On the device display:

Chiller Temperature

21.43 ℃

OK

10/03/17 - 13:32:54

User Manual, Set Up & Installation Guide

Covering
D3LITE, D3 & D3MEDICAL
Monitoring System Base Stations

Klipspringer

Compliance with confidence

Systems covered by this manual;

UK, Europe & Zone 2 (For 2.4Ghz systems)
P1-D3101-0433   D3 LITE 433Mhz
P1-D3102-0433   D3 433Mhz
P1-D3103-0433   D3 MEDICAL 433Mhz
P1-D3104-0433   D3 BRIDGE 433Mhz
P1-D3101-0868   D3 LITE 868Mhz
P1-D3102-0868   D3 868Mhz
P1-D3103-0868   D3 MEDICAL 868Mhz
P1-D3104-0868   D3 BRIDGE 868Mhz
P1-D3101-2400E   D3 LITE 2.4Ghz Europe
P1-D3102-2400E   D3 2.4Ghz Europe
P1-D3103-2400E   D3 MEDICAL 2.4Ghz Europe
P1-D3104-2400E   D3 BRIDGE 2.4Ghz Europe

Zone 1 (these units are not CE or UKCA marked an must not be used in the UK or Europe)
P1-D3101-2400   D3 LITE 2.4Ghz
P1-D3102-2400   D3 2.4Ghz
P1-D3103-2400   D3 MEDICAL 2.4Ghz
P1-D3104-2400   D3 BRIDGE 2.4Ghz

Zone 1 & Zone 2
Refer to the radio power section in the Technical Specification at the rear of this document for the transmission power of each system. Ensure the correct system has been ordered to meet the radio power requirements for the territory the systems will operate within. If you are unsure please contact your supplier for assistance.

Approvals

FCC & ISEDC
The following products comply with FCC & ISEDC; P1-D3101-2400E, P1-D3102-2400E, P1-D3103-2400E, P1-D3104-2400E, P1-D3101-2400, P1-D3102-2400, P1-D3103-2400 & P1-D3104-2400.

FCC
Contains FCC-ID: QOQMGM12P3

ISEDC
Contains Transmitter Module IC: 5123A-MGM12P3

1. SAFETY INFORMATION

Read all the instructions carefully before using the base station and keep a copy of all documents for future review.

1.1. Electrical Safety

Before mounting/dismounting the base station and/or connecting the power supply ensure the units is powered down and switched off at the mains. Any connected peripheral, hard wired devices with live feeds should also be powered down before mounting/dismounting the base station.

Before opening the base station casing to change the battery back-up battery, isolate the electrical supply and also the live feed to any hard wired peripheral connected equipment.

Before connecting peripheral, hard wired devices with live feeds, power down and disconnect the base station from the main supply.

Caution, live feeds may derive from more than one source.

If the power supply or supply cable is damaged then it must be replaced, switch off the unit at the mains and contact the system supplier.

1.2. Battery Back-Up² Battery

The battery in the battery back-up² must be disposed of in accordance with your local laws & regulations, or ship to the supplier in the new battery packaging.

Replace the battery with the same part number as the type originally installed. Replacement instructions are contained with the new battery shipped.

CAUTION RISK OF EXPLOSION IF BATTERY IS REPLACED BY INCORRECT TYPE

Do not dispose of the battery in a fire, the battery may explode.

Do not open or mutilate the battery. They contain an electrolyte which is toxic and harmful to the environment and to the skin and eyes.

Note - ² Battery back-up not available on LITE versions

1.3. Damage

Inspect the base station & power supply for damage after unpacking.

If the base station is damaged during normal operation and you are unsure of its operational performance, switch-off at the mains & unplug. Contact the system supplier for assistance.

The unit contains no user serviceable parts, the battery back-up² battery should only be replaced by suitable trained personnel. Do not attempt to disassemble the unit or attempt repair.

1.4. Location of the unit

The base station should be located on a flat, even wall on the mounting plate supplied. The unit slides from right to left onto the mounting plate, at least 30cms needs to be free of obstacles to the right of the unit for future mounting/dismounting.

Avoid mounting the unit next too or directly beneath electrical conduit, this may impact the wireless range of the unit

Ensure the mains socket and network port are near to the mounting point and are easily accessible.

1.5. Temperature & Moisture

The base station should be mounted in a dry environment with an operational temperature range of between 5°C to 55°C.

To reduce the risk of damaging the unit, causing a fire or personal electrical injury, do not expose the base station to rain, moisture, dripping or splashing.

1.6. Loss of Life & Personal Harm Applications

The D3 family of monitoring systems must not be used in life support, critical care, medical, safety equipment, or similar applications where product failure could result in loss of life or personal or physical harm..

The systems can be used for environment monitoring to gain performance data but must not be used as a primary alarm system.

System Overview

The D3 base stations are designed to be used with the D3 range of sensors. Sensors communicate with the base station each minute, the probe data is; automatically reviewed, assigned alarm actions (if necessary) and saved for later access.

Functionality across the D3 range varies, this manual covers all base station types. Differences in functionality will be noted within this document as necessary.

Refer to the Set-up & Installation Guide section for powering up, power connection, networking, installation & Administrator level access actions.

D3 Base Station Assembly
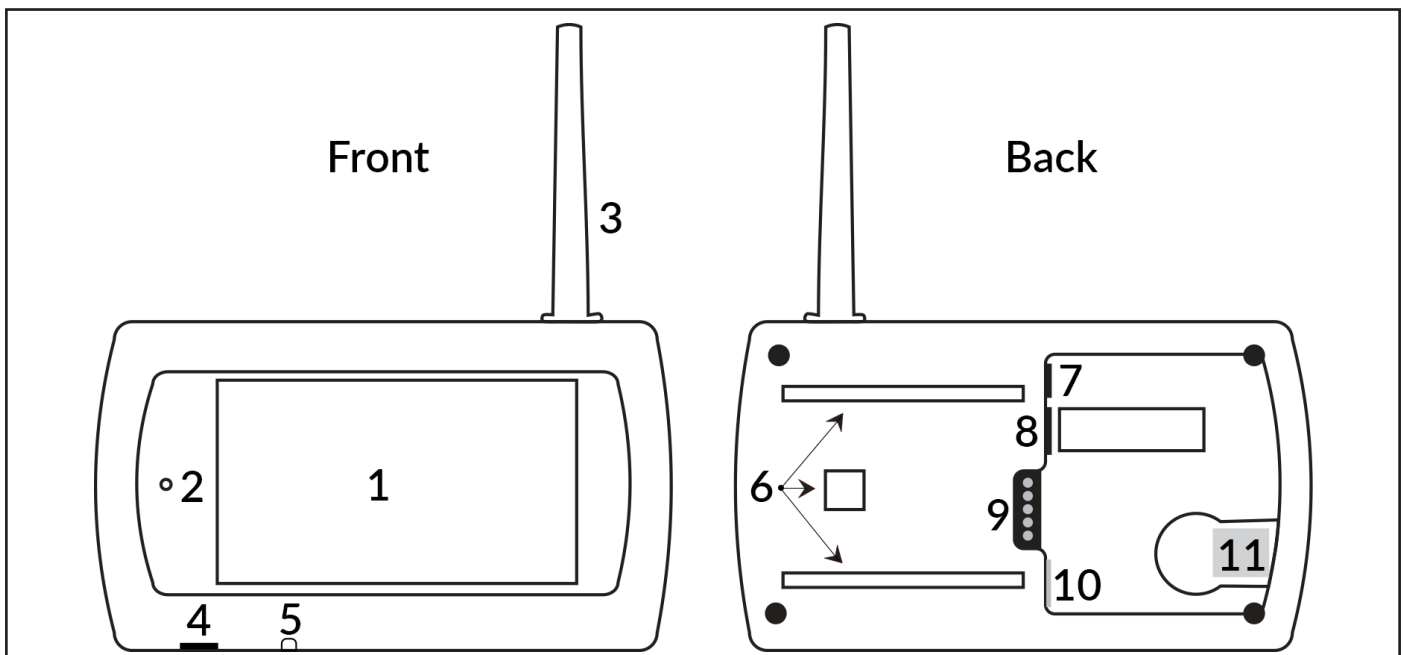
Front
1 - Colour Touch Screen
2 - Indication LED (Green & Red)
3 - Aerial Enclosure
4 - Micro USB Port
5 - On/Off Switch

Back
6 - Wall Plate Fixing Points
7 - Power Connector
8 - Mini Din Connector
9 - Dual Relay Output
10 - Ethernet Connector
11 - Micro MMC Slot[1]

Table of Content

User Manual

2.   Base Station

2.1.   Indicator LED

Green - powered on and no alarms.
Red Flashing - un-acknowledged alarm status.
Red Constant - acknowledged alarm status.
> - If a new alarm occurs the LED will return to Red Flashing until acknowledged

2.2.   Base Station Touch Screen

The touch screen allows navigation by firmly pressing on the icon/option required.

The date and time are shown on all system versions.

The battery charge indicator shows the current charge level on the internal battery back-up[2].

Default view - home screen
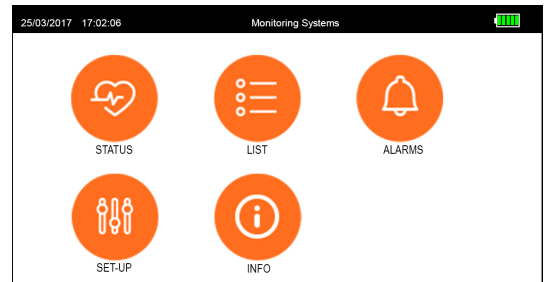
Note - Do not press on the screen with sharp or pointed object as this will cause surface damage

2.3.   Status

HOME => STATUS

Sensor status view, shows; ID, Name, Current Reading, Current Status (colour coded);

Green – OK.
Amber – in alarm delay count down.
Red – in alarm.

Info icon shows set points & alarm delays set for the device.

The up & down keys scroll through added devices, automatic scroll will commence after 30 seconds of inactivity.

2.4.   List

HOME => LIST

Overview of all devices sorted by ID reference (lowest to highest).

Shows device: ID, Name, Current Reading (with status colour coded) and the sensor reading type – e.g. °C.

Scrolled with up & down keys.

2.5.   Alarms

HOME => ALARMS

List of all unacknowledged and current alarms, scroll using up & down key.
Red - unacknowledged alarms
Black - newly acknowledged (via the base station) & current alarms

NOTE -Individual alarms can be acknowledged by a user with the appropriate access level on the base station.

