Software Administration Guide

About this document

This document is supplied as a part of the Reactec Eco-system.

Intended purpose

This guide is intended to help configure and use the Reactec Eco-system.

Intended audience

This document is intended for all users of the Reactec Analytics software.

Original instructions

Read this document before using the equipment

Retain this document for future use

Document information

Published on: 23 September 2022
Document ID: 290-101 - 30

Copyright and proprietary information

Trademarks

Data protection

Personal data is operator level data detailing tool usage. For the avoidance of doubt, for the purposes of the Data Protection Act 1998, the Data Controller is at all times, the Customer. Ultimate responsibility to ensure that any personal data is fairly and lawfully processed in accordance with the principles of the Data Protection Act 1998 rests with the Data Controller. The Data Processor shall process personal data in accordance with its obligations under the Terms and Conditions of Service and/or the Software License or otherwise in accordance with any written instruction of the Data Controller.
"Data Processor" shall mean any person who processes personal data on behalf of the Customer (who shall be the Data Controller) and may include (but not be limited to) Reactec Limited or any other supplier of the Services from time to time. The "Authorised Purpose" shall mean any purpose, which is reasonably necessary to perform the Services (as defined in the Terms and Conditions of Service) and/or comply with the Data Processor's obligations under the Software License or such other purpose as may be authorised by the Customer (acting as the Data Controller) in writing from time to time.

Contact address

Reactec Ltd.
Vantage Point,
3 Cultins Road,
Edinburgh,
EH11 4DF

Contact Reactec support if you have any questions:
helpdesk@reactec.com
www.reactec.com/support
Registered in Scotland (no. SC221428).

Conventions used

This guide uses the following formats for safety notices.

WARNING

Provides important information to prevent serious problems, for example, the loss of data.

Caution

Provides important information to prevent serious problems, for example, the loss of data.

Information

Provides additional information.

Tip

Provides useful hints and tips.

Contents

1 Reactec Eco-system

The Reactec Eco-system is a group of hardware and software components which allow the collection, organisation, and analysis of HAV (Hand Arm Vibration) exposure data, proximity data and other health risk data.

The main component of the Reactec Eco-system is the watch worn by the Operator. The watch is part of the R-LINK and HAVwear eco-systems.

WARNING

I f the equipment described in this guide is used in a manner not specified by Reactec, the protection provided by the equipment may be impaired

