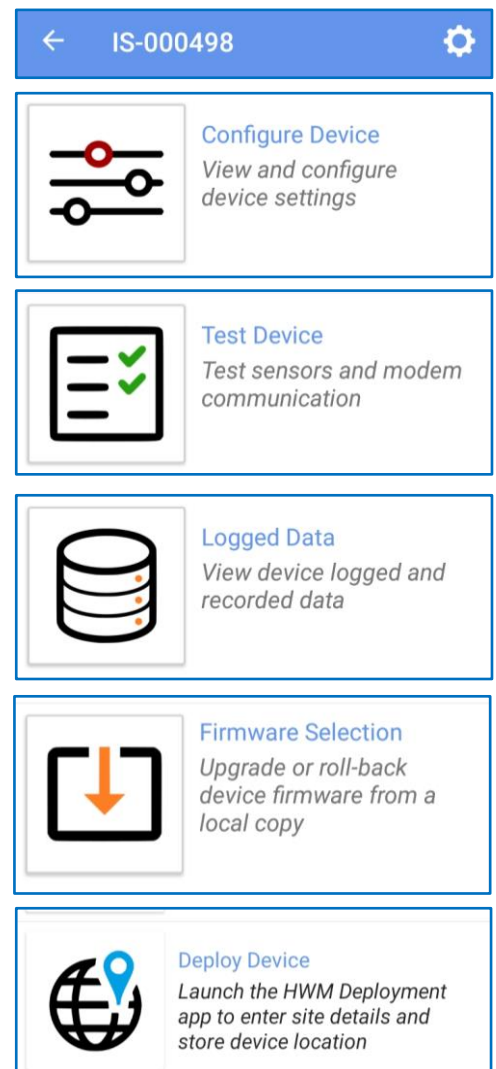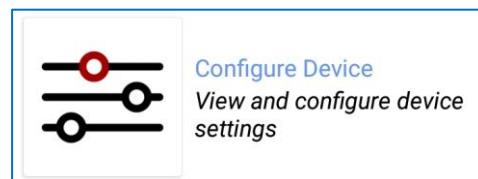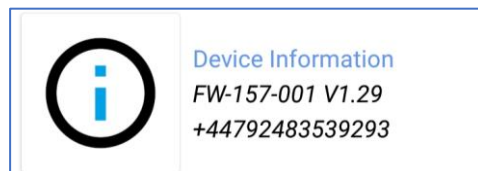## 3.1 DISPLAYING LOGGER DEVICE INFORMATION

3.1.1 ID information / Telephone number (SMS)

From the main page, tap on the "Configure Device" selection.

A new menu page will open with various configuration options. Select "Device Information".

A new page will open with a read-only area showing various logger parameters, including the firmware version, serial-number, and its current time.

The refresh symbol on this page updates the displayed Logger Time.

The "Editable settings" section allows the user to:

- (Optionally) input a unique identifier in the ID field, up to 32 characters.
- Modify the "Telephone Number" of the logger.
   Note: This acts as an identifier of the logger to the DataGate system, so **caution** should be taken.
   Only modify this field if advised by HWM.

This number is not read from the SIM card but has to be independently programmed into the logger memory.
It should match the number that appears on the logger front-panel label, (see example opposite).
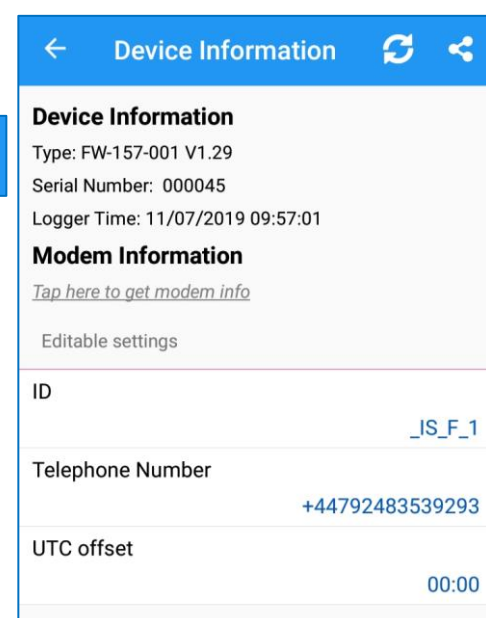
The telephone number is usually pre-programmed into the logger by HWM prior to shipping and should remain unchanged. This is the case even if the SIM is changed.

3.1.2 Time-zone (UTC offset)
The logger communicates to DataGate using the global time reference, (called "UTC"; Coordinated Universal Time; it is similar to Greenwich Mean Time, GMT).
IDT allows the user to program loggers using local time. The logger needs to know the offset of the local time zone from UTC so it can communicate the correct timestamps for data to the server. This can be set by the user by tapping the "UTC offset" line.

When a user adjusts the UTC offset, the setting does not *immediately* change the displayed "Logger Time". The update only takes effect after the logger next calls into the server; the server then changes the logger's time. This allows the server to be able to correctly interpret logger timestamps during any UTC offset change.

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

3.1.3   Logger mode / Security PIN

The "Mode Settings" area contains miscellaneous controls that affect device operation.

Device Mode should be "normal"; this is unavailable to edit for most users and is password protected.

Shipping mode is used to render the device inactive and is used for shipping the unit and for long term storage. (Refer to section 5.1).

Device PIN gives the user the option of setting a user-defined PIN on an Unprotected device.
Tap on the line if you wish to set a PIN.
The PIN can be up to 8 characters in length.
Once set, IDT will not allow access to the device without a valid PIN being entered.
If you forget the PIN, the device can only be recovered using a HWM Master PIN; the PIN is unique to each device.

Mode settings	
Device Mode	Normal
Shipping Mode	Off
Device Pin	Disabled

Device Pin
CANCEL   OK

3.1.4   Modem Information

Modem details can be shown by tapping the "... get modem info" line.
These can be forwarded to expert users for assistance by tapping on the share control.

Modem Information
Modem: GE866-QUAD
Firmware: 16.01.200
IMEI: 356850083066769
IMSI: 204043807139293
ICCID: 8944538531002822936
CSCA: "+316540791031",145

3.2 DISPLAYING / EDITING CALL-IN SETTINGS

From the main options page, tap on the "Configure Device" selection.

Configure Device
View and configure device settings

A new page will open with various configuration options.
Select the "Call Settings" option.

Call Settings
mobiledata
inbound.hwmonline.com: 23024

The current call settings of the logger will be displayed.

Tap on any line to change the setting; the change is made to the logger immediately without having to confirm it.

The page is divided into 4 areas of settings (1 for IDT in "Basic mode"):

- Call-in settings (also available in Basic mode) ; Refer to section 3.2.1.
- Data Destination settings   ; Refer to section 3.2.2.
- SIM settings   ; Refer to section 3.2.3.
- Modem settings   ; Refer to section 3.7.1.

19

3.2.1 Call-in settings

The Call-in settings for an IDT user-level of Basic are shown opposite.

←	**Call Settings**
Call-in Settings	
Call Mode	Frequency
Call Frequency	01:00

Additional settings can be accessed at a user-level of Advanced.

Continue to call in when there is no data to send	No
Fast call rate (min)	

⋮

The Call-in settings affect when the logger calls in with measurement data.

Note: These settings should be carefully chosen since every call-in uses some power from the battery.
To prolong battery life, keep the number of call-ins per day minimal.
3 calls per day (maximum) are recommended.

IDT provides some warnings and restrictions to limit very excessive call-levels being set by a user (e.g. at hourly intervals or less).

> Warning: setting too high a frequency can have a serious impact on your loggers battery life
>
> **OK**

Call mode:

- Select "Time" to have the logger call-in at fixed times.
  (Then set the required call times).
- Set to "Frequency" to have the logger call in regularly after a set period of collecting measurement data.
  (Then set the required period between calls).

Continue to call when there is no data:

- This should usually be set to "No"; It is to save battery power.
  It takes effect when measurements are made infrequently; if there is no new (or unsent) data then do not call in.

←	**Call Settings**
	User level: Advanced
Call-in Settings	
Call Mode	Time
Call Times	07:00
Continue to call in when there is no data to send	No
Fast call rate (min)	5

If the logger is unsuccessful at the first attempt to call-in (e.g. the network is busy), it will re-try at the next earliest call time, until it is successful. A logger can send in data from several previous days if it needs to (e.g., if the data could not be sent because the site was temporarily flooded, and the antenna signal was degraded).

The selection method can vary according to what is call-mode details are being set (time or frequency). Tap on the part of the field you wish to change (i.e., hours or minutes), then make the adjustment.
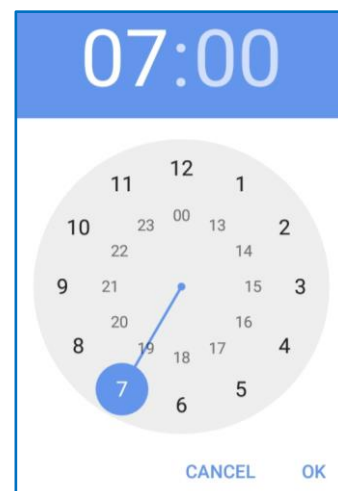
When the Call-mode is set to "Time":

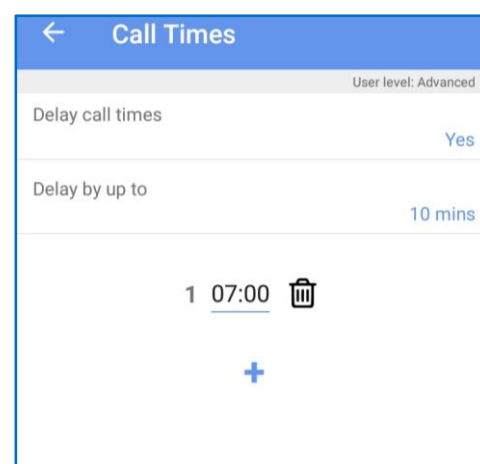- Controls are available to delay the Fixed call-in times by a short random time; this can be used to reduce the peak load on the server.
- Fixed call-in times can be added. (Logger has a typical limit of 8).
- Fixed call-in times can be deleted.

When the Call-mode is set to "Frequency":

- The logger calls-in at the chosen interval, starting at midnight.
- If less than 1 hour, the logger calls in hourly, and the minutes setting governs the time past the hour when the call-in is made.

3.2.2 Data Destination settings

- Set the URL (sever address) and port number as required for your server.
  (Check with your system administrator).
  (Settings shown are for illustration purposes only).
- The SMS backup number is the telephone number that the logger can use to send messages to the server. (Settings shown are for illustration purposes only).
  The SMS (text message) service is a fall-back connection path only used if the internet cannot be accessed for some time. Not all loggers or SIM cards support the SMS messaging service.

21

3.2.3 SIM settings

- Confirm the settings match those of your mobile-network data service provider.
- Edit any that are incorrect.
  (Settings shown are for illustration purposes only).