Alarm acknowledgement via the networked access allows multiple alarm acknowledgement – see section 6.2 Unacknowledged Alarms

2.6. Alarm Acknowledgement via Base Station

HOME => ALARMS => SELECT => ACKNOWLEDGE ALARM =>ACK

1 - Select alarm using up & down keys.
2 - Once selected press alarm acknowledge key.
3 - Alarm details are displayed, press ACK key (acknowledge alarm) Press Username box, select user & press the Enter key.
4 - Press Passcode box, enter passcode & press the keypad Enter key.
5 - Press Confirm
6 - Details screen shows alarm acknowledge.

Press back key to return to alarm list.

Note - 1-6 need to be repeated for each alarm to acknowledge.

2.7. Set-up

HOME => SET UP
Passcode protected, Administrator access only.

2.7.1. Home
Returns to home screen

2.7.2. Edit IP Configuration (at Base Station)
HOME => SET UP => IP => CHANGE

Shipped in DHCP Client configuration, allowing network to assign IP settings automatically.

Change IP to DHCP Server only if the system is to be set up using a PC/Laptop prior to network connection.

The Static IP configuration can only be entered/updated via network interface. Once set the last Static IP configuration is retained allowing the unit to be switched to Client or Server mode during maintenance.

DHCP Client
Default - network to assign all required IP configuration

DHCP Server
Allows the base station to be directly connected to a PC or Laptop

See section 10. Networking the Base Station for more on IP configuration.

2.7.3. Re-Calibrating the Touch Screen
HOME => SET UP => TOUCH => START

The touch screen is calibrated at manufacture, to re-calibrate follow on-screen instructions.

2.7.4. Drive
HOME => SET UP => DRIVES

Current information on internal and external memory drives.

2.7.5. Utilities
HOME => SET UP => UTILITIES

For higher level actions via USB drive and restoration of configuration from the uSD - micro SD card if installed, contact your system supplier for more information.

2.8. Information

HOME => INFO

Overview of system information, showing:
>   Network mode.
>   IP address - for networked access to the system.
>   IP Subnet, Gateway & Preferred DNS (preferred DNS will be blank in DHCP server mode).
>   IP Mac Address – unique mac address.
>   Http Port – the IP connection port.
>   Battery – battery back-up status (if installed).
>   Version - software version & radio software version and frequency.

3. Networked Interface

The interface uses a standard internet browser on a PC/Laptop or mobile device with access to the same network as the base station. For the purpose of this manual Google Chrome has been used.

3.1. Accessing the D3 Base Station

INTERNET BROWSER => LOGIN SCREEN => SITE PAGE

User are assigned access privileges by systems Administrator(s). D3 user's access privileges will determine what information and access levels on the systems screens.

1 - Open a standard internet browser on a PC/Laptop or mobile device.
2 - Type D3's IP address in to the navigation bar – e.g. 192.168.100.100 then press enter.
3 - Enter Username and Password, press Sign In.
4 - The default Site Page will open.

Note - New users need to set their Base Station password, see section 12.1. My Details.

Hint - Add IP address to browser favourites.

4. Site (Default Screen on Login)

1. Main menu bar for all system menu pages

>   SITE (default page) – overview of sensor details.
>   ALARMS – Overview & access to current, unacknowledged and historical alarms and audited system events.
>   REPORTS – User generated reports.
>   SETTINGS – The user privilege level will determine the settings page display.
>   INFO – System information page.

2. Current date and time.

3. Portal Access Indicator

   Only shown if Portal Access is enabled for the base station - see Section 16.5 - Portal Access.

4. User Status Indicator.

   Green - Logged in, click to log out. Inactivity for more than 5 minutes will log the user to guest level (grey).
   Guest the user can view data but an attempt to access any restricted part of the system will require a re-login.

5. View Selector

   All – shows the readings and status of all sensor (scroll to see all).
   In Alarm – shows only those sensors currently in an alarm – see section 6. ALARMS.
   In Warning – shows only those sensors that are currently in a warning status and on alarm delay countdown.

6. Export Buttons - current screen data to be exported to various outputs.

7. Sensor Type – Expanded for individual or multiple sensor types to be chosen and viewed.

8. Expand all - Expands view for grouped sensors – see section 11.3 Adding a Device Group.

9. Search - allows a search of current viewed data.

10. Sensor Detail & Details Bar.

    Details Bar– allows sorting by ID and current status
    Sensor Details - includes (from left to right)
    Graphing Button – opens the Graphing Tool for data review, see section 5. Graphs
    Sensor Description – opens a Sensor Details page, see section 4.2 Sensor Details
    High/Low Alarm 1 – the warning alarm set points
    High/Low Alarm 2 – the critical alarm set points, if set
    Current Reading
    Status

The Site page is the default system landing page on login.

   Hint -No system changes can be administered on the SITE page itself, users should familiarise themselves with this page by clicking on the various elements.

Re-entering or refreshing will reset the page.

4.1.   Sensor Readings & Status Messages

4.1.1.   Sensor Readings
Power Up – awaiting reading, if no reading received a communications alarm will trigger.
Current Reading – shows the last reading received.
Sensor Fault – the sensor is faulty.
Inhibit – The alarm status is inhibited, the current reading shown but no alarms occur until inhibit is cleared.

4.1.2.   Status Messages

OK – reading within set points.
Alarm Pending – reading is outside set points and the alarm delay period has been activated, time remaining until alarm shown.
Alarm – reading is outside set points, alarm delay expired and alarm triggered.
No Communications – no readings received, alarm triggered.

4.2.   Sensor Details

SITE => SELECT SENSOR
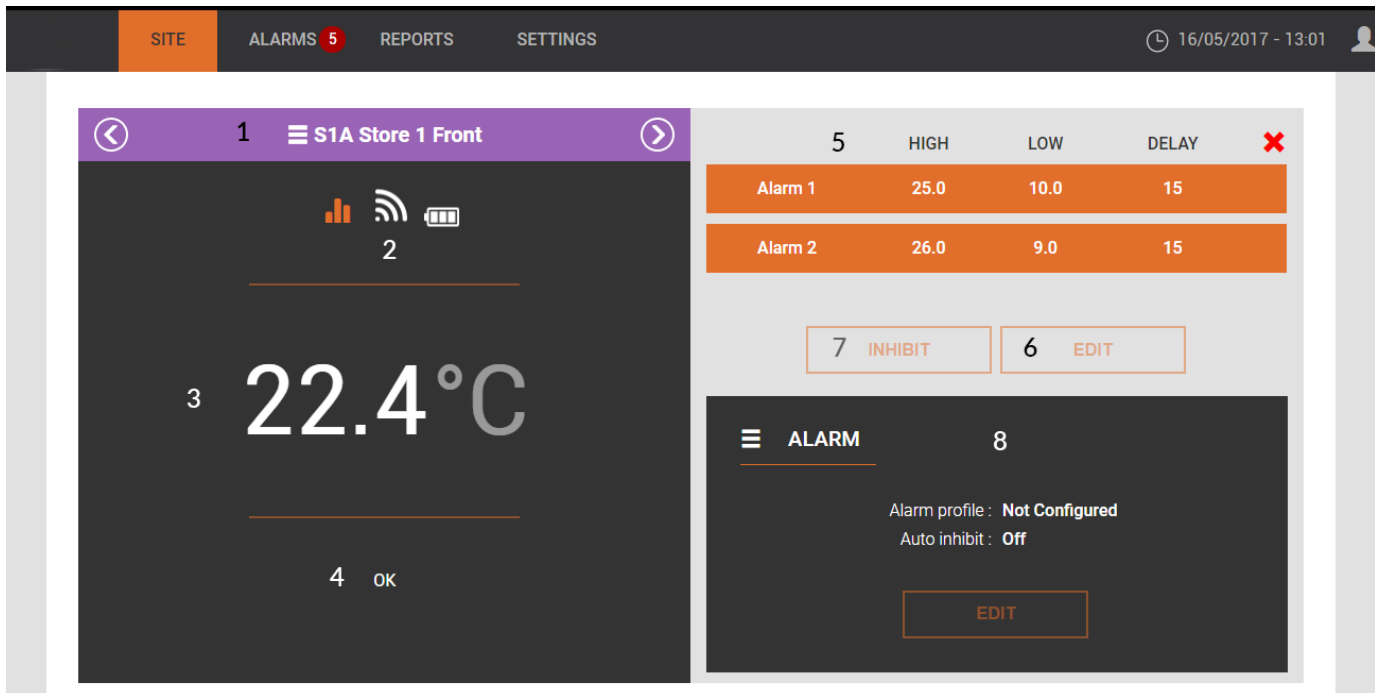
1. Current Sensors Name and Reference ID – scroll in ID order (low to high) using back and forward keys.

Clicking the purple bar will generate a list of all sensors that can then be selected.

2. Graphing Tool, Signal Strengths and Battery Level Icons –

    Graphing Tool - opens the graphing tool – see section 5. Graphs.
    Wireless Signal Strength Indicator – Four bars = full strength, No bars/red = low strength, also see section 11.1 Manage Devices.
    Battery Wear Level Indicator - Red = replace battery.

3. Current reading.

4. Sensor Status.

5. Alarm 1 & 2 Set Points & Delays – set points and alarm delays, see section 4.2.1 Edit Alarm Set Points Alarm 2 shaded = Critical set points not activated.

6. Alarm Edit Button – for amending set points and adding Alarm 2.
Note - users access privileges will determine if set points can be edited. All changes are recorded in audit history.

7. Inhibit/Clear Inhibit – for sensors alarms to be inhibited and re-activated. Inhibited sensor will not alarm, see section 4.3 Sensor Inhibit/Clear Inhibit.

Note - users access privileges will determine if inhibit and clear inhibited can be edited. All changes recorded in audit history.

8. Alarm Profile & Auto Inhibit – configures actions taken on alarm, see sections 13.2 Alarm Profiles & 14.2 Scheduler.

Select red cross to return to default menu.

4.2.1.   Edit Alarm Set Points

SITE => SELECT SENSOR => ALARM SET
POINTS => EDIT

High Alarm – high reading before alarm delay
countdown starts.
Low Alarm – low reading before the alarm delay
countdown starts.
Delay – alarm delay countdown time.

Warning alarm set points (single points).
    1 - set high, low and delay in Alarm 1, submit to confirm alarm set points.

Warning & Critical alarm set points.
    1 - set warning level high, low and delay in Alarm 1, then;
    2 - select toggle button to activate Alarm 2, set the critical level high, low and delay, submit to confirm both alarm set points.