1.1 R-LINK eco-system

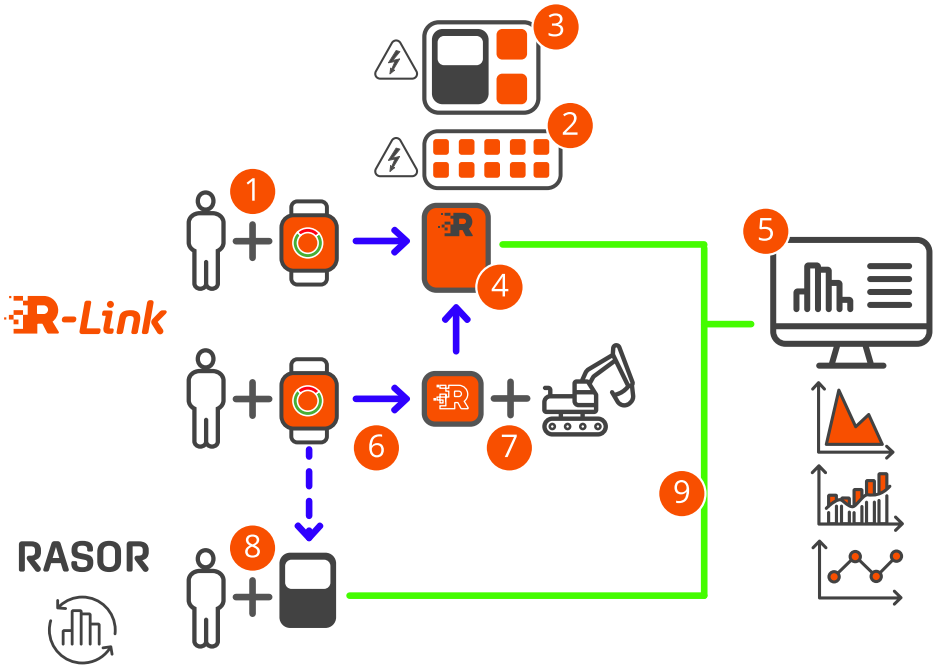

Figure 1 - R-LINK eco-system

1	R-LINK watch	Used to collect HAV and other important information. Also used to notify users of any potential hazards.
2	Charging station	Used to quickly charge the R-LINK watches.
3	R-LINK Dual charger	Used to charge RASOR and two R-LINK watches. (Available October 2022, contact Reactec for details).
4	Gateway	Used to collect data from the R-LINK watch and to then transmit this data, using mobile or networked connection, to be analysed using the cloud-based Reactec Analytics.
5	Reactec Analytics	Cloud-based software for reporting and managing your users, tools, and plant.
6	Data transfer using Bluetooth	Data transfer from R-LINK watches to the Gateway, Beacon, or RASOR.
7	Beacon	Attached to equipment or fixed location and used to highlight potential hazards or proximity issues.
8	RASOR	Optional: RASOR captures real-time, multiple workforce risks and supports remote and lone workers with location information, slips/trips and fall detection.
9	Data transfer to Reactec Analytics	Data transmitted to Reactec Analytics using mobile or networked connection.

1.2 HAVwear eco-system

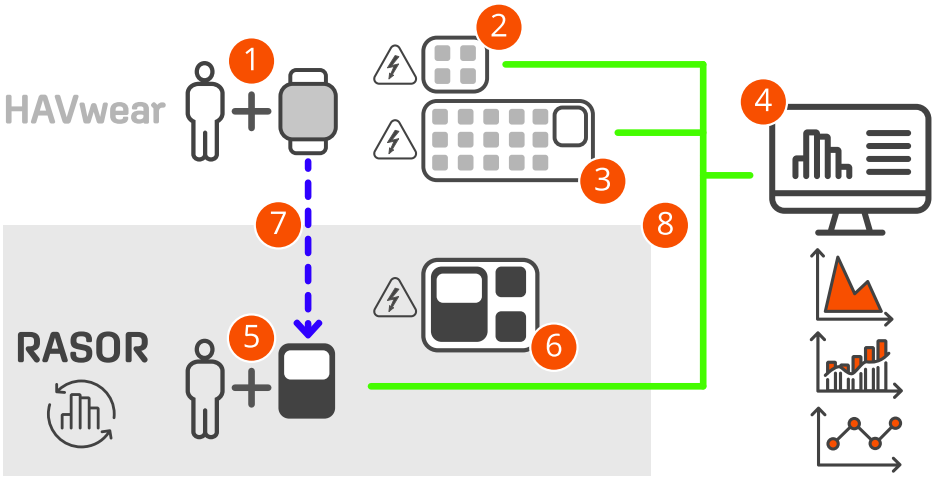

Figure 2 - HAVwear eco-system

1	HAVwear watch	Used to track HAV exposure.
2	4-bay docking station	Used to charge four HAVwear watches and to transmit HAV data to Reactec Analytics.
3	15-bay docking station	Used to charge 15 HAVwear watches and to transmit HAV data to Reactec Analytics.
4	Reactec Analytics	Cloud-based software for reporting and managing your users, tools, and plant.
5	RASOR	Optional: RASOR captures real-time, multiple workforce risks and supports remote and lone workers with location information, slips/trips and fall detection.
6	HAVwear Dual charger	Used to charge RASOR and two HAVwear watches.
7	Data transfer using Bluetooth	Data transfer from HAVwear watches to RASOR.
8	Data transfer to Reactec Analytics	Data transmitted to Reactec Analytics using mobile or networked connections.

1.3 Employer's responsibility

The employer is the person who operates and manages the Reactec Eco-system or allows a third party to use the system and bears legal responsibility for the system during operation for the protection of the user, personnel or third party.

1.3.1 Vibration regulations

When monitoring vibration exposure Reactec's wearables, HAVwear, and the R-LINK watches use a traffic light system to warn of exposure levels. The indicator lights are related to the HSE Control of Vibration at Work Regulations 2005 (Vibration Regulations).

The vibration regulations include an Exposure Action Value (EAV) and an Exposure Limit Value (ELV) based on the vibration at the grip or contact points on vibrating tools or equipment and the time spent using the equipment.