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.
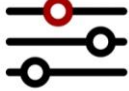
SIM Settings	
APN	mobiledata
APN Username	
APN Password	

3.3 TIMING INTERVALS FOR MAKING MEASUREMENTS

These settings determine what time periods the logger uses for its background activity of gathering data.

From the main options page, tap on the "Configure Device" selection.

Configure Device
View and configure device settings

A new page will open with various configuration options. Select the "Channels" option.

Channels
No: 1
Combos: 0

The "Channels" summary page is displayed.

Tap on the "Parameters" line, or the "Global Settings" link.

← **Channels**   ⇅ GLOBAL SETTINGS

User level: Advanced

Parameters

Sample Period:	Log Period:
N/A	00:05:00

Logged Channels

A new page is shown, called "Global settings".

Global Settings

User level: Advanced

Logging Parameters

Last start at 03/09/2020 09:30:00
Last stop at Never

The page gives details of when the logger was activated or last restarted.
(This is for information only).

Sample Period
00:00:30

There is a slider switch which determines if the logger "logs more than once per day" or conversely if it produces just a single log value in a day.

Log more than once per day

Log Period
00:05:00

Most general-purpose loggers should be set to log more than once a day.

Pulse Input Frequency

Pulse sample rate:
High Speed

Note: Where just once a day is selected, the user must program the time that the measurements are to be made and logged. (e.g. This is used in scenarios where the logger is being used with specialised sensor to run a daily test and log the result).

Log more than once per day

Logging time
09:30:00

The "Sample Period" sets the time interval between making measurements on most of the interfaces.

Sample Period
00:00:30

00:00:01	03:00:00
00:00:02	04:00:00
00:00:03	06:00:00
00:00:05 · · ·	08:00:00
00:00:10	12:00:00
00:00:15	1 Day

The value can be selected from one of the many available options.

The "Log Period" sets the time interval between storing values and is set in a similar manner to the sample period.

Log Period
00:05:00

The Log period must be a multiple of the sample period.
If the user does not select an appropriate value, IDT will automatically adjust the input.

The data value stored is known as a "datapoint", normally produced at the log period rate. The value is formed by (optionally) applying some mathematical function on a set of raw data measurements (made at the sample rate); the samples obtained between the log period intervals.

Loggers with a pulse collection type of interface (e.g. digital flow interfaces detect and count pulses output from meters) have to respond rapidly to the input signals.

Pulse input interfaces are therefore sampled at a much higher rate than regular channels and have their own setting for selecting timing.

Pulse Input Frequency	
Pulse sample rate:	
	High Speed

Select the most appropriate setting based on the expected maximum pulse rate and also the minimum pulse-width.
Where appropriate, battery life can be extended with the "power save" setting option.

Pulse sample rate:

High Speed (16ms min pulse)

Power Save (500ms min pulse)

3.4 CREATING A LOGGER CHANNEL

Note: Loggers are usually shipped from the factory pre-configured to the requirements of a customer order. The steps described here therefore only need to be followed for setup of a new channel or modifying existing settings.

As discussed in section (1.8), a channel requires:

- A way to identify the channel and its data-stream.
    (IDT gives the channel a "channel number" for this purpose).
- A "channel type" (electrical interface and software driver)
    (IDT uses "input selector" and "sensor type" for this purpose).
- A means of interpreting data obtained from the sensor.
    (IDT uses such things as "input multiplier" and "units" for this purpose).
- Settings to govern when and how datapoints are produced for storage.
    (IDT uses the "log period" and "Logging mode" for this purpose).

The actual fields that are needed are *dependent on the type of sensor* and what a measurement from it represents. This user-guide will therefore give an example of the considerations needed and steps taken to set up a *typical general-purpose* logger channel for a *simple sensor*. This is for introduction purposes only; many channels will follow a similar setup procedure. However, some loggers employ specialised sensors or algorithms which require further discussion. (Refer to section 6 for further details).

Note: A channel can contain:

- A stream of data measured *direct from the sensor interface*.
- A stream of *indirect data* derived the direct data stream.
    e.g., Meter pulses can be used to indicate consumption.
        Indirect data can be in the form of flow (when timed)
        or a calculated meter reading (if the initial meter reading is known).

The example is based on simple sensor that is able to detect if a switch is open or closed. These can be used for a variety of applications including detecting output pulses from a gas meter.

3.4.1   Example 1: Gas flow and meter readings

A gas meter pulse represents a volume of gas that has travelled through the meter. To interface with the meter pulses, the logger is required a *digital flow* input channel.

Note: This type of logger interface has many uses and could equally be set up to interface with water meters.
The wiring of the interface will not be considered here. However, it is important to know the characteristics of the equipment that the logger is being connected to, since flow meters can have several "flavours" of output pulse signals.
e.g.:
1. Uni-directional flow is represented by a single output from a meter.
2. Bi-directional flow is represented using two outputs from the meter, and therefore require two signals within the input to the logger.
This is handled by allowing the installer to select from several available driver options when setting up the channel.

A typical gas meter has uni-directional flow, with a single pulse output.

The rate of gas flow is derived from the pulses by requiring the logger to count the number of pulses obtained during a fixed interval of time; this is to be repeatedly logged.
A meter reading could also be obtained (if we also record the initial meter reading) by accumulating the total number of meter pulses.
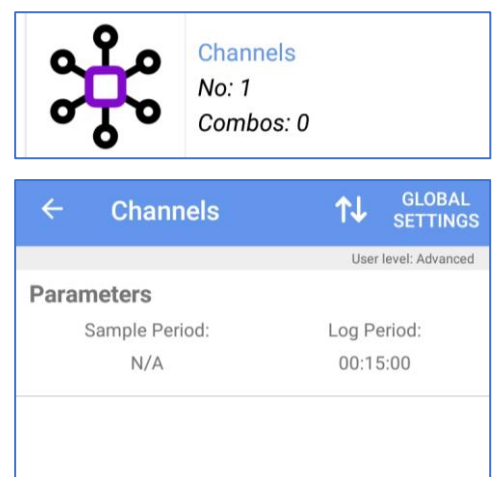
3.4.2   Setup of a new channel
Tap the Channels icon to begin setup of a channel.

A summary of any channels and trigger-action combos (discussed later) that are already configured is shown on the page.
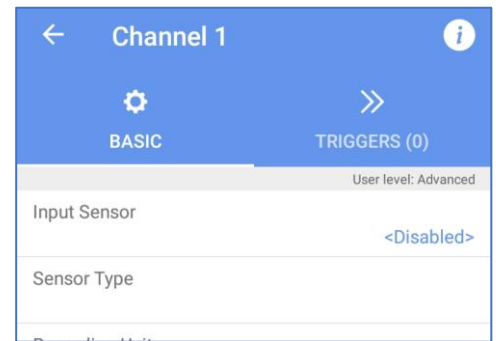
(Here, the list is empty).

Tap the " + " line to add a new channel.

The new channel is enumerated; here it is channel "1".

There are two tabs, select the "BASIC" tab.

Tap the "Input Sensor" line.
(Currently, it shows "<Disabled>"; it is unconfigured).

A pop-up selection box appears listing all installed sensor interface options.

e.g. The digital flow interface of this particular logger can handle a single bi-directional flow meter, or up to two uni-directional flow meters. These are listed as "Flow Bi", "Flow Uni 1.1", and "Flow Uni 1.2" respectively.

Notes:

- The list will vary according to logger model-number and also any requirements specified at the time of it being ordered.
- Selecting an interface for a particular use on one channel will remove some or all of the other options when the list is next produced.
  e.g., Flow1 Uni and Status1_0 cannot be used together; they share the same electronics; using one excludes the other from being available.
- The list will show available interfaces:
  Those that are not yet committed in the logger's current configuration.
  Those with a use already committed (which can be re-used).
- Selecting "<Disabled>" will delete any current configuration of the channel.
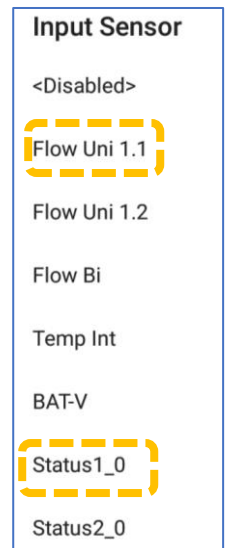
For this example, a uni-directional flow sensor is required.
… Select "Flow Uni 1.1" from the selection list it by tapping it.

The selection commits the electrical interface for use by the logger.
(i.e., The relevant pins of the connector are now committed for a specific use, as is the software driver being used).

In this example, the software driver will count meter pulses.

The selected Input Sensor is added to the field in the channel configuration screen.
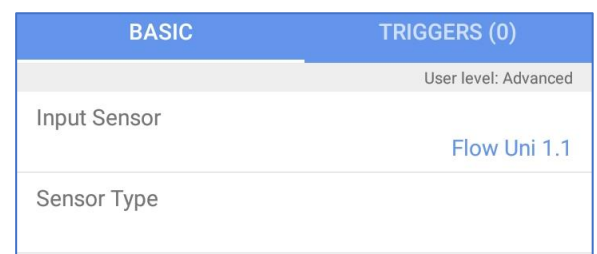
The software is now prepared to count pulses but has no idea of whether it is measuring the flow of electricity, water, or something else. The next steps are used to identify what the pulse count is representing.

Tap on the "Sensor Type" line.

A list of options is presented.

Select the type of measurement being made.
(In our example we are measuring gas. ... Therefore, choose "Gas").

Next tap on "Recording Unit"

Select a unit of measurement from the list.
(Units of measurement listed will vary according to earlier-made selections).

(In out example this has to match the units used by the specific gas meter installed. e.g., m³ for the example shown opposite).

A relevant calibration factor for a gas-meter is units per meter pulse. (Other types of equipment may require a different type of calibration factor).

Tap on "Units/Pulse".

This selects the pulse significance of the meter. Select the correct setting based on the equipment you have attached the sensor to.

e.g. If the meter pulse represents 0.1 m³ of gas, the units/pulse should be set to 0.1.

By repeatedly counting the number of pulses from the meter over a fixed period of time, the logger is able to determine the flow rate through the meter.

Next select the required logging mode.

Recording Unit	
	m³
Logging Mode	
	Spot

Logging Mode

Average

Min

Max

Spot

Time closed

Time open

Logging Mode

Minimum

Maximum

Spot

The available options depend on what is being measured.

For example, "Average" will produce a datapoint (logged data) that is an average of the measurement samples it has made since it last produced a datapoint.
(i.e. A new datapoint value is produced and saved to memory at the rate set by the Log period setting).

However, for a gas flow measurement, the options are less. (IDT presents only useful options based on previous selections).

For a gas flow reading, the channel should be set to "Spot".
The result will be the pulse count (i.e., total flow) since the last datapoint was produced.