4.3.   Sensor Inhibit/Clear Inhibit

SITE => SELECT SENSOR => INHIBIT/CLEAR INHIBIT

Used when a location being monitored is out of service or known to be faulty, Inhibiting stops false alarms during a known outage.

To Inhibit Alarm – Click Inhibit key, the sensor will be inhibited. Alarms are deactivated for sensor.
To Clear Inhibit – Click the Clear Inhibit key and the inhibit will be removed.   Alarms are activated for sensor.

Note - Also see Auto Inhibit in section 14.2 Scheduler to inhibit sensors at set time periods.

5.   GRAPHS

5.1.   Graphing Tool

The graphing tool can be entered on any page displaying the graphing icon by clicking the icon.

1. Select Device – the current device (default), another device can be selected via the drop down menu.
2. Select Traces –
    Default - Sensor Reading.
    Default - High Alarm 1 set point.
    Default - Low Alarm 1 set point.
    Default – Status.
    User Defined – High Alarm 2 set point.
    User Defined – Low Alarm 2 set point.
    User Defined – Communications – shows the quality of wireless signal.
    User Defined – Signal Strength – shows the strength of wireless signal.

Note – default traces automatically load, other traces only need to be selected if more than the default are required.

3. Select Data Range – 4 selections, these are;
    Today – data from 00:01am to the latest reading.
    Week – last 7 days of data.
    Month – last month's data.
    User Defined – user selected date range (up to 1 year).

5.2.   Graph View

1. New Graph Trace, Pan Left, Refresh, Pan Right, PDF & CSV.

New Graph Trace – see below.

Pan Left & Right – allows for panning when zoomed in.

Refresh – reverts to 100% zoom level - also completed by double clicking on zoomed graph.

PDF – downloads the selected traces (see 2 below) to a pdf format for printing or saving.

CSV - allows for selected traces to be output to CSV format, output data in 1, 5, 15, 30 or 60 minute intervals, data at selected interval can be averaged (if >1 minute intervals), the average of readings over interval selected are output.
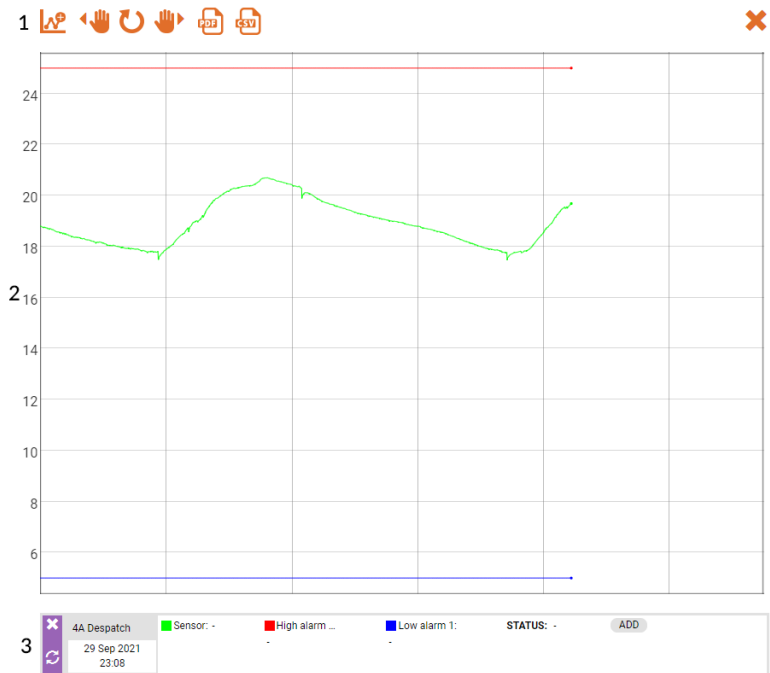
2. Selected Traces – clicking the mouse cursor on trace area shows the cursor line, trace data is seen in trace detail box (3 below). Move the cursor line to show data along the trace line.

Click and drag to zoom in, double click to zoom out.

3. Trace Detail Box – shows sensor id and name, time, date and readings for cursor line.

Select the cross above the trace element to remove from graph, the eye icon will hide/show a trace. The add button allows other traces from the sensor to be added.

New Graph Trace
Clicking open the Select Trace tool for comparison traces to be added. A comparison can the same sensor against a different time period and/or another sensor over the same or different time period.

4 sensors traces can be compared on the same graph.

Multiple sensor comparisons show, each; time, date and data for cursor line, zooming one will zoom all. Change trace colours via colour box in trace box.

The red cross in the top right corner opens the Status page.

Hint - No system changes or data changes can be administered within the graphing tool, only data can be viewed, users should familiarise themselves with this tool by clicking on the various elements.

6. ALARMS

SITE => ALARMS
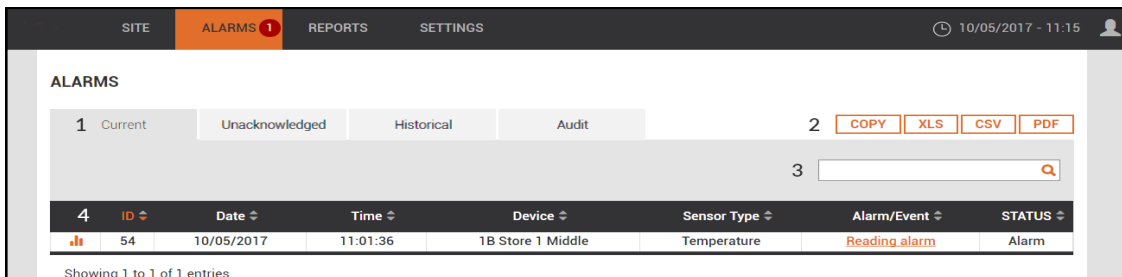
1. Selection Tabs;

> Current (default)– the current alarms (including unacknowledged alarms). If alarm status has cleared the sensor will show until the alarm is acknowledged.
> Unacknowledged – all alarms to be acknowledged by authorised users. When acknowledged the alarm will disappear from this tab.
> Historical – a record of all system alarms.
> Audit – a record of all alarms and user system change events.

2. Exports the current view.

3. Searches the current data.

4. Description Bar – allows sort by; Alarm/Event ID, Date, Time, Device, Sensor Type, Alarm/Event.

> Graphing Button – opens graph showing alarm occurrence.
> ID – system generated unique ID for each event.
> Date & Time – when alarm occurred.
> Device - device Ref and Name.
> Sensor Type.
> Alarm Event – reason for alarm event (Reading, Communications, etc), select the alarm message to open Alarm Details Box for more information and to add alarm notes.
> Status – sensors current status; Alarm - still in an alarm, Cleared - alarm cleared but unacknowledged.
>
> *Note - only users with acknowledge access privilege can acknowledge and add alarm notes.*

6.1. Alarm Details

> SITE => ALARMS => select ALARM/EVENT
>
> Shows:
>> Name – Device ID and name.
>> Serial Number – Device serial number.
>> Sensor Type - e.g. Temperature.
>> Details – the alarm causal fault.
>> Asset Ref - shows user defined range for sensor, see 11.2 Add a Device/Sensor for more information.
>> Reference (not on communications or fault alarms) – reading at point of alarm & min or max reading achieved during the alarm period.
> *Note - if the base station is switched off during an alarm period then the alarm max/min will not be shown.*
>
>> Duration - the length of time the device was in alarm
> *Note - if the base station is switched off during an alarm period then the alarm duration will not be shown.*
>
>> Triggered – the date and time the alarm was generated by the base station
>> Generated - the date and time the max, min threshold was exceeded starting the alarm delay countdown.
>> Acknowledged – date and time acknowledged, if blank then alarm is unacknowledged.
>> Acknowledged by – user who acknowledged, if blank then alarm is unacknowledged.
>> Cleared - date and time the alarm cleared, if blank the alarm is still active.

Email – alarm email status

Add – allows user notes to be added. Max 20 notes per alarm. Each note is unique and stored with the users ID details, notes cannot be deleted nor amended. Notes show on system reports.

Graphing Icon (top left corner) – opens the graph for the alarm.

6.1.1.   Adding an Alarm Note

SITE => ALARMS => select ALARM/EVENT => ALARM DETAILS => ADD

Max 255 alpha/numeric character message length.
Max 20 records per alarm.
Notes show in audit view and on system reports.

6.2.   Unacknowledged Alarms

SITE => ALARMS => UNACKNOWLEDGED

Unacknowledged alarm page is similar to the Current Alarm page, the differences being
1. Acknowledge Alarm button is available
2. The graphing key is replaced with a selection button

Exporting, sorting and the search capabilities are the same

6.2.1.   Acknowledging an Alarm

SITE => ALARMS => UNACKNOWLEDGED => select Alarm/s => ACKNOWLEDGE ALARMS

Default - Acknowledge Alarm key is shaded and the Selection Buttons are a solid colour.

Acknowledging alarms individually - click Selection Button for the alarm and then Acknowledge key.

Acknowledging a number of alarms – click Selection Button for alarms and then Acknowledge key.

Acknowledging all alarms – click Selection Button on Description Bar, all alarms are selected, click the Acknowledge key.

Acknowledge key press requires user to enter password to confirm action.

Note - Acknowledged alarms are removed from Unacknowledged tab, if still current they are in Current, If cleared they are in Historical

6.3.   Historical Alarms

SITE => ALARMS => HISTORICAL

Gives access of all alarm events in systems internal and back-up memories (if back-up memory installed).

The layout is similar to Current page with two additions. These are;
1. User Defined Date Search – search based on selected start and end periods
2. Show per page tab – alters number of records per page. The next and previous keys allow users to scan through alarms by page.

6.4.   Audit Information

SITE => ALARMS => AUDIT

Identical to the Historical Alarm page in look and function.

The Audit page contains all alarms events and system change events. System change events are recorded and show details of all changes made with the parameters changed documented.

7. REPORTS

SITE => REPORTS

All reports generated by the system are in PDF format with date of creation and user details (including electronic signature).

Note - For reports generation the network browser MUST support pop-ups and pop-ups must be enabled for the assigned IP address.

7.1. Select Date

Using date selection tool select required report date. Once a date is selected the report generation buttons become available.

Note – any date from the full recorded system history can be selected.

7.1.1. Daily Overview Report

Includes a list of all sensors on the date selected. Shows: set points, max, min, average reading per sensor and readings every 2 hours.

7.1.2. Daily Sensor Report

Shows; set points, max, min and average readings per sensor. It has a graphical representation of the data over the day and includes sensors readings at 15 minute intervals.

Alarm events & notes are shown at the end of the report.