Information

EAV: Daily exposure to vibration of 2.5 m/s^2 over 8 hours that represents a clear risk requiring management. Equivalent to 100 points.

ELV: Daily exposure to vibrations of 5m/s^2 over 8 hours that represents a high risk above which employees must not be exposed. Equivalent to 400 points.

As an employer you may choose lower EAV or ELV threshold values depending on individual or collective risk factors or historical vibration exposure. Organisations may also use alternative values in accordance with their policies.

The watch calculates and records HAV exposure caused by operating a tool. The watch display shows the number of points the Operator has accumulated during a shift when working with vibrating tools, or alternatively displays the time remaining to reach a threshold while using a tool based on the current tool's vibration level and the exposure points already accumulated.

In addition, a colour coded indicator shows the Operator's HAV exposure relative to their EAV and ELV values.

Table 1 - A colour-coded indicator shows Operator HAV exposure relative to EAV & ELV.

Indicator	Definition	HAV exposure
Green	Go	Below EAV. Aim to stay in this region.
Amber	Be aware	EAV exceeded. Reduce tool usage, share workload. Supervisors on alert.
Red	Stop	ELV exceeded. Stop using hand-held power tools.

1.3.2 Tool tag programming

It is the employer's responsibility to adhere to legal requirements applicable to workplace health and safety and to determine vibrations that are representative of the actual vibration emissions applicable during tool use.

Information

Detailed information is available on the HSE website: https://www.hse.gov.uk/vibration/hav/index.htm.

Typically, there are two sources of vibration data for the purpose of calculating HAV exposure points:

- The published manufacturer's data
- Vibration measurements taken by a competent individual in the workplace

Manufacturer's test methods may not represent the vibration levels in the workplace and results can vary significantly. The employer is responsible for determining the most appropriate vibration magnitude to use in a HAV risk assessment, considering the influence of factors including:

- Variation over time
- Variation by specific task
- Variation by user
- Correct maintenance of tools and accessories

1.3.3 Watch exposure points

The watch calculates vibration exposure points using the HSE points system. Exposure points are calculated based on two methods:

1. Tool Exposure Points (TEP):

   The length of time a tool is in use, trigger time, and the vibration value that is programmed on the Tool Tag are combined using the HSE HAV exposure point calculation.

   It is important that the employer programs the Tool Tag with a vibration value that is representative of the actual vibration emission of the tool over time. This should take into account the specific tasks it is used for and other parameters that can cause variation.

2. Sensed Exposure Points (SEP):

   The watch has an internal capability based on the use of a tri-axial accelerometer to sense the vibration magnitude where the watch is attached to the wrist and applies an algorithm to adjust for the transmissibility through the hand to the wrist to give an approximation of the vibration at the grip point. This vibration magnitude is not compliant to the ISO standard BS EN ISO 5349 (ISO 5349) because the standard defines methods required to make measurements on a tool.

   Concurrent tool testing can be used to determine if the watch data is comparable with an ISO 5349 tool evaluation on a periodic basis.

   The watch uses the HSE calculation methodology to calculate SEP based on the length of time a tool is in use (trigger time) and the vibration magnitude sensed by the watch during use. This functionality is included for customers to determine if the sensed vibration is a more realistic representation of the risk experienced by the tool user than the static data programmed in the tool tag.

Tip

If SEP data is used to manage risk, the employer is responsible for determining if the watch SEP is a safe estimate of the risk faced by their employees.

> **Information**
>
> For more information on the HSE points system, refer to http://www.hse.gov.uk/vibration/hav/regulations.htm

1.3.4 Vibration measurement guidance

Reactec Analytics reports data collected at the point of attachment of the watch to the tool operator's wrist.

This data can be used for the following:

- To indicate a more representative vibration exposure
- To identify tool tagging errors

  Indicated by large variations to tool tag values
- To monitor the wearing of tools

  Indicated by changing measured values with time
- To identify potential operator misuse or unsafe use of tools

  Indicated by large variations to the tool tag data and or large variations between operators using the same tool
- To assess tool tag programmed values for appropriateness to the actual use of the tool

1.3.5 Data group management

To help analyse and report on the data gathered by the Reactec Eco-system, data can be organised into groups to create granular reports. Reactec Analytics can filter all reports to allow viewing of data by group, region, or division.