BASIC	TRIGGERS (0)
	User level: Advanced
Input Sensor	
	Flow Uni 1.1
Sensor Type	
	Gas
Units/Pulse:	
	0.1
Recording Unit	
	m³
Logging Mode	
	Spot

The completed settings are now shown within IDT but have not yet been saved.

Tap the "ACCEPT" button. IDT will save the channel settings to the logger.

Then tap the "back" button.

← Channel 1

ACCEPT	CANCEL

The channel is now set up and will appear in the Channels list.
("1" shown here represents channel 1).
Datapoints will appear as the "Channel 1" data stream sent to the server.

Where multiple channels have been set up, they will all be shown here as a summary of their settings.

(To edit settings, tap on the relevant line).

Further discussion of setup of a logger for automated gas meter readings will not be discussed here, except to summarise:

- Because the context of the channel use is connection to a gas meter, additional options become available for a logger to be used in that application...
- The current meter reading can be taken and recorded in the logger as part of the setup of "meter readings" settings within IDT. It is linked to the flow channel.
- The logger may offer the ability to regenerate meter pulses on an output channel. This allows the pulses to be passed to other instruments using a logger output interface. Enable this feature if required.

For further information refer to section 6.7.

3.5 SETTING TRIGGERS AND ACTIONS FOR A CHANNEL

Once channels are set up, a steady stream of data is made by the logger at both the log rate and also (stored temporarily) at the sample rate. Trigger-Actions can now be created.

A "Trigger" is a monitoring function within the logger. It monitors for a single condition or combination of conditions to occur on the data produced by selected channels. If the condition(s) are met, the logger can be set to take one or more actions (e.g., inform the server of the event, thus indicating a potential alarm condition).

The conditions being monitored are referred to as a "Trigger" by IDT. Any subsequent action is referred to as an "Action" by IDT. The Trigger-Action(s) are sometimes referred to as "combos" (short for "Combination").

Within any trigger-action combo, either a *single condition*, or a *set of several conditions* can be used to evaluate the trigger result. Where multiple conditions are set, Boolean logic functions (AND or OR) can be applied.

This section will use an example of setting a trigger-action for a sensor.

3.5.1 Example 2: Introduction to Triggers and Actions

A channel has been set up, with samples and datapoints being obtained as summarised in the diagram opposite.

Trigger-actions are summarised with the number currently set within the logger being shown on the bottom line. The logger has no trigger-actions set, as indicated by "No: 0".
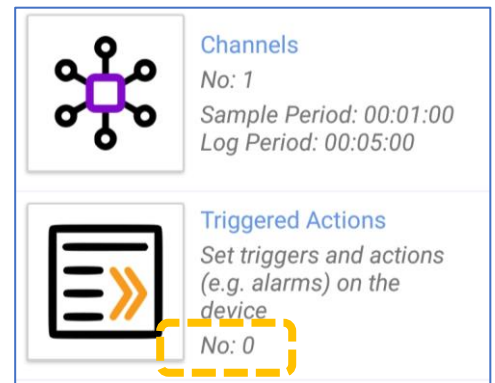
The requirement for our example is for a trigger to be setup, looking at the data from a sensor using channel 1, and used to inform the server (send an alarm message) for when the trigger condition is met. Similarly, we wish to inform the server (send an alarm clear message) when the trigger condition is no longer met. We require the trigger to be activated at a value of 50 or more and to be removed at a value of 40 or less. Both messages are required be sent immediately.
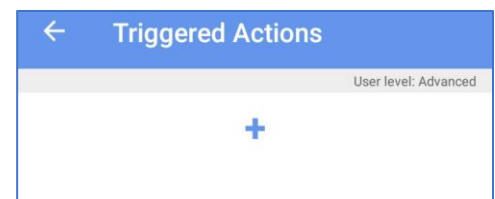
3.5.2 Setup of conditions for TRIGGER *start* and *end*

To setup the trigger action, tap on the "Triggered Actions" line.

This page summarises any existing trigger-actions.
It also gives edit-access to any listed action.
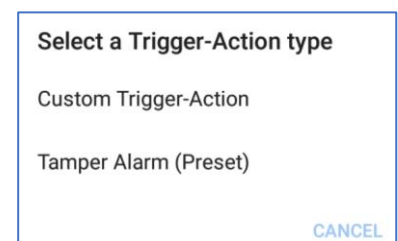(Currently none are set).

To add a new Trigger-Action, tap the " + " icon.
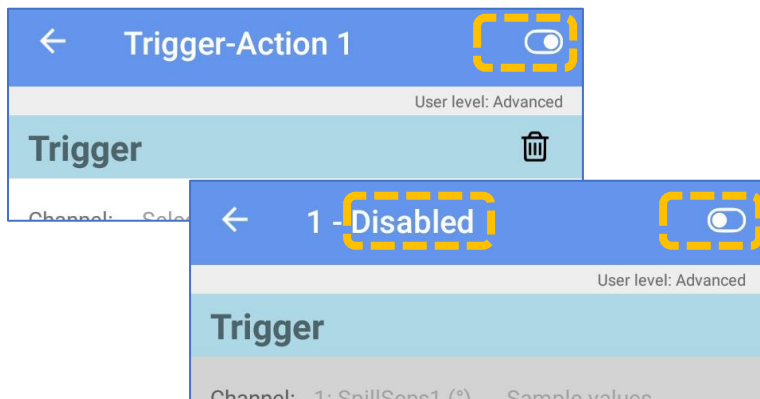
Then select a Trigger-Action type.

For our example, tap the "Custom Trigger-Action" line.

(Pre-set alarm types are also listed here but are not relevant to our example).

A Trigger-Action details page appears, which requires completion. Once completed, tap on "Save" to store the settings in the logger.

The slider-control at the top-right can be used to enable or disable a Trigger-Action.

Set the triggering conditions, as follows:

Tap on the location which currently displays "Select a channel".

A list appears showing all currently configured channels.

Tap on a line to select the required channel.

(In the logger used in this example, only one channel has been programmed; it is monitoring data from a SpillSens sensor, which produces angle measurement data).

The channel is selected.

The data values being watched are, by default, the Log values; this can be changed to the sample values if required.
(Tap on the value and make a new selection).

Tap on "Select a condition".

Select a condition to monitor for from the available list.

In our example, we wish to monitor for an angle exceeding 50°.
The appropriate selection is … Above 'A'.

Note: IDT display content is adaptive.
The list can vary according to the type of channel or other settings.

Add the appropriate value threshold(s).

In our example, we want to trigger when the angle is above the threshold of 50°.
The appropriate selection is … 50.

Tap on "Select a persistence".
Then select the type of persistence that is required before the trigger condition is evaluated as true.

Select a persistence
For ≥ 'C' of last 'D' samples
For greater than 'C' seconds
Between times 'C' and 'D'

Trigger-Action 1 — User level: Advanced

Trigger

Channel: 1: SpillSens1 (°)   Sample values

Above 'A'   A= 50

For ≥ 'C' of last 'D' samples   C= 1   D= 1

Hysteresis: ⓘ   0.0

Complete any other settings required for the persistence.

e.g.   The settings shown will meet the trigger condition on first time the angle is above 50°.

If you try to set an impossible situation, IDT will highlight the error (e.g., red text).

For ≥ 'C' of last 'D' samples   C= 2   D= 1

In our example, we want to trigger when the angle is above the threshold of 50 degrees for 2 out of 4 samples.
(e.g., We may have chosen to use persistence in order to disregard any transient "glitch" measurement conditions.
There is a side-effect to this that the trigger will be slightly delayed).

Trigger-Action 1 — User level: Advanced

Trigger

Channel: 1: SpillSens1 (°)   Sample values

Above 'A'   A= 50

For ≥ 'C' of last 'D' samples   C= 2   D= 4

Hysteresis: ⓘ   0.0

When selecting some trigger conditions, an additional field (hysteresis) is added.

Hysteresis can be used to provide a different threshold for when the logger releases from a triggered state. Thus, the logger trigger will **start** (or activate) when it first meets the triggering conditions, and it will remain *held in a triggered state* until it no longer meets the second threshold (determined by the hysteresis value); then the trigger will **end** (or clear).

The example shown opposite requires a minimum of 2 of the last 4 samples to exceed the angle threshold (A) to **activate** the trigger.
This requires between 2 and 4 measurement values to evaluate.

Once triggered, it will be held in its triggered state providing the holding condition remains True.

The evaluation for **holding** the triggered state is that a minimum of 2 of the last 4 samples is required to be over the release threshold
(i.e. A – hysteresis).
For the settings shown in this example, this is 40;
(A=50, Hysteresis = 10   ;   50 – 10 = 40).

If the holding requirement is no longer met, the logger returns to the normal (non-triggered) state.

3.5.3 Setup of ACTIONs related to a triggered condition

A trigger does not do anything on its own; actions should be linked to it in order to accomplish something useful.

To set an action that should begin when the trigger activates … tap on "ADD ACTION ".

(This is not required if only one action is needed).

ADD ACTION

Within the action area, tap on "Select an action".

Several options may be listed:

Logging a channel at a faster rate or calling into the sever more frequently will only occur whilst the in the triggered state.
Normal operation resumes afterwards.

Tap on the required action to select it.

In our example we want to generate messages to the server; these are also known as alarms … so select "Generate an alarm".

Select the required condition(s) that should be reported...

Note:
This control determines what messages get sent *immediately*, rather than waiting until the next scheduled call-in time.

The conditions are shown in the setup screen.

Action 🗑

Generate an alarm

Report alarm immediately   Never

Send 'alarm cleared' message ⚪   Report as tamper alarm ⚪

When "On activating and clearing" is set, the "send alarm cleared message" is also becomes selected. The server will therefore be informed of when the triggered state is activated and also when it is cleared.

Report contition

On activating

On clearing

On activating and clearing

Never

Action 🗑

Generate an alarm

Report alarm immediately   On activating and clearing

Send 'alarm cleared' message 🔵   Report as tamper alarm ⚪

(An alternative would be to report the alarm immediately "On activating", and to use the slider control to also send an "alarm cleared" message. However, with these settings the "alarm cleared" message would not be sent until the next scheduled call-in time).

Note: The "Report as tamper alarm" slider should be deactivated (greyed out); A tamper alarm is not relevant to this type of sensor.

Tap the back-arrow and a summary of the Trigger Actions is displayed.

(Additional trigger-action combos can be added if required, using the "+" button).

Tap the "Save" button to write the combo(s) into the logger memory.

← **Triggered Actions**

User level: Advanced

1 If **CH1** (SpillSens1) is above **50 °** for at least 2 of the last 4 readings
   -Then- generate an alarm 🗑

+

| SAVE | CANCEL |

When a channel is being monitored for a trigger-action combination, this will be shown in the channel summary page, as shown here.

← **Channels**   ↑↓ GLOBAL SETTINGS

User level: Advanced

Parameters

Sample Period: Log Period:
N/A   00:05:00

Logged Channels

1   SpillSens1 - Angle (°)
    Multiplier: 1 - Spot   ≫ x1

3.6 LOGGER AND SENSOR TESTS

IDT provides access to be able to test some of the logger interfaces and the functioning of attached sensors.