7.1.3. List Over Time Period

Shows; a PDF page for each date required with set points, max, min, average reading per sensor and readings every 2 hours.

7.1.4. Graph Over Time Period

Shows;a PDF page graph for each sensor over the dates specified with the set points, max, min and average readings for the period shown.

7.1.5. Raw CSV

Creates a CSV download of data over the selected date range for all sensors. Readings are download at a 15 minute interval.

8. Users Login Details

8.1. Updating/Changing User Login Details

SITE => SETTINGS => MY DETAILS => EDIT

User editable;
Username – Max 25 alpha/numeric characters, upper & lower case.
Unit Passcode – Max 8 numeric characters only - used directly on base station.
Web Password – Max 25 alpha/numeric characters, upper & lower case - used when accessing with a internet browser.

Once new Username, Unit & Web Codes are set re- enter the current or administrator provided web password to confirm changes.

8.2. Forgot Login Details

For Users - contact system Administrator, the Administrator can reset a default login, then see section 8.1 Updating/Changing User Login Details.

For Administrators - another Administrator can reset a default login, if only 1 administrator has been registered on the system then contact system supplier or manufacturer for support.

9.   Portal Access - Using "mydataportal.co.uk"

Mydataportal.co.uk is a reverse proxy that allows access by users to the base station, access is enabled for devices with a browser from any location.

See section 16.5 - Portal Access for setting the base station to use this function
See section 13.3.2 - User Management for setting user access rights for this function

WWW.MYDATAPORTAL.CO.UK => Username => Password => Site ID => Login

Access information
        Username – the users base station login username
        Password – the users base station login password
        Site ID – the site ID is a unique base station - shown in the site INFO page

On login the user have access to the base station with their appropriate access rights.

Set-Up Guide

Overview

For System Administrators & System Installers
Set-up & Installation should be completed by competent persons, please read this manual in full before commencing any work on the base station.

Note (No.) Number in brackets refers to the System Overview D3 Base Station Assembly of the User Guide.

New System Set-up
Hint - Once set-up the base station retains the configuration of all sensors, users, etc. even when powered down. Setting a new system up over a laptop connection and then connecting to the site network is by far the simplest and quickest set-up method.

New system set-up work-flow - best practice;
Network the base station.
Check and set time & date.
Complete the default Site Settings.
Create additional sensor types required in the Customer Sensor Database.
Add & pair all required sensors.
Create alarms profiles.
Create required Schedules (if needed).
Edit sensor set points, attach to alarm profiles & auto inhibit schedule (if needed).
Complete Email Set-up & send test email.
Create Users & access levels.
Attach any peripheral hardware & Mount the Base Station.
Install the sensors & repeaters as necessary.
Issue Users with login details.

If a site plan is available, mark the positions of installed sensors and repeaters along with their assigned ID's (this will simplify finding these items at a later date if required).

10. Powering the D3 Base Station

10.1. Powering Up

Connect the power supply male jack to power connector socket (7), secure power cable with the internal securing lug

Plug the power supply into the mains socket, the unit should power on automatically, if not, press and hold the power button (5) until the unit powers on.

The LED shows a solid colour indicating the system is powered.

10.2. Powering Down

Press power button (5) and select confirm on display.

Emergency power down - Press power button (5) for 15 seconds.

10.2.1.   Internal Battery Back-Up[2] (operation & testing)

On connection to mains power the internal battery back-up will commence charging, on mains power loss the battery back-up will auto switch and power the base station.

Note - It is recommended that the battery back-up operation is tested regularly (manufacturer recommends monthly). To test; remove the mains power to the base station, the base station should continue to function.
Replacement of the battery - the battery back-up must only be completed by competent persons, refer to the system distributor.

11. Networking the Base Station - IP Connectivity

The D3 can operate in 3 different IP modes;

DHCP Client - (default from new) the network provides all the relevant IP settings - see section 3. Network Interface.
Note - on occasions the network can re-assign the base station a new IP, meaning browser favourites would need to be updated.

DHCP Server – for direct connection to a pc/laptop. This option is frequently used when setting the system up on installation.

Systems permanently connect to a dedicated PC or Laptop have limited alarm capabilities - Not connection method is not recommended for on-going monitoring applications.

Note – do not connect a base station in DHCP Server mode directly on to the network as a conflict in IP settings could occur.

Static – set to a static IP address on the site network. A static IP does not change (unlike DHCP Client).

11.1. IP Setup via the Base Station

11.1.1. DHCP Client Mode

HOME => SET UP => Authorise => IP => Change => NETWORK MODE => Select DHCP Client

The network will automatically assign the IP configuration. The IP address assigned is visible in the Info view (HOME => INFO).

11.1.2. DHCP Server Mode

HOME => SET UP => Authorise => IP => Change => NETWORK MODE => Select DHCP Server

The IP Address is fixed at 192.168.100.100

11.1.3. Static Mode

HOME => SET UP => Authorise => IP => Change => NETWORK MODE => Select Static

The last Static configuration set, the Static IP details can only be entered/updated over the network interface.

11.2. IP Setup via the Network Interface

SITE => SETTINGS => NETWORKING => IP SETUP

11.2.1. DHCP Client Mode

SITE => SETTINGS => NETWORKING => IP SETUP => DHCP CLIENT

Host Name – editable, visible on the network for IT departments.

The IP Address, Subnet, Gateway, Preferred & Alternate DNS - auto supplied by the network.

The HTTP Port - auto supplied, editable if required.

11.2.2. DHCP Server Mode

SITE => SETTINGS => NETWORKING => IP SETUP => DHCP SERVER

11.2.3. Static Mode

SITE => SETTINGS => NETWORKING => IP SETUP => DHCP STATIC

The IP Address, Subnet, Gateway, Preferred & Alternate DNS and HTTP Port are manually configured.

Note – If a static IP has been set other modes can be used, on return to static mode the last configuration is used.

11.2.4. NTP Service Hostname/IP

SITE => SETTINGS => NETWORKING => IP SETUP =>Edit

NTP (Network Time Protocol) service allows for automatic updating of time on the base station. By entering a NTP service hostname/IP the manual time set on the base station is overwritten and updated.

Update rate - once per hour.

Status
This shows the current operational status to the connected NTP service.

SETTINGS

SITE => SETTINGS

Users view of the settings page will vary depending on access rites, only Administrator's have full Settings access outlined below.

Settings Menu
Sensor Administration – for management of sensors/devices .
User Settings – user management.
Alarms – setting general alarm actions and creating alarm profiles.
Site Settings – basic system set up, management of scheduler and Time/Date.
Networking – IP configuration, email server set-up, connection to 3rd party notification bureaus and to allow portal access to the base station.
Administrator – configuration download/restore, software updates and maintenance functions.

Menu Content - Left hand window

Editing/configuration area on right hand side of screen.

12.   Sensor Administration

NOTE - Network Diagram - 868Mhz & 2.4Ghz SYSTEMS ONLY - pictorial view of sensor communication routes and status.

12.1. Manage Devices

MANAGE DEVICES ↻   **1** | PDF | ADD DEVICE | ADD GROUP |

Default View ▼ **2**   **3** ■ Expand All

4 Ref	Description	Type	Data Source	Batt	Link	State
OBD	+ Office's & Development			--		✖
SF1	Kitchen Fridge 00:01:0B:B8	Temperature	Wireless	69%	🔗	●
SF2	Kitchen Freezer 00:01:03:19	Temperature	Wireless	89%	🔗	●
SR1	Server Room 00:01:00:94	Temperature	Wireless	68%	🔗	●

SITE => SETTINGS => MANAGE DEVICES

1. Manage Devices PDF
This creates a PDF of all devices on the system and shows their status and connection statistics.

Add Device/Group keys.
Add device is used for creating new devices on the system.

Device groups allows for sensors to be grouped together, it also allows for an average from a chosen sensor type to be displayed. A sensor group appears as a black naming convention in the device Description list

2. View Selection.
Default View - view, add, remove and manage devices/groups.
Communication Status - quality and strengths of wireless signal by device.
Calibration Offset - single point calibration off-set by device.
Remote Address - access address for 3rd party notification bureaus systems (refer to system distributor for more information).

Note - Best practice is to achieve a signal quality greater than 80% and strength greater than 40%. If below these than a repeaters should be considered.

3. Expand All – expands groups to show all devices.

4. Device information.
>   Ref – short device id.
>   Description – device name.
>   Type – device type.
>   Data Source – communication method e.g. Wireless.
>   Batt - Battery level remaining (for wireless sensors only)
>   Link key – Status of linked devices, colour coded:
>>   Grey – Device not linked.
>>   Amber – Linked but waiting for data from device.
>>   Green – Linked data received.
>   State – connected status of the device/group, colour coded:
>>   Green – Device is Active.
>>   Purple – Device is Disabled.
>>   Grey – Device is Decommissioned.
>>   Delete – Allows for device/group to be deleted.

12.2. Add a Device/Sensor

SITE => SETTINGS => MANAGE DEVICES => ADD DEVICE

Adding a device is a 2 stage process, device creation then linking

Note - Devices can be added to groups on creation– see section 11.3 Adding a Device Group. Or edited to a group later – see section 11.5 Editing a Device/Group.

Hint - best practice create all of the devices first then link each.

12.2.1. Adding the Device/Sensor

Select Add Device key
>   Short Reference – required, must be unique & max 5 alpha/numeric characters.
>   Name – required, max 25 alpha numeric characters.
>   Group – default = None (not added to group), all created groups appear in the drop down and can be selected.
>   Sensor Type – default = Not Configured, required, available sensor types appear in the drop down.
>   Standard probe types are:
>>   Temperature –   for NTC, Thermocouple & PT100 & PT1000 sensors only.
>>   Humidity -   %RH only.
>>   Repeater -   wireless repeaters (wireless extenders) only.

Other sensor types are created in the Custom Sensor Database – see section 11.6 Customer Sensor Database. Once created the custom sensor type will appear in the drop down.

Once added devices appear in the Manage Device view.

12.2.2. Linking a Device

Legacy Sensors (P2-WS100, P2-WS101 & all sensors starting M02WS???) & the Intelligent Sensor Range (P3-DS???-HR) can be linked, the linking process differs slightly.

All device types are linked through the Link Manager window.

1 - Device name.

2- Details of linked sensor, "not assigned" = no device linked, if a device is linked then its internal serial (for Legacy) or serial no (for Intelligent) will be shown.

3- Details Intelligent Sensors available to link.

12.2.3. Legacy Sensors - compatible with 433Mhz base stations ONLY

The wireless sensor must be within communications distance for pairing to be completed.