Data can be assigned to groups to reflect relationships, for example, by project. You can capture additional levels of organisation by categorising groups by region or division.

> **Tip**
>
> There is no hierarchy between regions and divisions.

1.3.5.1 Example

An organisation works on civil engineering projects throughout the UK. Management responsibility is organised by region and project type. Therefore, management requires HSE reports for individual projects as well as for each region and project type.

This can be described by the following organisation units:

- Regions, for example, Scotland, Northern Ireland, England, Wales
- Divisions, for example, Roads, Rail, Demolition
- Individual projects split across locations

To produce the required reports for this organisational structure using Reactec Analytics, follow these steps:

1. Create a group for each project.
2. Assign operators or Reactec communicting devices to the appropriate group.

   This ensures that exposure data for Operators is assigned correctly, regardless of their location.
3. Create divisions for each project type and categorise the groups to the appropriate division.
4. Create regions and categorise the groups to the appropriate region.

Reports can now be run by filtering parts of the organisation as required.

Table 2 - Example of group categorization

Group	Organisation Region	Organisation Division
Project A	Scotland	Road
Project B	Scotland	Rail
Project C	Northern Ireland	Road
Project D	England	Demolition
Project E	England	Rail
Project F	Wales	Road

► *For more information, see "Groups, regions, and divisions" on page 37.*

1.3.6 Location information

If a RASOR device is used by Operators while using the watch, the RASOR device collates location information using GPS technology to associate exposure data with a specific location.

When collecting data from nearby colleagues the RASOR device records the location of the RASOR user at the time it receives data from the colleagues' watch.

Caution

GPS technology only operates successfully outside of buildings.

1.3.7 Proximity (available for R-Link only)

The Proximity feature helps employers manage the movements of their employees by understanding when an R-LINK watch is within a prohibited distance of an R-LINK Beacon.

The Beacon is configured with a detection distance set in the Reactec Analytics. The Beacon is physically placed on a piece of equipment or vehicle around which the employer wants to set an exclusion zone. For larger pieces of equipment more than one Beacon may be needed.

When an R-LINK watch comes within the detection radius of the Beacon the R-LINK watch user receives a configurable alert that they are too close to the Beacon.

The R-LINK watch records data on how long the watch remained within the exclusion zone of the Beacon. Data on incursions within the exclusion zone of a Beacon help inform near misses and allow corrective actions on workflows or operator behaviour to be developed.

WARNING

The ability of a watch to warn of close proximity should not be relied upon as a fail-safe for collisions. The duty holder should verify satisfactory coverage has been achieved from the installed arrangement of Beacons, for example, checking for blind spots.

1.3.8 Social distancing (available for HAVwear only)

The SAFE-DISTANCE feature helps employers manage the movements of employees in accordance with Government guidance on social distancing.

For example, employers should plan work to ensure workers minimise time spent in close proximity to colleagues. Where possible, keep groups of workers working together in teams that are as small as possible (cohorting).

SAFE-DISTANCE is designed to indicate when two Reactec devices have come within an unsafe distance of each other for a period of time that indicates they are not social distancing.

SAFE-DISTANCE includes functionality to designate employees as belonging to a cohort; proximity time is recorded but does not cause watch alerts, and, when within a SAFE ZONE, any detections of other watches will not be recorded and will be regarded as false detections.

Information

The employer is responsible for implementing social distancing policies. SAFE-DISTANCE is an aid to provide auditable confidence of employee adherence to policy.

2 Reactec data protection

Reactec Analytics cloud servers that host customer data are managed by Microsoft Azure, a leading provider who host a wide variety of well-known corporate and Government bodies.

2.1 Data transmission

Gateways, docking stations, and RASORs are collectively known as Reactec communicating devices.

Data collated by R-LINK, HAVwear, RASOR's and third-party sensors is transmitted from Reactec communication devices at regular intervals.

All data is encrypted during transmission using AES 128 CBC according to American National Standards NIST SP 800-38a. An IPSEC VPN is used between the Reactec communicating devices and the mobile phone service provider, and between them and Microsoft Azure.

Transmitted data is automatically allocated to a customer when the Reactec communicating device is allocated to a customer account. An unallocated Reactec communicating device will not function and transmit data, ensuring that data cannot be transmitted without the originator being known.