To access the logger test menu, tap on the "Test Device" line.

A new view will open with various test options.

(Signal Test and Call Test are tasks to be performed at the end of logger installation and are covered in section 3.7).

Tap on "Hardware Test".

A "Hardware Test" page will be generated.

The test requires an interface to be configured for use before tests can be made; a channel must be configured to use the interface. Often the sensor also needs to be attached.

The content of the test page will therefore depend on the logger model number (interfaces available) and configuration (settings).

Each of the interfaces that have been configured for use by a channel will be shown, along with some additional internal sensors.
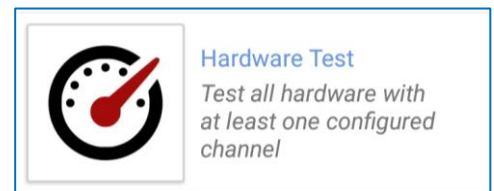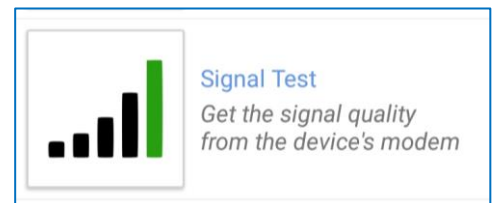
e.g. The diagram opposite shows a logger with Channel1 configured to use a SpillSens sensor.
The sensor is also fitted.

The hardware in this example can be tested by changing the position of the SpillSens digital float switch.
The example shows a sensor at 22 degrees from vertical; when the angle is changed the display will update to show a new angle; it can be proved to be functioning OK.

The display is updated at 1 second intervals (approximately).

Similar methods will exist for many other interfaces and sensors.
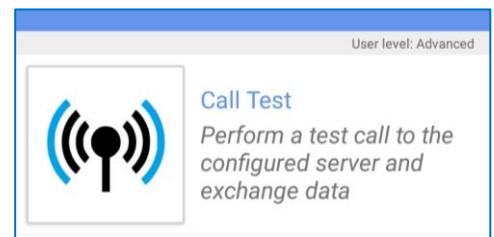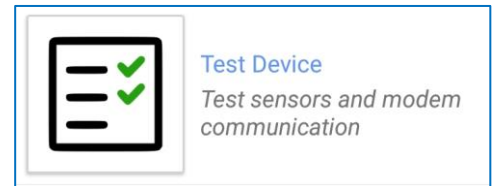
3.7 Cellular network setup - protocols and tests

The IDT app can be used to check that the logger can connect to the cellular network and provide information to help the installer to choose the optimal position of the antenna.

- Inspect or modify modem settings (if required).
- Perform the "Signal Test" to confirm the logger connects to the mobile network and find the best location of the antenna.
    - Note: The process is different for 4G networks in comparison with the 2G and 3G networks.
- Perform a "Call Test" to confirm the logger can communicate with the DataGate server.

3.7.1 Modem Settings

CAUTION: Most installers **should not modify** these settings (Skip to section 3.7.2 or 3.7.3); They are for expert use only.

(See section 3.2 for how to navigate to these settings).

The loggers have a built-in modem circuit for connection to the cellular network. Depending on the part fitted, IDT can show a different content of control settings within the "Modem settings" section.

e.g. No setting options, shown opposite.

Modem Settings	
Modem Type	GE866-QUAD

or …

e.g. Many setting options, shown opposite.

These settings are normally best left at the factory default, unless you understand cellular mobile technologies.

For those that do understand cellular mobile technologies, the controls are available to use if you are aware of the SIM capabilities and also the radio services available local to the installation site.

Modem Settings	
Modem Type	ME310G1-WW
Network Type	2G & 4G
4G Tech Type	LTE-M → NB-IoT
4G Band Selection	B8, B20
2G Band Selection	GSM 850MHz + GSM 900MHz + DCS 1800MHz + PCS 1900MHz
Operator Lock	None
DNS Mode	Mode 1

Network Type setting determines which network generation should be used to establish a connection.

2G
4G
2G & 4G

4G Technology Type setting determines which network generation should be used to establish a connection.

LTE-M
NB-IoT
LTE-M → NB-IoT
NB-IoT → LTE-M

4G Band Selection setting determines which frequency bands can be used to establish a 4G connection.

←	4G Band Selection		
			User level: Advanced
B1	B2	B3	B4
B5	B8	B12	B13
B18	B19	B20	B25
B26	B27	B28	B66
B85			

2G Band Selection setting determines which frequency bands can be used to establish a 2G connection.

GSM 900MHz + DCS 1800MHz
GSM 900MHz + PCS 1900MHz
GSM 850MHz + DCS 1800MHz
GSM 850MHz + PCS 1900MHz
GSM 900MHz + DCS 1800MHz + PCS 1900MHz
GSM 850MHz + GSM 900MHz + DCS 1800MHz + PCS 1900MHz

Operator Lock

The Operator lock screen allows you to lock the logger to a specific Mobile Network Operator.

When set to "none" the logger will try an assortment of operators sequentially until it finds one that accepts the connection attempt.

Operator Lock
None

38

Each Mobile Network Operator can be identified by a 5-digit code – The MCC / MNC code. (MCC / MNC codes can be found from an internet search).

If the code for the operator is known, it can be set from this screen. Tap on MCCMNC line and set the code.

Operator (MCCMNC)

CANCEL   OK

← **Operator Lock**

User level: Advanced

Operator (MCCMNC)

All

Network Type

All

You can initiate a scan to see which networks are visible to the device's modem and use the results to set your chosen operator and technology lock

START SCAN

Note:
For the above setting to be functional, the SIM must also support the chosen network operator.

If a specific type of network technology is required, it can be set from this screen. Tap on the Network Type line and select from the list.

Note:
For the above setting to be functional, the SIM must also support the chosen network type.

Network Type

2G

LTE-M

NB-IoT

All

There is a tool to help with making the above settings:

Tap on the "Start Scan" button.

You can initiate a scan to see which networks are visible to the device's modem and use the results to set your chosen operator and technology lock

START SCAN

The logger will scan for local networks.

Scanning For Networks

Please wait: Reading modem

CANCE

Scan Complete

Select Operator

<Select Operator>

Select Network Type

<Select Network Type>

SET

When finished, tap on each of the controls to make
a selection from those listed. (Contents vary according to what is found to be locally available).

Operator (MCCMNC)	Network Type
vodafone UK	2G
O2 - UK	NB-IoT
EE	All
All	CANCEL

Note:
For the above setting to be functional, both the SIM and the network operator must also support the selections.

DNS Mode (Domain Name System) is factory set to "Auto".

When the logger dials-in it resolves the Domain Name part of the URL by doing a DNS lookup over the network.
The network may not support all DNS protocol versions, so the logger (if set to Auto) tries several types until it finds one that works. It then uses that protocol option for future operation.

Auto
Mode 1
Mode 2
Mode 3
Mode 4

Alternatively, the user can pre-set this mode using the control.

DNS Mode	
	Mode 1

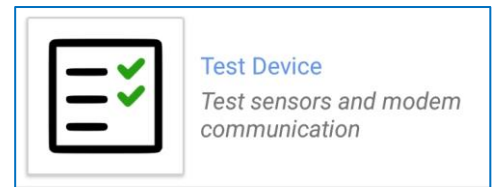### 3.7.2   2G and 3G Networks: Signal Test (signal strength - CSQ)

To access the logger test menu, tap on the "Test Device" line.

Access the "Test Device" menu and then tap on "Signal Test".

This test measures the **signal strength** (CSQ) of the received 2G mobile network signal.

Once connected to the mobile network, the provider details and signal strength indicator (CSQ) are displayed. The default is to show the average value of the last 10 readings, but it can be changed to show the latest value (by tapping on the number).

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.

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).

Note: When using a modem with 4G Network protocols (NB-IoT and LTE-M), CSQ levels are replaced with different quality parameters.
(Refer to section 3.7.1 to determine what modem settings are in use for the logger. Refer to section 3.7.3 for 4G Network signal quality assessment).
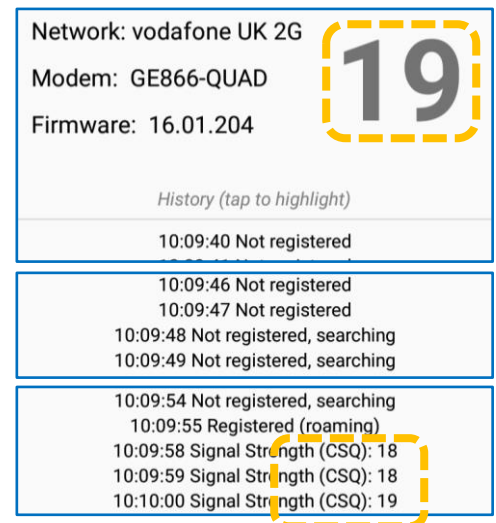
3.7.3 4G Networks (NB-IoT, LTE-M): Signal Tests

Modems that use 4G networks have a different set of parameters for signal quality than those using 2G and 3G networks.

Navigate to the Signal Test screen, as detailed in section 3.7.2.

The CSQ indication is replaced for 4G networks by a "Signal Strength" indication.

(Note: CSQ is missing from the lower listing).

Select "Show details" from the local menu to provide additional information.
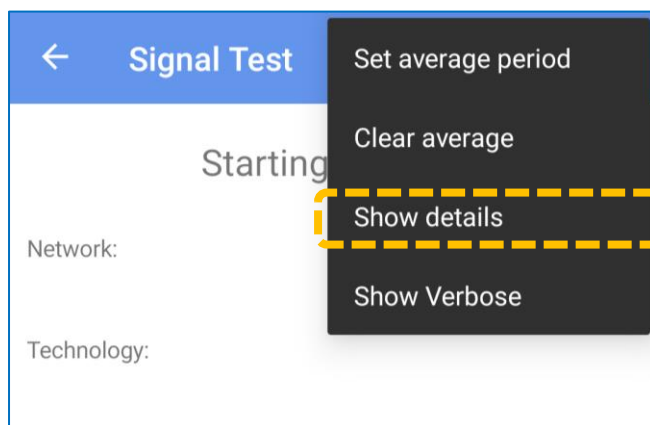
The lower listing will show additional parameters:

- Signal Strength
- Signal Power
- Signal RSRP (dBm)
  (Reference Signal Received Power).
- Signal RSRQ (dBm)
  (Reference Signal Received Quality).

These parameters may be used to assess the suitability of the logger communication with the cellular data network.