Step 1
Have the device to be linked at hand.
Hint – use a permanent marker pen to add the relevant system device ID to the wireless sensor once paired.

Step 2
Click on the link key for the sensor to pair, the link manager window will open.

Step 3
Press and hold the wireless communication button on the sensor, keep depressed, the LED will show green. Keeping the LED showing green click the Join Transmitter key, link manager window updates and start to count down. The countdown lasts 60 seconds, when the countdown begins release the wireless communications button.

Step 4
A messages will appear in the link device window.
  Legacy Sensor Paired - linking successful, to test, press and release the sensors wireless communication button, the LED will flash twice to indicate communication is established.
  Timeout! - linking failed, repeat steps 2 & 3. If repeated attempts fail contact distributor for support.
  Incompatible Device - linking failed, the device type being added does not corresponds to the type of device created. E.g. humidity probes can only be paired to a device type that is humidity.

Complete steps 1-4 for each device to be linked.

Hint – BEST PRACTICE - once the device is successfully linked write the system ID number on to the wireless device (the wireless device has an ID box for this to be entered).

12.2.4. Intelligent Sensors

The wireless transmitter must be within communications for linking to be completed.

Step 1
Have the transmitter & device to be linked at hand.
Hint – though not necessary it easier to have the intelligent device connected to the wireless transmitter prior to linking the transmitter to the base station.

Step 2
Click on the link key for the sensor to pair, the link manager window will open.

Step 3
Press and hold the wireless communication button on the sensor, keep depressed, the LED will show green. Keeping the LED showing green click the Join Transmitter key, link manager window updates and start to count down. The countdown lasts 60 seconds, when the countdown begins release the wireless communications button.

  433Mhz transmitters - the transmitter will pair on the button release.
  868Mhz & 2.4Ghz transmitters - the green LED will display quick flashes as transmitter establishes a connection, once connection is complete a longer 1 second flash will display and then the flashing will stop. If the long flash is not seen then transmitter has failed to connect.

Step 4
A messages will appear in the link manager window
  Wireless Transmitter Paired - pairing successful, to test, press and release the sensors wireless communication button, the LED will flash twice to indicate communication is established.
  Timeout! - linking failed, repeat steps 2 & 3. If repeated attempts fail contact distributor for support.

Step 5
Once the transmitter is paired, available Intelligent sensor serial numbers, that can be linked, appear in the Available Sensor List. Select the serial number of the sensor attached to the transmitter and click Link Sensor. The Serial Number of the sensor will appear in the Linked box (2).

The following possible message may appear in the link manager window

Incompatible Device - linking failed, the device type being added does not corresponds to the type of device created. E.g. humidity probes can only be paired to a device type that is humidity.

Complete steps 1-5 for each device to be linked.

12.3. Adding a Device Group

SITE => SETTINGS => MANAGE DEVICES => ADD GROUP

Devices can be added and removed from groups at any time.

Groups can be deleted, deleting a group does not delete the devices, they move to an un-grouped state.

On selecting the Add Group key the add group window opens.
Short Reference – required, max 5 alpha/numeric characters.
Name – required, max 25 alpha/numeric characters.
Active – default = Disable.
Disable – no averaging of device readings are displayed
Enabled – group average will be displayed, allows selection from a drop down for the Active Sensor Type to be selected.   Active device groups can have alarm set-points and delays set and alarm like a device.

Note – Groups can be edited to add an active device type – see section 11.5 Editing a Device/Group.

12.4. Deleting, Disabling & Decommissioning Devices & Groups

SITE => SETTINGS => MANAGE DEVICES => CHANGE STATE

Changing the state of a device is done by clicking the State circular icon corresponding to the device to be amended.

The state drop down allows the selection of the new device state.

12.4.1.   Deleting a Device
SITE => SETTINGS => MANAGE DEVICES => CHANGE STATE => Select Delete

868Mhz & 2.4Ghz, the wireless transmitter can be de-linked once the associated device has been deleted. To remove the transmitter press and hold the wireless communications button. Keep the button pressed until the green LED on the wireless device flashes on and then release. The transmitter LED will display quick green flashes, these will continue until the de-linking is complete.

WARNING - when deleting a device from the system the device is permanently being removed and will no longer be accessible. Historic data will not be viewable in a graphical format, but will appear on generated reports.

12.4.2.   Disabling a Device

SITE => SETTINGS => MANAGE DEVICES => CHANGE STATE => Select Disable

Disabled devices can be re-activated at a later date.

12.4.3.   Decommission a Device

SITE => SETTINGS => MANAGE DEVICES => CHANGE STATE => Select Decommission

Removed and the input freed for further devices to be added. The device data remains accessible and can be viewed graphically and in reports. A decommissioned device cannot be reactivated, a new sensor would need to be paired.

12.4.4. Deleting a Group

Clicking the red-cross in the State column deletes a group, devices in the group being deleted are moved from a grouped state to an un-grouped state, the devices are not deleted nor is their data affected.

Note – for an Active Group any averaged group data will be inaccessible in either report or graphical format once the group is deleted.

12.5. Editing a Device/Group

SITE => SETTINGS => MANAGE DEVICES => SELECT DEVICE/GROUP

Click the device/group Description (orange & underlined) & select Edit.

Changing a Device Reference and Name;
Ref, Name can be edited as per Add Device Section.

Adding or removing a Device from a Device Group;
Add or remove by selecting from the drop down menu;

Changing the Device Type;
For use with Linear & Pulse Input Sensors, the sensor type remains the same but can be configured to a different input option from the Customer Sensor Database.

Changing the Device Display Resolution;
The default is as set in general settings, see section 14.1 System Setup. The default is overridden by selecting a different resolution at the device level.
A resolution from Integer (no decimal places) to 3 decimal places can be selected

Asset Ref - a free text reference can be added, if added this appears on the device alarm detail page.
Default = Blank.
Maximum, 25 alpha numeric characters in length.

Legacy Sensors ONLY
Reset Battery Levels - if a battery is changed in a legacy sensor the system cannot detect the change, the battery level indicator will not change on the Manage Device screen until the battery level reset button is pressed.

12.6. Custom Sensor Database

SITE => SETTINGS => CUSTOM SENSOR DATABASE

For the creation of custom device types; Linear In-put (4-20mA, 0-10V, etc.), Pulse Counting and Digital Input for 3rd party meters and sensors. Allows for a limitless range of input readings from 3rd party meters, plant and sensors.

Note - Once a device type is created multiple sensors of the same type can be configured to use it.

12.7. Adding a Custom Sensor Type

SITE => SETTINGS => CUSTOM SENSOR DATABASE => ADD
Sensor Name – required, max 25 alpha/numeric characters.
Sensor Units – required, max 10 alpha/numeric characters – most 3rd party sensors have defined output units.
Hardware Type – can be;
Pulse Kwh – energy consumption from pulse emitting energy meters.
Pulse Flow – liquid/gas flow from pulse emitting flow meters.
Digital – volt free digital outputs.
Voltage – voltage over a range from 0-10v.
Current – current over a range from 0-25mA.
Resistance – resistance over a range of 0-10,000 ohms.

On selecting a hardware type further configuration boxes will appear for completion

12.7.1. Creating Pulse Kwh Sensor Type

Pulse ratio – energy meter documentation will have the number of pulses to represent 1kWh of energy used, this number is the ratio.

12.7.2. Creating a Pulse Flow Sensor Type

K Factor - flow meter documentation will have the number of pulses to represent the level of flow measured, this is the K factor.
Time Frame (seconds) – Flow meters typically represent flow over a period of time, this time period will be defined in the documentation (commonly in seconds).

12.7.3. Creating a Digital Sensor Type

These read an open/closed reading from a digital output, the equipment documentation will define what the open or closed reading represents – e.g. typically on plant equipment an open reading means the plant is running, closed indicates a failure and the plant has failed.

Tag On – Screen message in the open status.
Tag Off – Screen message in the closed status.
Status descriptions - max 25 alpha/numeric characters.
Invert Signal – some digital outputs are closed/open format, the inverse of the norm. Invert Signal allows for this inverse input.

12.7.4. Creating a Voltage, Current & Resistance Sensor Type

These 3 sensor types creation is essentially the same.

The 3rd party device documentation will have the output range and detail what the lowest and highest values represent.

E.g. - pressure sensor: 1-30 bar with 1-8v or a 4-20mA.
Lowest
　　Reading (x1) - the lowest reading value (1v = 1, 4mA = 0.004).
　　Output (y1)   - the lowest output value (1 bar in example).
Highest
　　Reading (x2) - the highest reading value (8v = 8, 20mA = 0.02).
　　Output (y2)   - the highest output value (30 bar in example).

Zero Threshold - for a notional zero threshold to be set, any reading under the threshold would show as zero.
Fault Threshold - to warn of 3rd party sensor failure, lower and upper inputs can be entered to trigger a fault alarm.

Note - the x1 and x2 inputs are defined as whole integer units e.g. Volts or Amps, device types of Millivolt (mV) or Milliamp (mA) value needs to reflect this.

1 x mV or mA has an input value of 0.001

13. User Settings

13.1. My Details

SITE => SETTINGS => MY DETAILS

See section 8.1 Updating/Changing User Login Details.

13.2. Setting Password Expiry
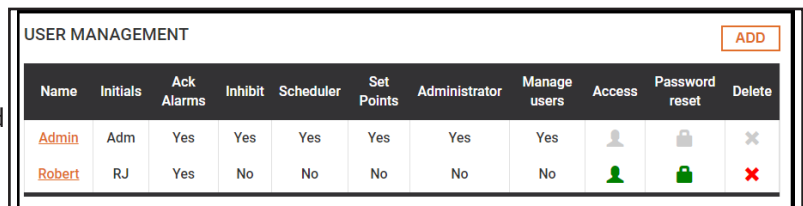
SITE => SETTINGS => PASSWORD EXPIRY

Set to expire passwords after defined period, 0 (zero) days = Off (never expire). Max period = 365 days.

On expiry users are required to update/create a new password on next login.

13.3. User Management

SITE => SETTINGS => USER MANAGEMENT

System are shipped with a single Administrator access level enabled, a minimum of a single Administrator must be enabled at all times. When only one Administrator remains then this user cannot be deleted or the user account disabled.

USER MANAGEMENT										ADD
Name	Initials	Ack Alarms	Inhibit	Scheduler	Set Points	Administrator	Manage users	Access	Password reset	Delete
Admin	Adm	Yes	Yes	Yes	Yes	Yes	Yes	👤	🔒	✖
Robert	RJ	Yes	No	No	No	No	No	👤	🔒	✖

An Administrator is defined as a user with Alter System Configuration & Manage Other User Capabilities enabled, see section 12.3.2 Adding Users.