2.2 Data security

Data stored on Reactec Analytics web applications has a firewall to prevent intrusion and is backed up daily to a different server location.

Secure Sockets Layer (SSL) encryption is supplied between the hosted server and Reactec Analytics web applications. The web application and network infrastructure have been penetration tested by a CREST certified third-party, which consisted of:

- Reconnaissance
- Authentication, authorisation, and session related testing

- Encryption analysis
- Information leakage tests
- Input validation analysis
- Application logic testing
- Network mapping
- Automated vulnerability assessment.

2.3 Data protection

For the purpose of data generated by Reactec Analytics, the reseller is a data processor only, and processes data on behalf of each customer, who remains the data controller as defined in the Data Protection Act 1998.

Information

The reseller is the system administrator commercially contracted as the supplier of access to the Reactec Analytics reports.

2.3.1 Software license

Upon first login to Reactec Analytics, every user is presented with the software license. The terms must be accepted to access Reactec Analytics. By accepting the terms, the customer gives the reseller and Reactec authority to manage and process personal data on their behalf.

The terms also give Reactec the right to use aggregated, anonymised data for analysis:

- Aggregated data

  Data that has been anonymised and is tracked across time. Aggregated data is not confined to one customer.

- Anonymised

  It is not likely, acting reasonably and having regard to other data available, to identify a living individual from the information.

2.3.2 Personal data

Personal data that is visible to the reseller to effectively support the system includes:

- Employee names
- ID numbers
- Authorised users' email addresses

Information

The reseller must be aware that some customers use National Insurance numbers or payroll numbers as ID numbers. Thus, even ID numbers can constitute personal data.

The reseller can view reports of customer data, but by default does not have access to vibration exposure reports, unless the customer chooses within the software to grant the reseller access, for example, to assist with a support issue. Such permissions can be time-limited and revoked by the customer.

Data permissions are set by the customer administrator from the ***Permissions*** tab. The ***Permissions*** tab is not visible to the reseller.

The data processor audit log allows customer administrators to identify when personal data has been accessed by reseller staff to ensure this is under authority from the customer.

Information

To ensure data security and validity is maintained, it is fundamental to the nature of the system that data records cannot be altered.

2.3.3 Customer responsibilities

Each customer is responsible for data access by their own authorised users. Access rights can vary depending on user types.

Employee access can be limited to viewing specific data or reports within specific groups. Reports can be extracted from the database at any time and can be emailed to selected authorised users.

As the Data Controller, the customer is responsible for data access requests by employees and for long-term storage of employee data. Suitable arrangements for appropriate long-term storage of paper or electronic reports must be made before their subscription expires.

In line with GDPR requirements for employee privacy, all SAFE-DISTANCE reports have an auto-deletion rule which can be configured to your business needs.

Upon termination of use of Reactec Analytics, Reactec can provide the customer with an export of data records from the database, if requested in writing within 30 days of termination.

Information

Reactec strongly recommends that the customer has a data policy covering use of, and access to, personal data, as well as user access and data protection policy for Reactec Analytics.

The customer's data controller must consider whether it has the necessary contents for gathering and processing personal data using Reactec Analytics.

3 Reactec Analytics overview

Reactec Analytics is a cloud-based software application with multiple functions to support the analysis and reporting of workplace risk data as collected by Reactec devices and Reactec partner devices.

Reactec Analytics provides fully auditable and tamper-proof data management, allowing users to view a variety of online reports and to manage the monitored risk:

- View live collated exposure data and employee location
- Access daily HAV exposure trends and KPIs from specific teams to company-wide activity
- Monitor alerts and alarms from daily activities
- Monitor social distance proximity detections
- Track third-party sensor exposure trends and KPIs
- View reports by division, region, or other categorisations, for example, by project
- Email or download reports as PDF documents
- Record interventions and control measures to support risk management

3.1 User administration

Employees must have a Reactec Analytics account to access the system.

System Administrators, Resellers, and Customer Administrators can hide disabled Users. This helps to de-clutter the interface menu. Disabled users are hidden by default.

The ***Users*** page allows user administration. Employees require a Reactec Analytics user account to access the system. The following user account types are available:

- **Report** - View reports and set up own alerts, no ability to add or amend any information within the Reactec Analytics.