42
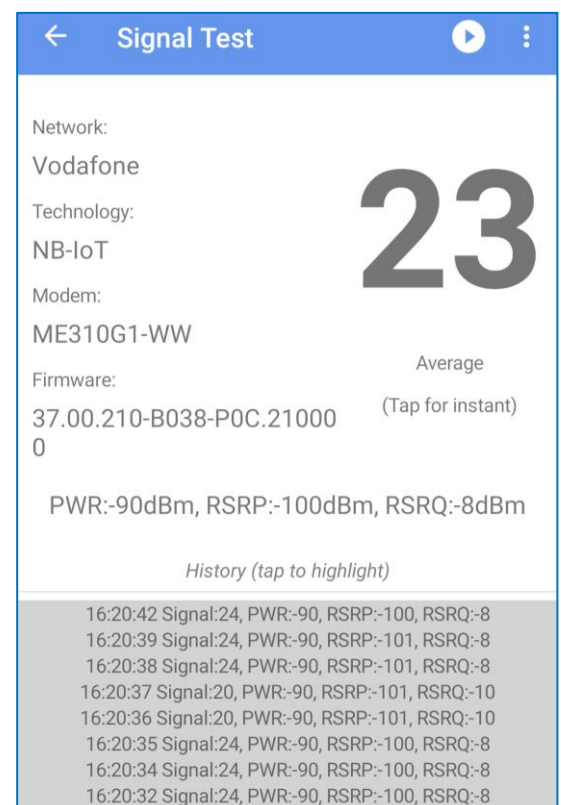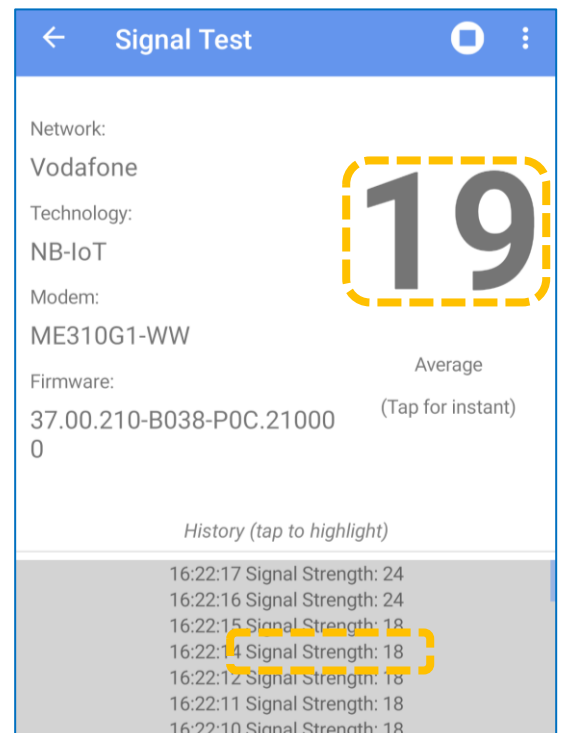
RSRP value: The following guidelines are given for the cellular network signal, (as measured with the chamber closed):

>= -80
Excellent.
(Data transmission should be reliable).

-80 to -90
Good.
(Data transmission should be reasonably reliable).
It is important to select the correct antenna and install it in the most suitable location).

-90 to -100
Fair to Poor.
(Reliable data speeds may be possible but drop-outs may occur.
Performance drops considerably as the value approaches -100.
The logger may be able to register with network but will not be able to send or receive data reliably).

Note: The above values are negative. The higher the value (less negative) the better.

RSRQ value: The following guidelines are given for the cellular network signal, (as measured with the chamber closed):

>= -10
Excellent.
(Data transmission should be reliable).

-10 to -15
Good.
(Data transmission should be reasonably reliable).
It is important to select the correct antenna and install it in the most suitable location).

-15 to -20
Fair to Poor.
(Reliable data speeds may be possible but drop-outs may occur.
Performance drops considerably as the value approaches -100.
The logger may be able to register with network but will not be able to send or receive data reliably).

Note: The above values are negative. The higher the value (less negative) the better.

3.7.4 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 call test will automatically start.
(The top-right corner of the display has a control to start and stop the test).

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

The call will progress through various stages until it is complete.

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. (Tap the "Details" button to show).

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

Note: When the equipment is installed below ground level, the Call Test can be made initially with the chamber lid 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.
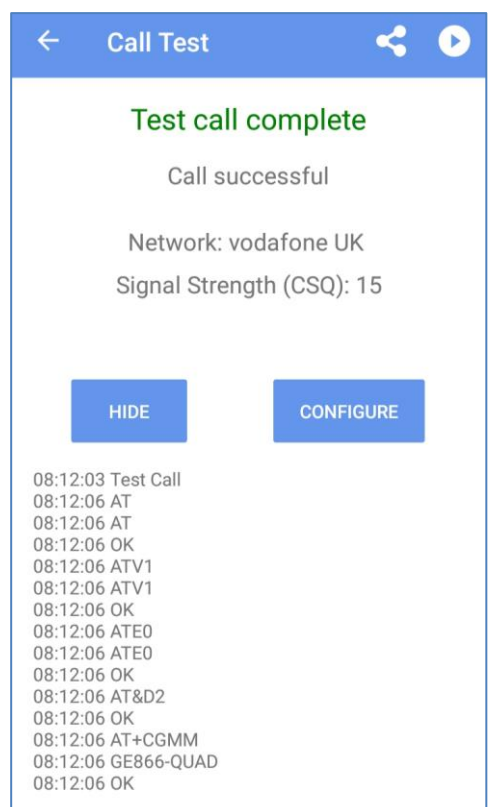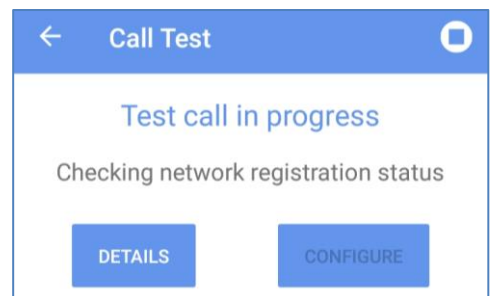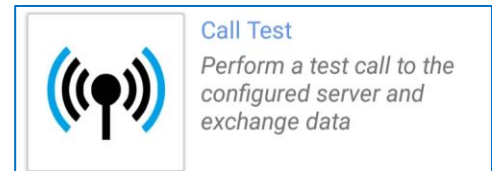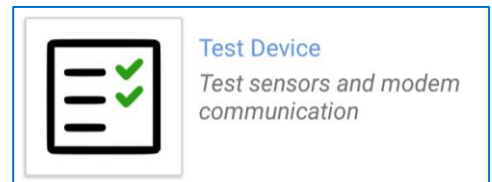
3.7.5   Troubleshooting a Call Test failure

Possible Issues and Checks

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

IDT provides some error messages to help diagnose problems:

e.g.:

- SPC low. Please wait for charge.
  (Power boost circuit within the logger requires time to re-charge).
- SIM card error. Please check SIM fitment.
  (SIM must be clean and fitted correctly).
- No networks found. Please check antenna connection and position.
  (Check antenna is undamaged and connected).
- DNS lookup failure. Please check server address.
  (Check with your system administrator that the URL entered as the server address is correct).
- Network registration was denied. Please check that SIM is activated on network.
  (Check SIM card is able to use the selected network operator for data).

(The above list is not exhaustive).

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.
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.

4 VIEWING DATA (WITHIN IDT)

The logger is usually set up to call into a server, where the data is stored. It is best viewed with the viewing tool linked to the server data-store (refer to the appropriate manual or instructions for your viewing tool).

The data can also be viewed graphically by using the IDT app to make a temporary copy of the data stored within the logger.

Tap on the "Logged data" line.
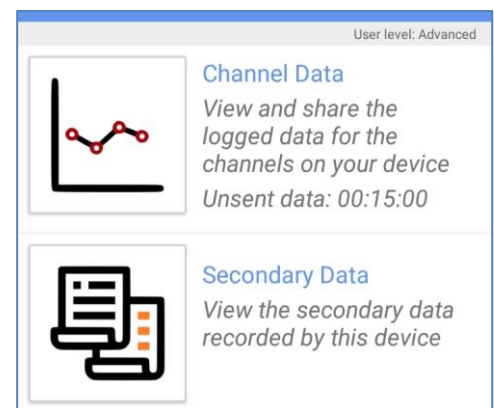
Logged Data
View device logged and recorded data
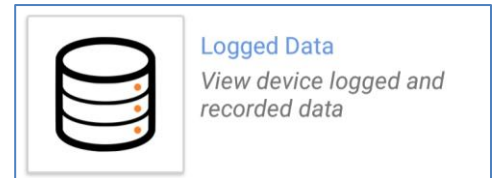
A new screen is displayed.
This screen gives access to any data contained in the logger's primary and secondary data recordings.

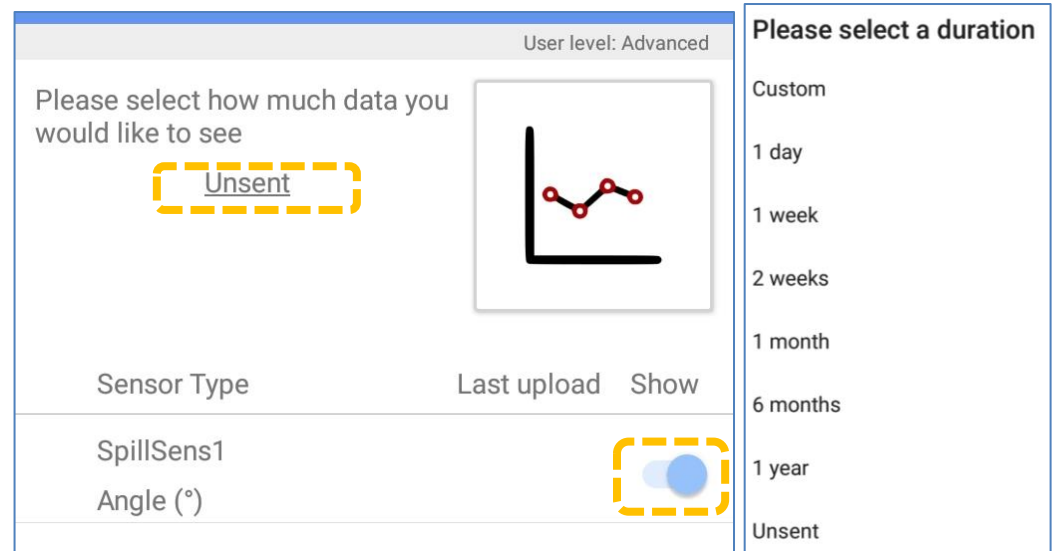Tap "Channel Data" for access to the primary data recordings.
The duration of unsent data is shown
(format: d.hh:mm:ss)

Tap "Secondary Data" for access to the primary data recordings.