13.3.1. Default Administrator Passwords/Login Details

Default New System Administrator Login Details
Username: admin
Network Password: 1234
Base Station Passcode: 1234

Note - It is recommended that default log in details are changed.

13.3.2. Adding Users

SITE => SETTINGS => MANAGE USERS => ADD

Number of Users: 20 max, user privileges are set by Administrator/s.

User Details;
   Forename, Surname and Initials – Captured on reports, alarms acknowledgements and system changes. Users are automatically assigned a unique electronic signature that is also captured.
   Email Address – for alarm notifications, if no user email is entered then username and passcode need to be manually configured by the system administrators.

User Privileges;
Default = No, privileges need to be set to Yes to enable.
   Alarm Acknowledge – ability to acknowledge alarms and add notes capabilities.
   Inhibit Alarms – inhibit & clear inhibits on sensors.
   Adjust Scheduler – administer the schedules.
   Adjust Alarm Set Points – administer sensor set points and alarm delays.
   Alter System Configuration – administer the full system settings with the exception of Manage Users.
   Manage Other Users – manage password resets and to disable users, cannot delete users nor disable full Administrator level users. Only Administrators can add and delete system users.
   Receive Email Alarms – receive system alarms, also see section 13.2 Alarm Profiles.
   Portal Access - allows a user to access the system remotely using the "mydataportal" access function - see Section 16.5 Mydataportal Access

Note - Authorise - Administrator/User Managers need to re-enter their username and password details to authorise user creation.

13.3.3. Editing an Existing User

SITE=> SETTINGS => MANAGE USERS => SELECT USER

Administrator only
Click the user name (orange & underlined) and select edit.
User details and access rights can be amended.

13.3.4. Enable/Disable Users

SITE => SETTINGS => MANAGE USERS => ENABLE/DISABLE

User Management only
Click the Access icon to edit.

13.3.5. Resetting a Users Passwords

SITE => SETTINGS => USER MANAGEMENT

User Management only
Click the Password Reset key to edit;
   Send Email – emails user a temporary username and password to changed on login.
   Manual Override – user name and password are manually entered.

13.3.6. Deleting a User

Administrators Only
Click Delete icon to edit;
Administrator user name & password confirmation is required. Notes can be added and will be recorded against the event in the system Audit history.

WARNING – deleting a user removes them from the system, their access cannot be re-enabled

14. Alarms

14.1. General Alarm Settings

SITE => SETTINGS => ALARMS => GENERAL ALARM SETTINGS
For device alarm set points see section 4.2 Sensor Details.

Default = Off, the alarm actions required need to be configured to On.
Internal Relay 1 & 2 – controls the 2 internal relays. An activation can be selected for each;
   Sounder – relay activation follows the internal sounder. When the internal sounder is muted the relay is deactivated, if the internal sounder re-activates the relay re-activates.
Note – the internal sounder cannot be set to off if the relay option of sounder is enabled, if the sounder is off the relay will not activate on alarm.
   Dial Out – pulsed relay output commonly used by 3rd party alarm outputs and auto-diallers.
   Beacon – continual relay output, continues until the alarm event has cleared.
Note – if a sound beacon is added and is required to be muted then the Sounder relay option should be used

Relay Operation on Battery – If on the relays operate on power loss, this will reduce the operational period of the base station on battery back-up.
Sounder – on/off function of internal sounder
Alarm roaming at home – Default = Off, allows alarms when roaming sensors are at home
Note – covers all roaming probes when at home, it is a general setting and cannot be applied to sensors individually.
Repeat Alarms & Repeat Period – repeats alarms at defined repeat period (set in minutes).
Repeat Alarms Until;
   Not Current - all current alarms will repeat.
   Acknowledged - all until the alarm is acknowledged.
   Cleared - all until alarm clears (even if alarm remains unacknowledged).
Comms Time Out – period before notification of sensor communication failure (set in minutes) - Minimum = 5 minutes.

Sensor Fault Time Out – period before notification of sensor fault (set in minutes) - Minimum = 5 minutes.
Notify on Battery – notifies on power loss, Default = Disabled. attach to an Alarm Profile to enable.
Notify Backup Fail – notifies on backup failure, Default = Disabled, attach to an Alarm Profile to enable.

14.2. Alarm Profiles

SITE => SETTINGS => ALARMS => ALARM PROFILES

Alarm profiles determine the actions for associated sensor/device alarms, also see section 13.2.3 Adding/Editing a Sensor/Device Alarm Profile.

ALARM PROFILES   ADD

Name	Reading	Comms	Sounder	Relay	Relay delay	Email	IP	Scheduler	Delete
Stores	Yes	Yes	None	None	0	Always	None	Off	✖

Note - Default = no alarm profiles are set from manufacture.

Numerous alarm profiles can be created, however a device can only be linked to 1 profile.

14.2.1. Creating an Alarm Profile

SITE => SETTINGS => ALARMS => ALARM PROFILES => ADD

Name – required, max 15 alpha/numeric characters.
Device Actions;
  Alarm on reading – alarm on sensor/device reading exceeding the warning/critical set points.
  Alarm on communications – alarm on sensor/device communications loss.
  Alarm on sensor fault – alarm on sensor in a fault condition.
  Alarm on Warnings - alarms based on system warnings - i.e. back-up failure.
  Send cleared alarm notification – send an alarm cleared notification.
Output;
  Schedule – Default = Off (outputs operate 24/7), outputs can be linked to follow a schedule (see section 14.2 Schedules).
  Output to Sounder – Default = None (Off), can be set to Always (On) or Schedule (set above).
  Output to Relay – Default = None (Off), can be set to Always (On) or Schedule (set above).
  Exclude Communications Alarms - Default = No, if set to yes then communications alarms will not activate the relay.
  Relay Delay – relay will delay (in minutes) before activation - Dial-out Mode only.
  Output to IP – see section 15.3 IP Dial Out Set-Up - Default = None (Off), can be set to Always (On) or Schedule (set above).
  Output to email – Default = None (Off), can be set to Always (On) or Schedule (set above).
  Alarm Action Notes - Default = No, Yes adds an action note sent with the alarm email message.

14.2.2. Editing an Alarm Profile

SITE => SETTINGS => ALARMS => ALARM PROFILES => Select Alarm Profile => EDIT

An alarm profile can be edited after creation if required.

14.2.3. Adding/Editing a Sensor/Devices Alarm Profile

SITE => Select Sensor => ALARM EDIT => Select Alarm Profile

Click the alarm edit button on the Sensor Detail page - see section 4.2 Sensor Detail, select the required profile from the drop down.

15.   Site Settings

15.1. System Setup

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP

General changes to operational configuration.

15.1.1.   Adding A Site Name

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Max 40 alpha/numeric characters, displayed on the base station screen, reports and alarm notifications.

15.1.2.   Dimming/Brightening & Display Sleep Mode

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Back-light Level – dims/brightens the screen on mains power connection.
Display Sleep Period – a period after which the screen goes into hibernation mode. Screen is woken by pressing.
Note – Default = On (will permanently scroll & display the latest reading received)
Back-light Level on Battery – dim screen on battery back-up to increase operational period on of the base station.
Note – only on D3 and D3 Medical

15.1.3.   Daylight Saving

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Default = Off, On the base station updates time for daylight saving.

Note - when using daylight saving the time will adjust by 1 hour in spring and autumn. In spring the time will move forward by 1 hour - meaning a gap of 1 hour will be seen on reports and graphs. In autumn time will move back by 1 hour meaning that an hours worth of data will be overwritten and cannot be seen nor recovered.

Warning - the effect of enabling Daylight Saving on data readings must be considered before activating this function.

15.1.4.   Change Displayed Temperature (°C or °F)

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Default = °C, °F selected via drop down.

15.1.5.   Change the Default Displayed Resolution

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Default = 1 decimal place, can be from integer to 3 decimal places.

Note – the resolution can be set/edited individually for each sensor, this will override the system default.

15.1.6.   Language

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Default - English

Note - Various Language settings are available, if required language is not in the drop down menu contact your system supplier for support.

15.1.7.   Date Format

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Affects the data format on the base station, report, graphs and alarm details.

Default = European, date shown in DD/MM/YYYY.
To edit select from the drop down menu;
   American - date shown in MM/DD/YYYY.
   DD/Month/YY - date shown in DD/Month/YY.

Note - delete browser viewing history and log out-in to the system to force date change to be seen.

15.1.8.   Redirect port 80 when SSL enabled

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Default = Off
To edit select On.
   On = redirects port 80 HTTP connectivity when SSL certificates are added for HTTPS secure connection. If left Off port 80 connectivity will still be enabled.

15.1.9.   Temperature Alarm

SITE => SETTINGS => SITE SETTINGS => SYSTEM SETUP => Edit

Default = Excursion Alarm.
To edit select Temperature Alarm from the drop down menu.
   When Temperature Alarm is selected this will appear against temperature excursions on the display, SITE view and Alarm notifications for any temperature sensor alarms.

Note - Only displays Temperature Alarm for temperature sensors, all other devices will show an excursion alarm.

15.2. Scheduler

SITE => SETTINGS => SITE SETTINGS => SCHEDULER

7 day schedule cycle with 10 exception dates per schedule, up to 5 different schedules can be implemented. Schedules can be linked to Alarm Profiles and/or Devices, multiple profiles or devices can be attached to the same schedule.

Note - A sensor or alarm profile can only be attached to 1 schedule.

15.2.1.   Setting/Edit a Schedule

SITE => SETTINGS => SITE SETTINGS => SCHEDULER => Select SCHEDULE => EDIT

1 - Highlighted Section in schedule set.
　　Active – the selected actions = On.
　　Inactive – the selected actions = Off.
2 - 7 week days.
3 - Exception date/date range.
4 - Schedule set.
5 - Selected Schedule fine tune.

To Add
Click and drag to highlight areas to a daily schedule - Max 5 areas per day, a selected highlighted area times can be fine tuned or deleted using the Selected Schedule fine tune.

Highlighted section
　　Status = Active -
　　　　Devices - auto inhibited (no alarms will be created or sent).
　　　　Profiles - outputs will be active and will operate.
　　Status = Inactive -
　　　　Devices - On and alarm notifications will be sent.
　　　　Profiles - outputs are inactive and will not operate.

To Edit/Delete;
Select highlighted section, drag and drop/fine tune to edit, click fine tune red cross to delete.