- **Group Administrator** – Manage Users, Operators, Asset Administration (Hardware & Tools), Manage Data, Control Measures, and Interventions for specified groups.
- **Administrator** – In addition to the above, manage all Users accounts, all Groups, Permissions, Set Up options and Data.

Tip

A Smart User can be set up with Report, Group Administrator, or Administrator account types. Smart Users have access to TEP and SEP data. Users not set up as Smart Users do not have access to SEP data.

► *For more information, see "Watch exposure points" on page 12.*

Information

User access can be restricted by Reports module and Groups. Only Administrators or Group Administrators can manage users.

3.2 Reports modules

The reports modules are accessible from the toolbar in Reactec Analytics. Reports modules are used to view information on exposure and tool usage. This allows analysis, policy monitoring and planning, and recording of required actions.

Table 3 - Report module types

Report type	Description
HAV	Reports HAV exposure data
Tools	Reports tool usage and behaviour
Resources	Detailed reports on employee system use
Location	Reports GPS location data
Notifications	Reports the alerts and alarms communicated to Reactec Analytics
Noise	Reports noise exposure data
Social distancing	Reports social distance proximity detection data
Dust	Reports dust exposure data
Proximity	Reports data on R-LINK watch proximity to R-LINK Beacons

3.2.1 Data overrides

If the pencil icon is shown in the ***Overridden*** column, it indicates the tool vibration level has been overridden for some, or all, of the data in this report.

3.2.2 Reactec Analytics reports filtering

The Reactec Analytics toolbar provides access to the available reports modules.

To access a report, follow these steps:

1. Select the drop-down for the required reports module.

   For example, ***Tools***.
2. Select a report.

Use the ***Filter*** panel to filter data used in a report by group, region, or division, and by date range. Labels can be assigned to Operators and allow dynamic grouping of Operators. All reports that contain Operator data can be filtered by one or more labels. Where multiple labels are selected, an Operator is included in the report results if they are currently assigned to one of the selected labels.

Information

Reactec Analytics maintains a history of label assignment to allow reports run on historical data to be filtered using the labels assigned to the Operators at the time the data was stored in Reactec Analytics.

To filter data, select the required filter criteria from the ***Filter*** panel drop-down, then select ***View***.

The report chart displays data for the chosen Report, filtered according to the selected filter criteria.

3.3 Data and project manager

The ***Data/Project Manager*** pages allow Administrators and Group Administrators to perform administration functions.

Example administrative functions:

- Permissions
- Users

- Operators
- Groups
- Asset administration (Hardware and tools)
- Data
- Control measures and interventions
- HAV options
- Export data

► *For more information, see "Correct data assignments" on page 57.*

Day-to-day management of Reactec Analytics requires an understanding of the software and hardware components, and the Vibration Regulations.

3.4 Supported browsers

Reactec Analytics supports the following desktop browsers:

- Google Chrome 36.0.1985.126 and above
- Internet Explorer 1.0 and above
- Firefox 30 and above
- Safari 7.0.5 and above

4 Operations

This section provides information about the common operations performed within Reactec Analytics.

4.1 Accessing Reactec Analytics

Reactec Analytics is a hosted service accessible using a web browser.

To access Reactec Analytics, follow these steps:

1. Using a web browser, access www.reactecanalyticsplatform.com.
2. Enter your username and password and select ***Login***.

4.1.1 Password policy

At a company level, organisations can choose to set a specific password policy to suit an organisation's requirements.

To define your password policy, follow with steps:

1. Select ***Data/Project Manager***.
2. Select ***Set up/Password Policy***.
3. In the ***Display Information*** window, set your password configuration to suit your company policy.
4. Select ***Save***.

4.2 Configuring the watch

Watches can be configured to suit your business needs.

4.2.1 HAV options

Use the HAV options to configure the HAV settings and operation of the watch.