User level: Advanced

Channel Data
View and share the logged data for the channels on your device
Unsent data: 00:15:00

Secondary Data
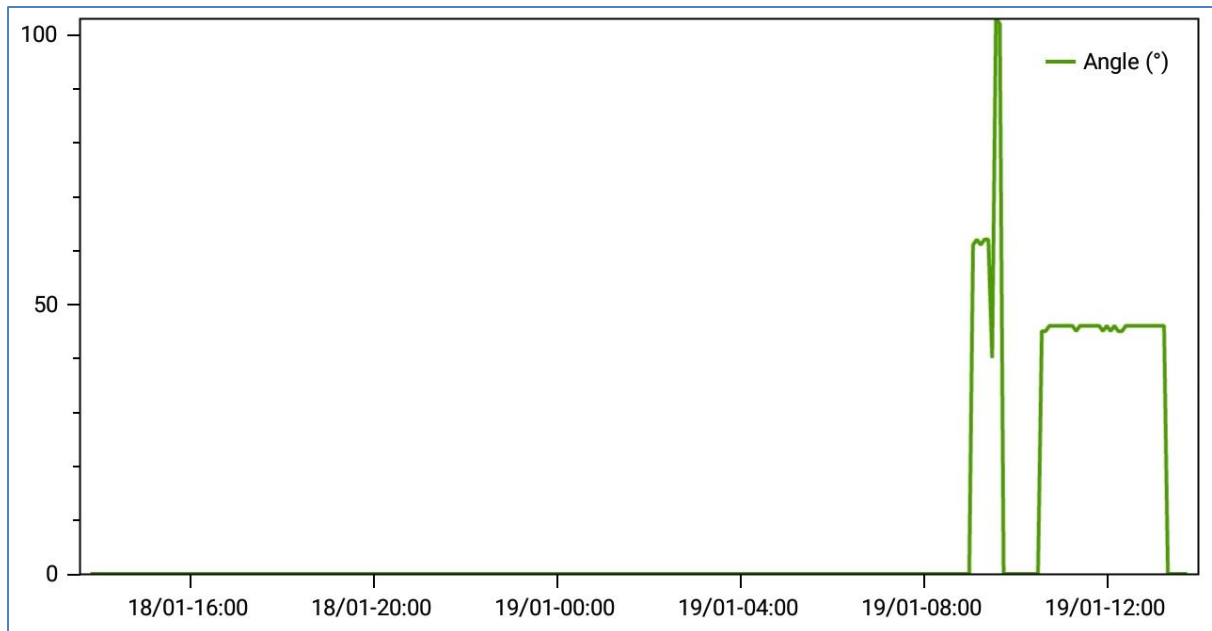*View the secondary data recorded by this device*

Tap to the left of the graph to select a duration that you wish to see on the graph.

Slider controls can be used to include or exclude data from a sensor on the graph.

User level: Advanced

Please select how much data you would like to see

Unsent

Sensor Type	Last upload	Show
SpillSens1 Angle (°)		

Please select a duration

Custom

1 day

1 week

2 weeks

1 month

6 months

1 year

Unsent

Tap on the graph symbol to produce the graph.

The graph can be examined in more detail using the standard techniques available on your phone.
(e.g. finger movements to zoom in or out, re-position the graph within the display, etc).

Tap the back-arrow control on your phone (or the back-arrow on the display) to exit.

Note: The graph contents will vary according to the sensors attached to the logger, the type of data produced, how long the logger has been running and other factors.

5 TROUBLESHOOTING

The app, the logger, the user and sometimes the server interact with each other. Any issues in use of the app should consider all four parts of the system.

(Refer also to section 7, which describes a few of the differences of operation of IDT under various use circumstances).

## 5.1 PUTTING THE EQUIPMENT INTO SHIPPING MODE (DE-ACTIVATING)

Before putting any HWM equipment into long term storage, moving an installed unit, or shipping for repair, it should be put into "Shipping mode" using IDT.

Note: Be sure to upload any unsent data before this operation.

To put the equipment into shipping mode:

Connect to the device using the normal procedure.

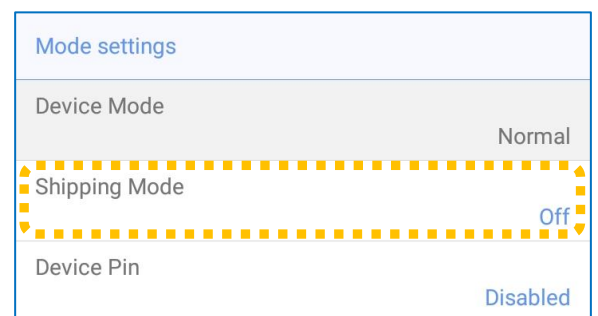From the main options page, tap on the "Configure Device" selection.

Configure Device
View and configure device settings
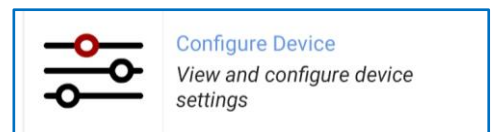
Then select the "Device Information" option.

Device Information
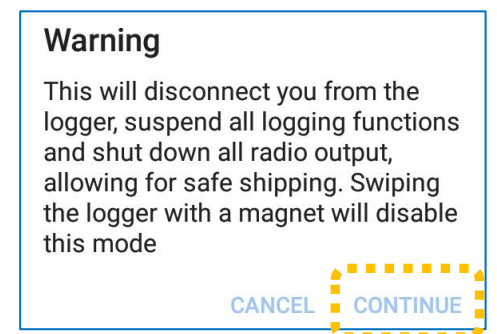*FW-157-001 V1.29*
+44792483539293
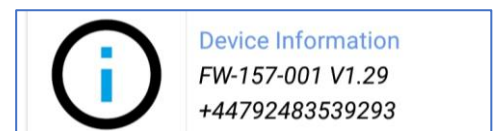
Move the display to show the Mode Settings panel.

The "shipping mode" setting will be shown as "off" since the logger is in use.

Tap on the shipping mode line.

Mode settings

Device Mode
                                    Normal
Shipping Mode
                                        Off
Device Pin
                                    Disabled

Read and accept the warning (by tapping on "Continue").

Warning

This will disconnect you from the logger, suspend all logging functions and shut down all radio output, allowing for safe shipping. Swiping the logger with a magnet will disable this mode

CANCEL   CONTINUE

IDT will update the device.

The device will go into shipping mode and drop the communications link.
(IDT will therefore begin scanning for devices).

Updating

Transfering data from device

48
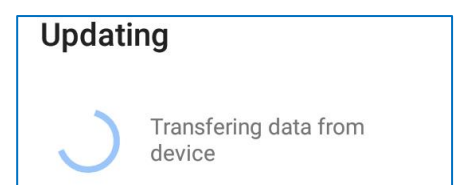
5.2 THE USER CANNOT LOG IN USING THE APP

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

(Refer to your system administrator for assistance if required).

5.3 THE IDT APP DOES NOT LIST THE LOGGER

- The logger communications link is not activated.
  – Activate the logger communication link again (see section 1.6).
- The phone may be out of the communication link range of the logger.
  - Bring them closer together.
- The logger battery may be flat or the logger may be defective.

When used with DataGate:

- The logger is not correctly registered on DataGate.
- The user is not logged into the app, or the initial synchronisation is incomplete.
- The user does not have the appropriate DataGate permissions.
- Try selecting "show unprotected devices". If the logger then appears listed in red, it is functioning correctly in "unprotected mode".
- Try re-starting the phone and the app.
  – Confirm the app Bluetooth connection is working correctly by trying with another logger.

5.4 THE DATA FROM THE LOGGER DOES NOT APPEAR ON THE SERVER.

- Ensure the logger uses the correct data destination URL and port-number for your server.
- Check the logger antenna is attached and in an OK condition.
- Make a Call Test and confirm OK.
- Ensure your server is correctly configured to receive and present the data from the logger.

5.5 TRANSFER OF LOGGER SETTINGS FOR ASSISTANCE / LOAD VIRTUAL LOGGER

If requested by HWM-water, the logger configuration settings can be saved to a file and forwarded to HWM-water for assistance.

Connect to the logger and from the main screen navigate to the Device Information screen.

Tap on the Share icon.

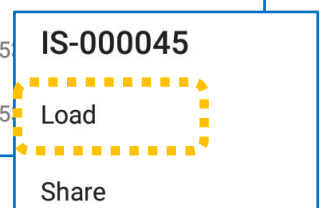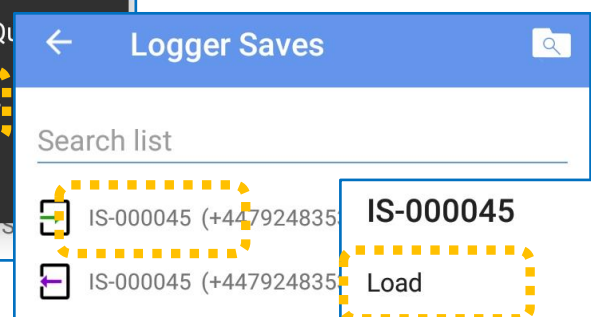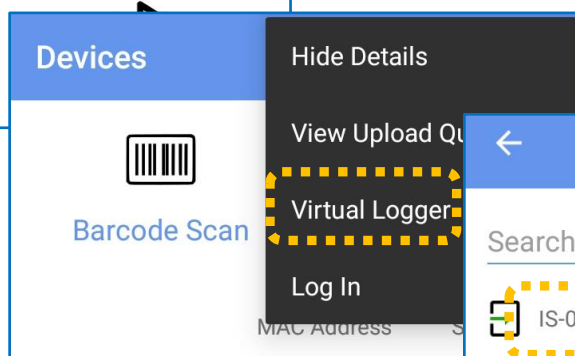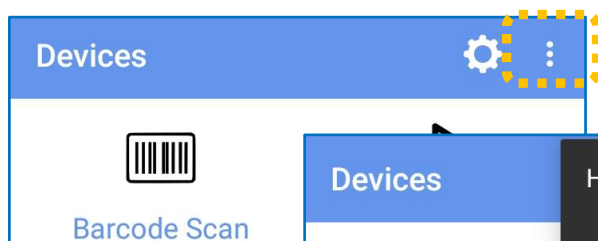Select a method for sharing the information (a logger configuration file + recent event log messages).

Typically, this will be via e-mail.

Select an e-mail program when the phone prompts you.

Share

Copy to clipboard

Email

Device Information

Type: FW-157-001 V1.30

Serial Number: 000045

Logger Time: 02/03/2021 16:06:41

Modem Information

Modem: GE866-QUAD

Tap here to get modem info

Device settings

ID

IS-000045

~~ Device Information ~~
Type: FW-157-001 V1.30
Serial Number: 000045
Logger Time: 02/03/2021 16:06:41

⋮

204, S: 0
UTC: 1614689036, Type: 3, Cid: 2, Err: 2, S: 0

1614701200_IS-...293_False.mbf
6 KB ✕

The contents of the e-mail are automatically generated. You will simply need to complete the destination e-mail address.

The logger details and a copy of its configuration file can now be sent for examination and debug.