15.2.2.   Adding/Delete an Exception Date/Date Range to a Schedule

To Add;
SITE => SETTINGS => SITE SETTINGS => SCHEDULER => Select SCHEDULE => EDIT => ADD

Max 10 exception date/date ranges.

Step 1
　　Single Day - select the same date in each of the date windows.
　　Multiple Days - select the start date and end date in the date window.
Step 2
　　Add highlighted sections and fine tune

To Delete;
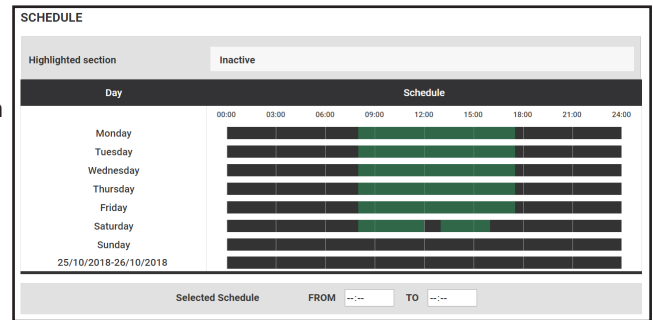SITE => SETTINGS => SITE SETTINGS => SCHEDULER => Select SCHEDULE => EDIT

Click red cross for date/date range to delete.

15.2.3. Example - Inhibit Sensors Outside Work Hours

Working Hours
Monday to Friday;   8:00am to 5:30pm
Saturday;   8:00am to 12:00 Noon
                              1:00pm to 4:00pm
Sunday;   All day

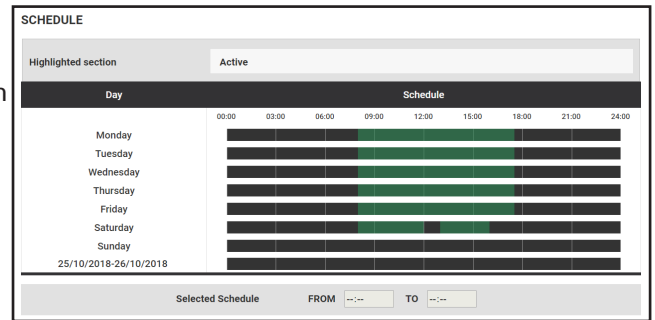**Device/sensors - linked to this schedule would be inhibited & no alarms created**

15.2.4. Example - Activate Profile Outputs Outside Work Hours

Working Hours
Monday to Friday;   8:00am to 5:30pm
Saturday;   8:00am to 12:00 Noon
                              1:00pm to 4:00pm
Sunday;   All day

Outputs - linked to this schedule would activate on alarm

15.3. Adding a Auto Inhibit Schedule to a Sensor/Device

SITE => Select Sensor => ALARM EDIT => Select Auto Inhibit - Default = Off

See section 4.2 Sensor Detail, select schedule from the Auto Inhibit drop down.
Note - No alarms are created during the auto inhibit period.

15.4. Setting/Editing Time & Date

SITE => SETTINGS => SITE SETTINGS => TIME/DATE

16. Networking

See Section 10 - Networking the Base Station for IP SET UP.

16.1. Email Setup/Editing

SITE => SETTINGS => NETWORKING => EMAIL SETUP

The D3 must be configured to send email alarms, failure to configure will result in email alarm notifications not being sent.

Enable Email - Default = No, Yes to activate.
SMTP Address- SMTP Server address or IP for outgoing mail.
SMTP Port - SMTP Server comms port.
Use Encryption - Default = No, if SMTP Server requires SSL or TLS encryption then select Yes.
Use STARTTLS - If encryption is required start TLS will start communications on a non-encrypted SMTP port in the default No status, if an encrypted SMTP ports is to be used then select Yes.
Username & Password - required, the SMTP server MUST accept username and password authentication.
Email From - email address associate with username and password.
Retries - if send fails the number of times to attempt a retry.
Retry Delay (minutes) - delay between retries.
Notify on Failure (warning) - Default = No, link to an alarm profile to enable failure notification.
Send Heartbeat - Default = No, link to an alarm profile to enable a heartbeat notification email to be sent daily at 8.00am.

Send a test message to ensure email setup completed correctly.

16.2. Bureau Access Setup

SITE => SETTINGS => NETWORKING => BUREAU ACCESS

Allows a remote bureau access/retrieve data to 3rd party monitoring application/cloud services.

Consult system distributor for more information.

16.3. IP Dial Out Setup

SITE => SETTINGS => NETWORKING => IP Dial Out

Automatically push alarm notifications in a text format over IP to an alarm bureaus.
Max - 3 alarm IP addresses.

Consult system distributor for more information.

IP Dial-Out Address (1,2 &3) - Default = 0.0.0.0 (Off) - alarm IP for the bureau for push notifications.
Port (IP1, 2 & 3) - Default = 5200, comms port for communication.
Retries & Retry Delay - number of retries on comms failure & the delay between retries (in minutes).
Notify on Failure (warning) - Default = Disabled, link to profile to generate failure notification.

16.4. Upload SSL Certificate

SITE => SETTINGS => NETWORKING => Upload SSL Certificate

To enable HTTPS communication between a browser and the base station, a SSL Certificate needs to be added to the system.

Step 1 – Create a sub-domain on your SSL certificate
A sub-domain for the base station will need to be created on the SSL certificate (issued by the certificate generating body).
A copy of the updated certificate needs to be downloaded from the issuer. The certificate file types can be ".pem, .crt, .cer, or .key" file format

Note - for SSL to work both the certificate and a private key are required see steps 2 & 3 below.

Step 2 – Certificate
Open the file to ensure it contains the certificate (the certificate can be opened using a text file editor like MS Word or Notepad).
The certificate will be contained within the file between the —- BEGIN CERTIFICATE—- and —-END CERTIFICATE—- statements.

Copy & paste the certificate including the —- BEGIN CERTIFICATE—- and —-END CERTIFICATE—- in to the Certificate box on the base station SSL certificate window.

Step 3 – Private Key
IMPORTANT– the private key MUST be in an RSA format.

The private key will normally be generated on your own servers or via a third party software programme, contact your IT department for a copy of your private key in an RSA format

Open the file to ensure it contains the RSA key (the .pem file can be opened using a text file editor like MS Word or Notepad).
The key will be contained within the file between the —- BEGIN RSA PRIVATE KEY—- and —-END RSA PRIVATE KEY—- statements.

Copy & paste the key including the —- BEGIN BEGIN RSA PRIVATE KEY—- and —-END RSA PRIVATE KEY—- in to the SSL key box on the base station SSL certificate window.

Step 4 – Authorise & Submit
To authorise the SSL Certificate re-enter the user password used to access the base station.

Press submit and after pressing submit the page should respond with 'success', if the SSL certificate has been successfully applied.

Switch the base station off, wait a few second then switch it back on. This reboots the system and the login over the network interface again is now in HTTPS mode.

Step 5 – Stop HTTP Connectivity
Redirecting port 80 is needed to stop HTTP non-secure connectivity once an SSL certificate has been added.

Route to redirecting port 80;
SETTINGS => SITE SETTINGS => SYSTEM SET-UP => Redirect Port 80 SSL

Select the On toggle to redirect port 80, HTTP connectivity over port 80 will no longer be accessible.

16.5. Portal Access -

SITE => SETTINGS => NETWORKING => Portal Access

Portal access allows remote access to the D3 base station using "mydataportal.co.uk" reverse proxy connection. Refer to your system supplier for more information on access and using "mydataportal.co.uk".

Users with remote access rights can use "mydataportal.co.uk" , to access the D3 base station from any device with a browser from any location.

Portal Access - Default = off, select enabled for portal access to be activated

Device ID - This is unique to the D3 base station and is required to access via "mydataportal.co.uk"
Connection Status - shows the current connection status of the base station with "mydataportal.co.uk"

17. Administrator

17.1. Software Update

SITE => SETTINGS => ADMINISTRATOR => SOFTWARE UPDATE => Select software package => UPLOAD

Contact system distributor for latest software package.

Drag & drop or click to find. Click Upload for software installation.
When completed delete browser history before logging back into the base station.

Note - Failure of delete the browser history may cause screens to be display incorrectly.

17.2. Back-up Configuration

SITE => SETTINGS => ADMINISTRATOR => BACK-UP CONFIGURATION => Download

Back-up of the systems settings, NOT a back-up of data.
This is a CRC file and should be saved to a secure location.

Note - it is recommended that a back-up of the configuration is taken once the system has been fully installed.
Note - configuration back-up is recommended after system changes are enacted.

17.3. Restore Configuration

SITE => SETTINGS => ADMINISTRATOR => RESTORE CONFIGURATION => Select Back-up => UPLOAD

Drag & drop or click to find. Click Upload to restore a previous configuration from the back-up selected.

17.4. Restore Configuration to a Replacement Base Station

Contact system distributor for assistance.

433Mhz systems - all system settings are uploaded and paired transmitters/sensors will resume communications with the new base station.

2.4Ghz systems - all system settings data are uploaded but the transmitters will need to be re-linked to the base station before any data can be received. The sensors will still appear on the base station and do not need to be re-created.

17.5. Maintenance

17.5.1. Cancel all queued alarms

Clears email alarm notifications not yet sent but queued to send.

During system set-up alarm events may occur before the system is networked, to stop these alarm emails being sent the queue can be cleared.

Note - only new alarms after the queue being cleared will create email alarm notifications.

17.5.2. Re-index archive files

Alarm and audit histories are re-indexed, this increases the speed of the search functions and is necessary after system configuration has been re-installed.

17.5.3. Start Manual Data Back-Up

Note - for D3 & D3 Medical system only with Micro SD cards installed.

Starts a manual back-up of recorded data to the internal micro SD card.

17.5.4. Re-boot System

Manually re-boots the system without the need for switching off and on.

17.5.5. Drive Maintenance

Starts a manual drive maintenance routine, this may be requested after a software update to improve performance of the system drives.
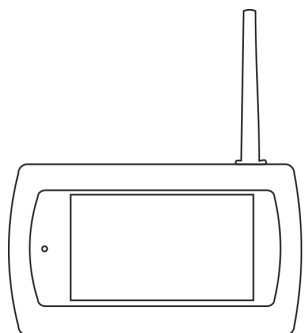
Note - re-enter the login password is required to authorise all maintenance functions completed on the base station.