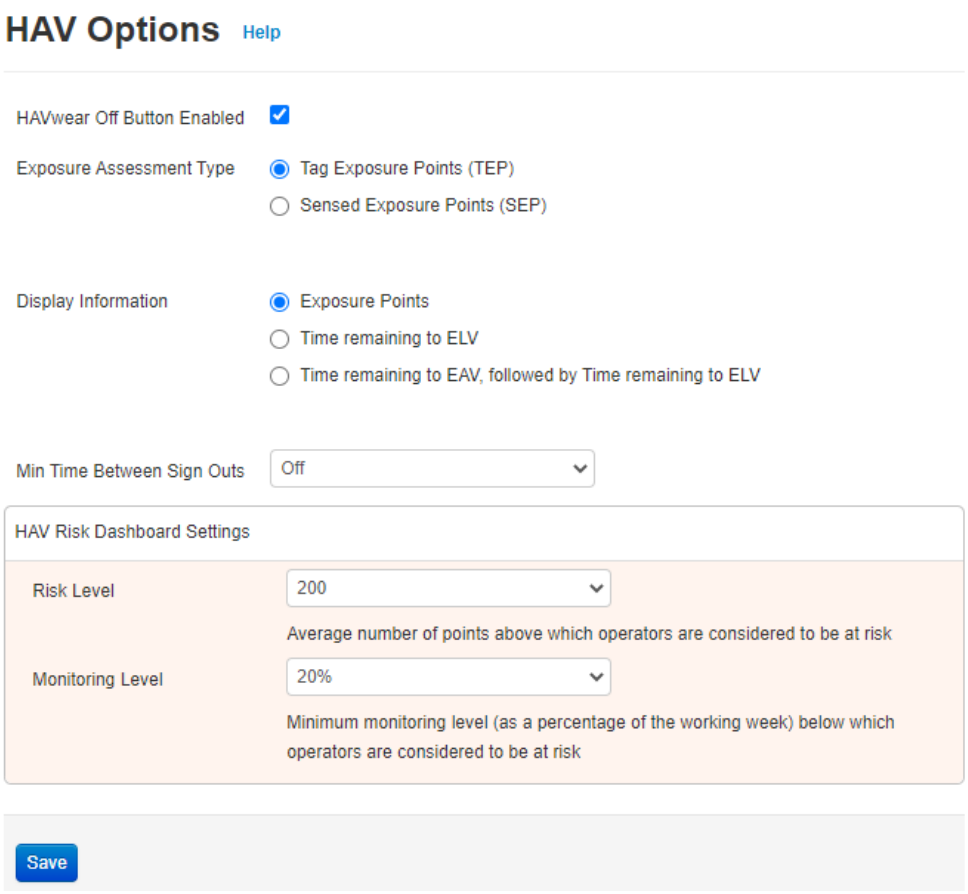

Figure 3 - Example of HAV options in Reactec Analytics

4.2.1.1 Enable operator to switch the watch OFF

There is an option to enable operators to switch the watch off. Switching the watch OFF is recommended after using tools with a vibration magnitude >5m/s2 to ensure TEP points are not accumulated for non tool use, for example, riding in a vehicle.

> **Caution**
>
> When this mode is enabled the operator at any time can prevent the watch from detecting any Tool Exposure Points (TEP). Sensed Exposure Points are not affected.

The operator switches the watch off during use by following a sequence of presses of the watch button. The operator switches the watch back on by reading a tool tag.

To enable the Off button, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***HAV Options***.
3. Select ***HAVwear Off Button Enabled***

   By default, this field is not selected.
4. Select ***Save***.

Information

If a customer has concerns about all operators having the ability to switch the watch OFF they can alternatively supply OFF tags as needed for only operators who can be exposed to significant off tool vibrations.

4.2.1.2 Choosing TEP or SEP data

There is an option to use either TEP or SEP data for reporting and to display on the watch.

► *For more information, see "Watch exposure points" on page 12.*

Typically, most organisations use TEP points, the default setting, initially to assess their operators risk.

To change the Exposure Assessment Type settings:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***HAV Options***.
3. Select one of the two options available from the ***Exposure Assessment Type***.

   By default, the system is set to ***Tag Exposure Points*** (TEP)
4. Select ***Save***.

Tip

Users can be enabled to view both TEP and SEP data, in order for an organisation to assess the value of both sets of data.

Information

Only users with Administrator level accounts can set the corporate policy on using TEP or SEP data.

Information

When an organisation chooses to select SEP data, the watch will display SEP points and the HAV exposure risk data reported will be based on SEP points wherever possible.