Devices ⚙ ⋮

Barcode Scan

Devices

Barcode Scan

MAC Address

Hide Details

View Upload Qu

Virtual Logger

Log In

← **Logger Saves** 🔍

Search list

IS-000045 (+447924835

IS-000045 (+447924835

IS-000045

Load

Share
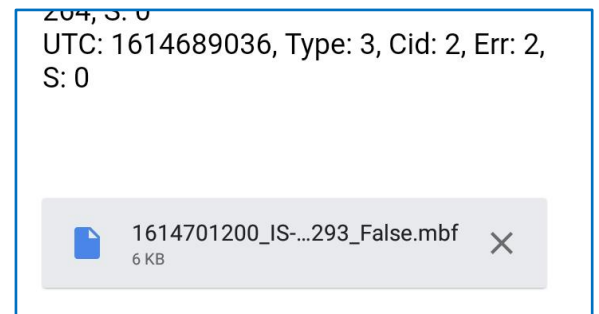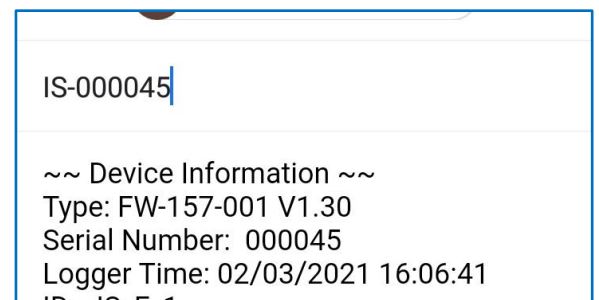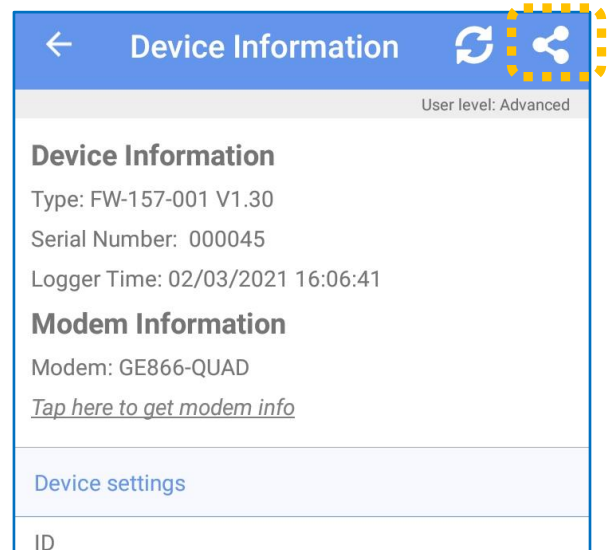
All setting details will be available for inspection once the email recipient loads the configuration details as a "virtual device" (click as shown above, from left to right).

50

6 PART2: ----- SENSOR INTERFACES AND TRIGGER-ACTIONS -----

Note: Certain sensors have their own User Guide regarding installation and configuration using IDT. Follow the additional guidance where available.

6.1 DATA VIEWING PORTALS

- Data from the logger can generally be viewed the webpages provided by HWM DataGate server software.
- Where other HWM data viewing portals exist for certain sensors, they are identified within each sensor description.
- Your utility company may also employ its own data viewing tool.
- To view data on any portal, the data must be delivered to that destination.

6.2 SUPPORT OF MULTIPLE TRIGGERS FROM SAME SENSOR

Loggers can support programming of multiple trigger conditions related to the same sensor.

This can be programmed within IDT by tapping the "+" line to add additional triggers.

e.g. Refer to the diagram opposite, which shows two triggers set up for different angles of a Spillsens sensor.
Here these are both set to generate an alarm, but alternative actions may be selected.
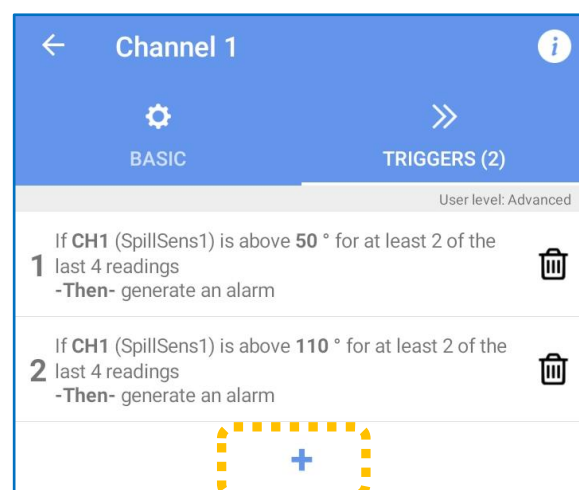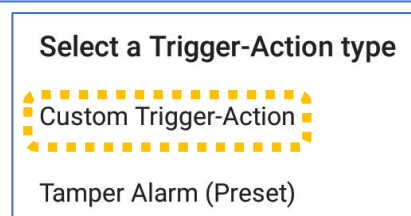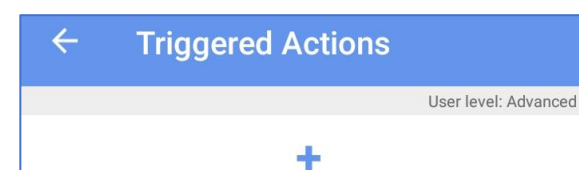

6.3 SUPPORT OF MULTIPLE CONDITIONS FOR A SINGLE TRIGGER

IDT supports setup of multiple-condition triggers, if supported by the logger.

From the main screen, select the Triggered Actions line.

Tap on the "+" symbol to create a new trigger action.

Select "Custom Trigger-Action".

51

Tap on "Add Trigger" to allow two or more conditions that are to be considered as part of the over-all trigger result.

Select each condition.

The conditions may be connected into either an "AND" gate or an "Inclusive OR" gate; only one selection is allowed per trigger-action (although additional Trigger-Actions can be set up to cover other combinations if required).

(Tap on the "-Or-" line to change the logic gate used).

Add trigger requirements.

Tap the back-arrow to show a summary:

> If **CH1** (Status1_0) is above **0** for at least 1 of the last 1 readings
> **1** **-Or-** if **CH2** (Status2_0) is above **0** for at least 1 of the last 1 readings
> **-Then-** generate an alarm

And then save the setting.

6.4 SUPPORT OF MULTIPLE ACTIONS FROM A SINGLE TRIGGER

Loggers can support programming of multiple actions conditions related to the same trigger.

This can be programmed within IDT by tapping the "Add Action" line to add the first and any required additional actions.

e.g.   Refer to the diagram opposite, which shows three different actions set up for a single trigger condition.

Available options will depend on the model number of your logger and the options supported / enabled.

6.5 STATUS INPUT

"Status Input" is a digital signal supported by some logger models.

Where more than one channel is available, they will be available as separate signals on the connector or cable.

Select the required sensor input.

6.5.1 Use as a logic-level data stream

Complete the settings as shown to use the sensor as a digital status input.
(i.e. it can be a value of either "1" or "0").

The recording unit must be set to "status" to use as a digital value (0 or 1).
The input is logged as a digital status and triggers are set to match specific conditions met by the data-stream independent of any consideration of time.

BASIC	TRIGGERS (0)
	User level: Advanced
Input Sensor	Status1_0
Sensor Type	Status
Units/Pulse:	1
Recording Unit	status
Logging Mode	Spot

Triggers and actions can be set using the regular setup process.

e.g. The settings shown opposite will trigger immediately if the input switches from 0 to 1.

Trigger-Action 1

User level: Advanced

Trigger

Channel: 1: Status1_0 (statu Log values

Above 'A'   A= 0

For ≥ 'C' of last 'D' samples   C= 1   D= 1

Hysteresis: ⓘ   0.0

ADD TRIGGER

Action

Generate an alarm

6.5.2 Use as a Time-On data stream

An alternative use of the status input is to set the recording unit as "secs" (seconds).
This changes the logger trigger options to consider the input status as a function of time; the number of seconds the input is at a logic level of "high" between each datapoint being produced.
The time counter resets to 0 seconds whenever a datapoint has been created.

Recording Unit

secs

status

(Refer to your logger user-guide for details of how a logic high or low can be input).

6.6 STATUS OUTPUTS

"Status Output" is a digital output signal supported by some logger models.

Where more than one channel is available, they will be available as separate output signals on the connector or cable.

IDT does not currently support the use of the outputs, except for their use for pulse replication (see section 6.7.2).

6.7 FLOW INPUT

6.7.1 Flow input selection

Flow input was introduced during an example earlier in the user-guide.
(See sections 3.4.1 and 3.4.2).

"Flow Input" is a digital signal interface supported by some logger models. Several options can exist.

Where more than one channel is available, they will be available as separate signals on the connector or cable.
Select the required sensor input.

On some models, the Status Inputs may share the same input electronics. However only one option can be used at any time.

"Flow Uni" is for a uni-directional flow measurement.
It collects a stream of digital pulses from a single input line.
It counts pulses (e.g. from a meter) per unit time to determine a flow-rate measurement and produces a stream of flow-rate datapoint values.

"Flow Bi" is for a bi-directional flow measurement. Two flow input signals are combined in use to detect both direction of flow and quantity of flow.
(Refer to your logger user-guide for details of which signal detects meter pulses and which detects forward and reverse directions of the bi-directional flow).

Input Sensor
<Disabled>
⋮
Flow Uni 1.1
Flow Uni 1.2
Flow Bi

The significance of the pulses is required to be programmed as part of the channel setup; the commodity type and unit of measure signified by each pulse.
(e.g. 1 pulse = 10 litres of the fluid "water" has passed through the meter).

Pulse speed / Timing

Consideration should be given to the pulse speed of the meter in order to ensure the logger is set to sample the interface signal level quick enough to catch the pulses.

Refer to section 3.3 for details of how to check or adjust this timing parameter (see opposite).

Ensure the logger can capture pulses that are generated at the *maximum* expected meter output rate.

Pulse Input Frequency
Pulse sample rate:
High Speed

Pulse sample rate:
High Speed (16ms min pulse)
Power Save (500ms min pulse)

6.7.2   Pulse Replication output

Utilities sometimes have several pieces of equipment installed that require access to the output pulse signal from a meter.

It is possible to re-purpose a Status Output from certain loggers to replicate the meter pulse signals.

If pulse replication is required check / adjust the setting using the slider control.

6.7.3   Tamper alarm sensor

Utilities sometimes have pieces of equipment installed that are used for billing purposes (e.g., a gas meter). The logger may be used for automated meter reading purposes and must therefore remain connected to the utility meter at all times.

Some loggers have the facility of providing some detection of customer tamper attempt.

Utility companies can apply mechanical seals to bear witness to any attempt to tamper with the equipment. The inter-connecting cable between logger and meter can also be monitored electronically for any disconnection attempt (if the meter is compatible).