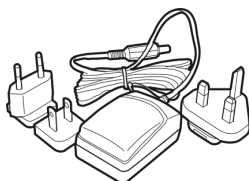# Installing the Base Station

Installation should be completed by competent persons only

When installing the base station ensure it and any connected hard wired powered accessories are fully powered off
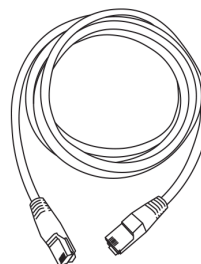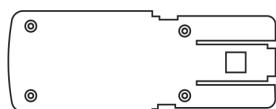
18. What's in the Box

1 x Base Station   1 x Power Supply   1 x Ethernet Cable

1 x Wall Fixing Plate

⚠ 19. Mounting the Base Station

Ensure power and a network connection are available in the chosen location.

19.1. Power Supply & Ethernet Connection

19.1.1. Power Supply

The power block supplied has international adaptors, the correct adaptor should be chosen and fitted.

The power supply cable has a maximum length of 1.4 meters.

Firmly push the power connector into the base station power connection point, route the power cable using housings cable securing lug.

19.1.2. Ethernet Connection

A 2 meter Ethernet cable is supplied from manufacture, longer Ethernet cables can be used if required.

Firmly push the Ethernet cable into the base station Ethernet port.

19.2. Mounting Wall Plate

30 cms

30 cms   30 cms

30 cms
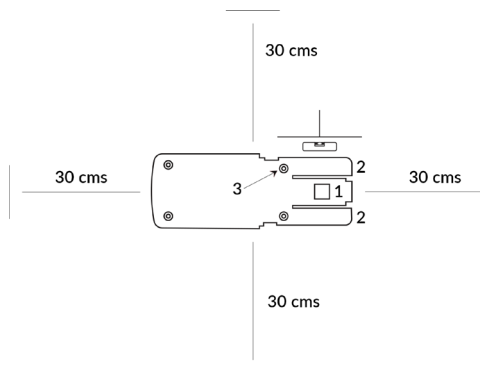
The mounting wall plate is shipped attached to the base station, it can be removed by lifting the Securing Lug and sliding from the base unit
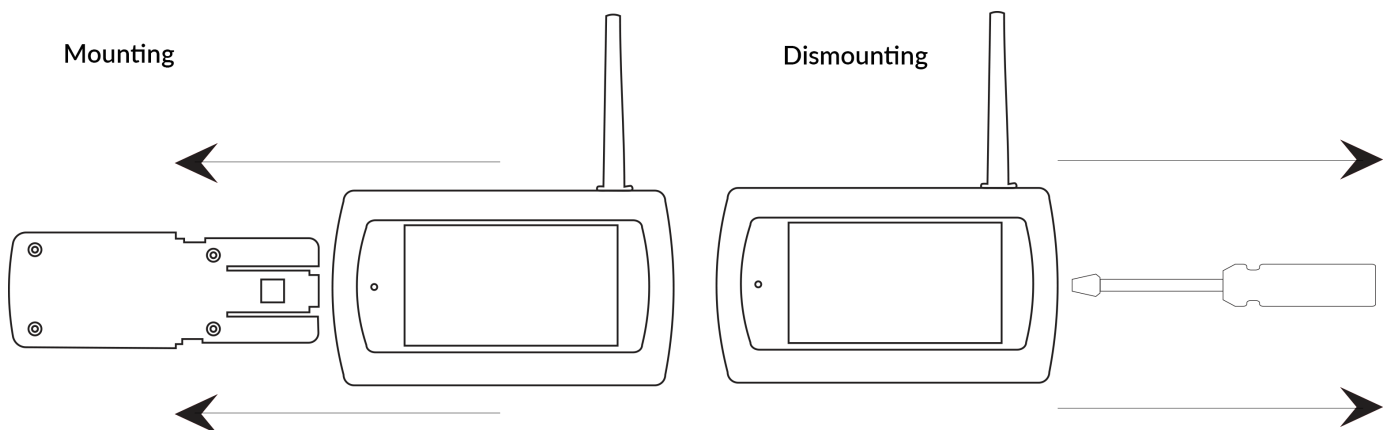
1 - Securing Lug.

2 - Securing Arms.

3 - Countersunk fixing holes.

To ensure maximum wireless transmission distances allow a minimum of 30cms free space above, below and to the sides of the wall plate once mounted.

Ensure the wall plate is mounted on flat wall, care should be taken to ensure the unit is level.

Note - Ensure the screw heads are below the level of the plate surface in the countersunk fixing holes. Failure to do so may result in damage to the back surface of the base station during the mounting process.

19.3. Mounting/Dismounting the Base Station

Mounting   Dismounting

19.3.1.   Mounting the Base on Wall Plate

Align the two mounting slots on the back of the base station with the guide runners on the securing arms of the fixing plate, slide the base station from right to left until the securing lug clicks into place.

The base station is now securely mounted on the wall plate.

Ensure all connecting cables and leads are securely and safely routed.

The base station and any connected accessories can now be powered on.

### 19.3.2.   Dismounting the Base from Wall Plate

Ensure the base station and any connected accessories are powered off.

Carefully insert a flat headed screwdriver between the base station and the tip of the fixing lug, ease the securing lug backwards and slide the base station to the right.

20. Connecting to the Internal Relays

The base station has two internal relays for connection to 3rd party accessories/systems.

Note - Refer to the 3rd party accessory/system manual for instructions on the wiring configuration required
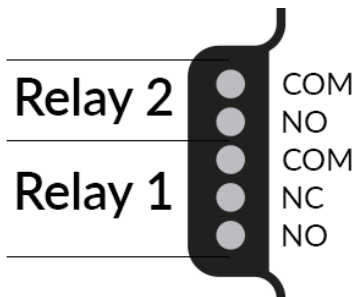
20.1. Relay 1 - Digital Relay Output

Configured for a Common (C) with a Normally Open (NO) or Normally Closed (NC) connection method. The accessory is connected using a two core cable, the relevant screw terminals are used.

20.2. Relay 2 - Solid State Relay Output

Mossfet switch provides a low powered output for signalling connected accessories

21. Changing the Micro MMC Card

From manufacture the base station is supplied with an industrial grade micro SD card as the back-up memory. This SD card can be changed by opening the micro card holder.

The card holder is opened by sliding the metal jacket to the right and then lifting it on its hinge from the left. The card can then be removed. To insert a new card the process is reversed.

Ensure the base station is powered down before removing the micro SD.

Note - any historic data contained on the micro SD will not be accessible from the system memory if the card is removed/changed.

22. Battery Replacement

Before working on the system isolate the electrical supply and also any voltage present on any incoming signals.

This work should be undertaken by suitably qualified personnel only, if in doubt contact the system distributor for assistance.

The system may have up to three batteries that may be required to be replaced. These are;

22.1. Coin Cell

Type - Lithium, 38mAh, 3V, 12.5mm battery
Manufacturer - Panasonic
Manufacture Part No. - CR1220

Replacement Method

Place the base station face down on a work bench. Unscrew the 4 retaining screws, one in each corner.

Remove rear case. Take caution to hold down the antenna casing to prevent it lifting and damaging the internal antenna as the rear case is being removed. For units with an internal battery backup hinge the rear case at the cable and place upside down alongside the unit.

Replace the coin cell. Ensure that the positive terminal is facing up.

Carefully replace the rear cover ensuring no trailing cables are snagged or trapped.

Re-tighten the four retaining screws.

Warning - do not over-tighten the retaining screws else the treads of the base unit may be stripped.

22.2. Battery Back-Up (if installed)

Type - Li-ion Battery Pack, 2000mAh, 3.7V
Manufacturer - Varta
Manufacturer Part No. - LIP 103450 SC

Replacement Method

Place the base station face down on a work bench. Unscrew the 4 retaining screws, one in each corner.

Remove rear case. Take caution to hold down the antenna casing to prevent it lifting and damaging the internal antenna as the rear case is being removed. Hinge the rear case at the cable and place upside down alongside the unit.

Disconnect the battery cable from the PCB. Unscrew and remove the battery retaining clip and remove the battery.

Replace battery. Ensure the new battery is in the same orientation as the original so that the cables are routed in the same position. Attached the retaining clip and screw down securely until the battery is held firmly.

Re-connect the cable to the PCB. Carefully replace the rear cover ensuring no trailing cables are snagged or trapped.

Re-tighten the four retaining screws.

Warning - do not over-tighten the retaining screws or the treads of the base unit may be stripped.

22.3. Wireless Transmitter Battery

Type - Lithium Thionyl Chloride, 2450mAh, 3.6V, AA Cell
Manufacture - Saft
Manufacturers Part No. - LS14500
Battery Life (in normal operation) - 5 years +
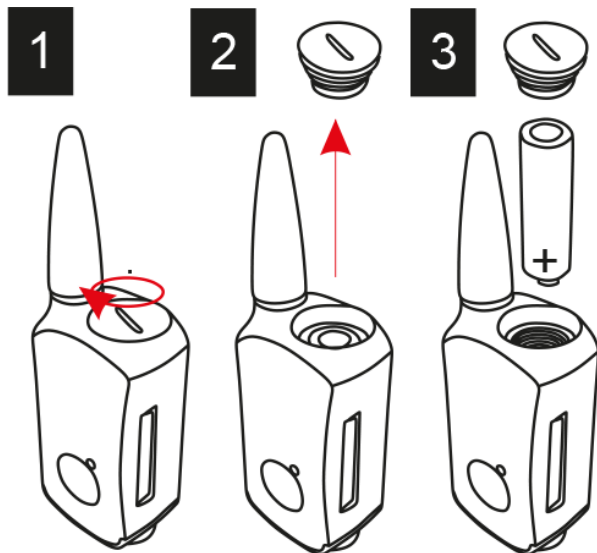
Replacement Method

1 - Ensure that the top cap is clean and wipe away any surface water. Using a large flat head screwdriver unscrew the lid with an anti-clockwise rotation.

2 - With the battery lid removed, invert the wireless sensor to allow the battery to be removed.

3 - Place the new battery into the sensor with the positive terminal first, Replace the cap and re-tighten in a clockwise rotation.

Legacy Sensors - after battery replacement reset the battery level - see section 12.5 Editing a device/group

Intelligent Transmitters - before inserting the new battery leave the transmitter without a battery for 2 to 5 minutes for the internal capacitors to drain, on battery insertion the base station should auto detect the new battery and reset the battery ware level.

Notes

Klipspringer

Compliance with confidence

Klipspringer
Rynor House
Farthing Road
Ipswich
IP1 5AP

Tel. :   +44 (0) 1473 461 800
Fax. :   +44 (0) 1473 747 200
Email: info@klipspringer.com

www.klipspringer.com