For loggers that support this facility, it is possible to re-purpose a Status Input to use for tamper-detection. The tamper input detects an electrical path exists when attached to the meter. If the cable is unplugged the path no longer exists and a tamper attempt is detected. (Note that this feature is available using a uni-directional flow channel and is used at the expense of disabling the availability of a second flow channel).

To set up a sensor for Tamper alarm, first setup the Flow channel for use (see section 6.7.1) then follow the following steps:

From the main page, find the Triggered Actions control and tap on it.

Tap on the "+" line to add a new Trigger-action combination.

IDT has a facility to use a *Tamper-Alarm pre-set* to simplify its setup. Tap on this line.

(Pre-sets can sometimes implement settings that the user may not have direct access to).

IDT will make several changes to logger settings to implement a tamper detection and the appropriate alarm.

(The illustrations opposite and below are for information only... The tamper detection has been implemented using the Status2 input signal, monitoring time open, and triggering immediately when first seen. It requires a compatible cable where Flow1 / Status2 share the same connector; Status2 protects against removal of Flow1).

6.7.4 Tamper alarm (message option)

It should be noted that the tamper detect facility described in section 6.7.3 is distinct from the ability to send a "report as tamper alarm" message, although they are intended to be used together.

The "Report as tamper alarm" option *includes an additional message* when sending the alarm to the server. It (if the server software supports) allows regular alarm conditions to be prioritised and handled differently to customer tamper attempts.
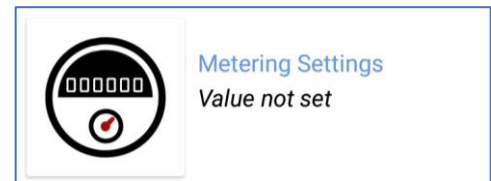

6.7.5 Meter Reading(s)

Digital Flow Interface channels are often used to track the usage of a commodity (e.g. of gas or electricity) supplied by a utility company. The commodity passes through an on-site meter (which can indicate use by providing meter pulses). An initial meter reading has to be taken and entered into the logger to enable this feature. When the

logger calls into the server with the flow measurements datapoints it can also include a calculated current meter reading.

From the main screen, locate the Metering settings control.
Initially, no value has been set within the logger.

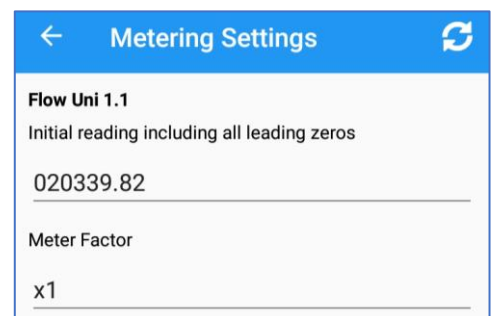Tap on the "Metering Settings" line.

Read the main meter, noting its format.

Enter the meter reading into the "Initial reading" field. (Include any leading zeros, the decimal point, and any other displayed digits).

Calculate and enter a meter factor.

$$\text{Meter factor} = \frac{\text{Unit of volume measurement used on the Meter for each digit.}}{\text{Unit of volume measurement used on the Flow channel.}}$$

Tap the back-arrow and the entered reading for Meter 1 is now shown. (This is not a live value).

You can confirm logger is set up correctly by doing the following:

> After waiting for the meter to change by a few digits, note the meter reading and tap the "Meter Settings" control.
> Confirm the "Current value" reading matches the meter reading (noted earlier).
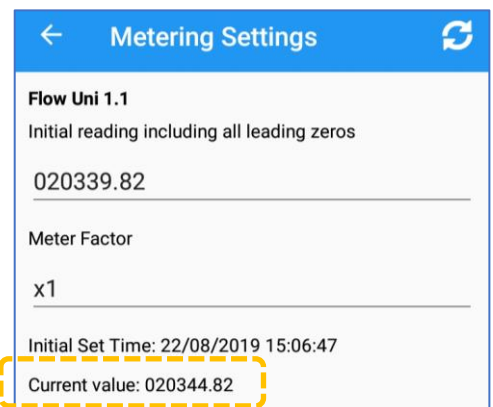
If the reading is not correct, re-check:
> The cables go to the correct meter.
> The meter factor is correct.
> The channel settings (units/pulse and recording unit) are correct.
... and then repeat the test.

Where two flow channels are used, the meter reading entry page will be as shown opposite.

Make the settings (as above) for each meter.

Add the initial reading and Meter Factor for the second meter.

Then tap the back-

A meter reading is now shown for both

Confirm the readings of both "Current value" fields are operating as expected, using the method described earlier.

6.8 LEAK-NOISE SENSOR

- A leak-noise sensor listens for leaks in water pipe networks.
- It is often used with the following viewing portals: PermaNETWeb.
- This is a complex sensor and requires a specialised method of setup.
- Refer to your logger User-guide for information if this sensor is supported and for more details.

6.9 SONICSENS3 SENSOR

- SonicSens3 is a sensor which measures distances with ultra-sound.
- It is often used with the following viewing portals: Datagate
- This is a complex sensor and requires a specialised method of setup.
- Refer to your logger User-guide for information if this sensor is supported.
- Refer to the SonicSens3 User-guide for more details.

6.10 SPILLSENS

- SpillSens is a digital float angle sensor.
- It is often used with the following viewing portals: SpillGuard.
- It requires a specialised method of setup.
- Refer to your logger User-guide for information if this sensor is supported.
- Refer to the SpillSens User-guide for more details.

7 IDT - OPERATION DIFFERENCES

The IDT app adapts the content of its screen options based on many factors:

- IDT User level.
- Use of IDT with or without login to the server.
- Type of logger (logger family).
- Interfaces available for use (unconfigured and configured).
- Sensor attached or missing (applies to certain sensors only).
- Previously entered setting choices.
- Device security settings.

This section describes how this may sometimes affect the operation of IDT.
The description is not exhaustive, but indicates typical issues which may arise due to circumstance of IDT use.

7.1 RESTRICTIONS OF IDT BASIC MODE

When operating IDT in BASIC mode, some features are restricted.

e.g. The ability to modify channel settings is restricted in BASIC mode (greyed-out), but available in Advanced mode. (See below for an example).
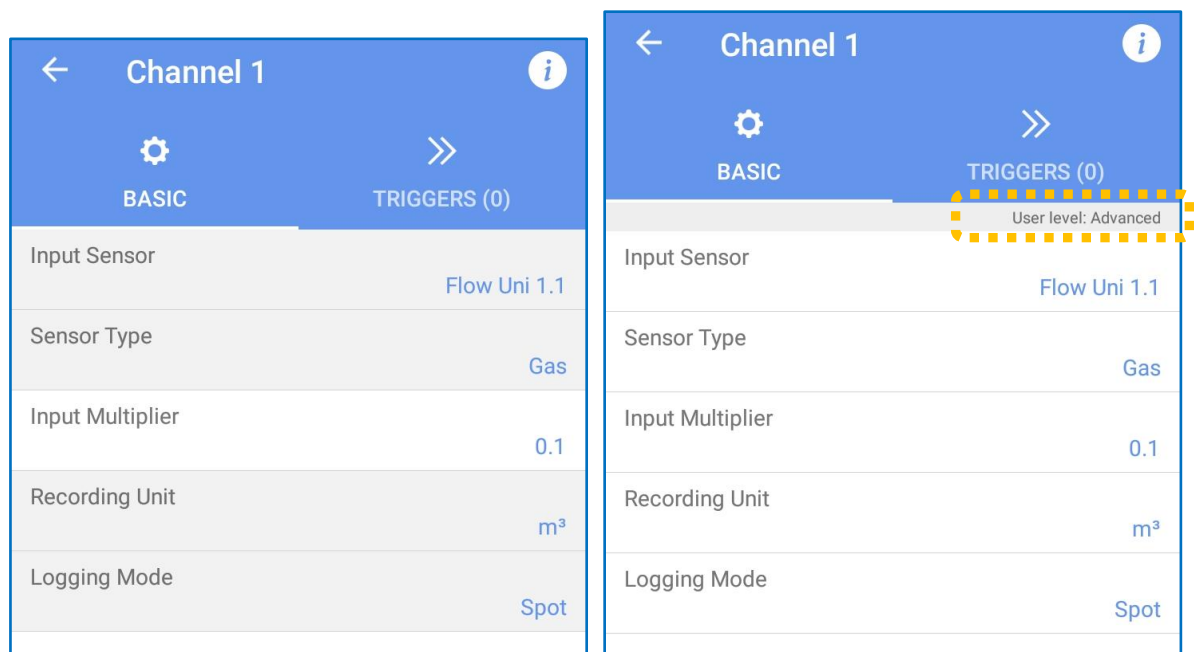
7.2 USE OF IDT WITH DATAGATE VS WITHOUT DATAGATE

Certain menus adapt to whether IDT is being used with or without the DataGate server.

Since DataGate is a player in the security of logger settings, the options to update allowed devices and see unprotected devices is removed when IDT is not used with DataGate.

Similarly, IDT will make no attempt to queue data for upload since it has nowhere to send the data from the phone device.
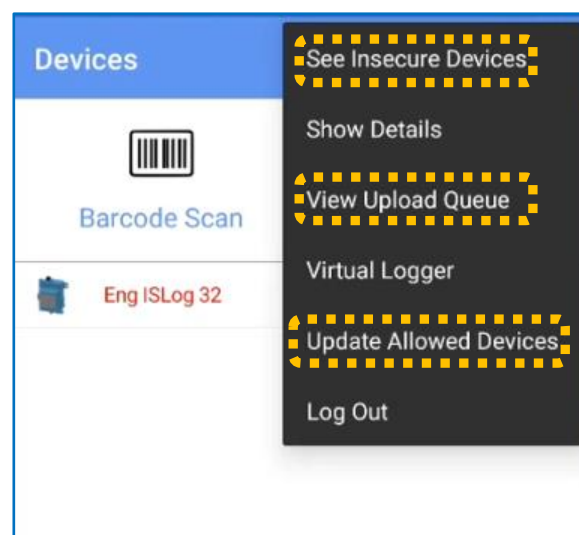
The main screen does not show the "Deploy Device" option.
It is not be possible to deploy the device using the same credentials as was used to log the IDT app into DataGate; you have not provided credentials as you have not logged in.
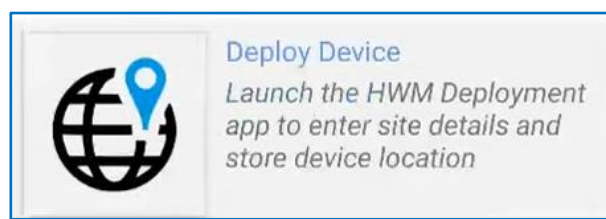
7.3 USE OF IDT WITH A VIRTUAL LOGGER

When IDT is used for inspecting the settings of a virtual logger (loaded from a logger settings file) it is read-only access. (See section 5.5)

IDT is not connected to any real device and has no facility to update either a real device or the settings file.

62

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

MAN-2000-0001-A