4.2.1.3 Configuring the watch screen display information

The watch can be configured to display one of three operations:

- Exposure Points
- Time remaining to ELV
- Time remaining to EAV, following by time remaining to ELV

To configure the watch display, follow these steps:

1. Log in to Reactec Analytics.
2. On the toolbar, select ***Data/Project Manager***.
3. Select ***HAV Options***.
4. From ***Display Information***, select from one of the three options.

   By default, the system is set to ***Exposure Points***.
5. Select ***Save***.

4.2.1.4 Operator sign out control

An option is available to limit the potential for an Operator to sign out more than one watch within a configurable time period.

The default for this option is set to ***Off***, which makes it possible for any ID card to be used to sign out more than one watch.

An Administrator can set a time period of up to four hours during which an ID card cannot be used to sign out a second device.

To set a limit on watches being signed out, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***SETUP > HAV Options***.
3. Select the required time from ***Min Time Between Sign Outs***.
4. Select ***Save***.

4.2.2 Social distancing options (available for HAVwear only)

The social distancing options let you configure the settings required for SAFE-DISTANCE functionality.

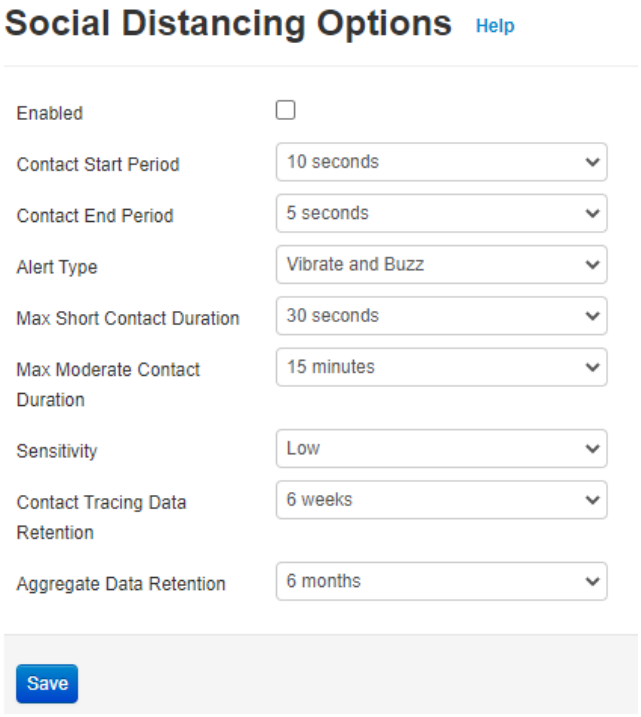

Figure 4 - Example of social distancing options in Reactec Analytics

4.2.2.1 Activating SAFE-DISTANCE functionality

At a company level, organisations can choose to enable or disable the SAFE-DISTANCE functionality. Any changes made to the settings are recorded in the Change Log.

> **Information**
>
> Only users with Administration level accounts can enable and disable SAFE-DISTANCE functionality.

Enabling SAFE-DISTANCE

To enable SAFE-DISTANCE functionality for all watches in the account, follow these steps:

1. Select ***Data/Project Manager***.
2. From the side menu, select ***Social Distance Options***.

3. Select ***Enable***.

Proximity settings

The following fields can be configured to suit your business needs:

- ***Contact Start Period***

  After a five second period to detect proximity, this setting controls for how much longer the watch waits to confirm the ongoing presence of a signal and start the period of detection.

  Reactec recommends five or ten seconds.

- ***Contact End Period***

  Defines the minimum period for which no signal is detected for the watch to end the detection of a proximity record.

  Reactec recommends five seconds.

- ***Alert Type***

  Defines the type of alert that is felt or heard on the watch. This can be set to vibration and buzz, vibration only, or none.

- ***Max Short Contact Duration***

  Defines a period where the detected proximity is considered short and reported as green in the traffic light report.

- ***Max Moderate Contact Duration***

  Defines a period above which the detected proximity is considered sustained and reported as red in the traffic light report.

- ***Sensitivity***

  Reactec recommends a sensitivity of standard to detect distances around two metres. A lower setting causes devices to need to be closer together to detect proximity.

Data retention settings

Following GDPR requirements for employee privacy, all SAFE-DISTANCE reports have an auto-deletion rule which can be configured to your business needs.

The following fields can be configured:

- ***Contact Tracing Data Retention***

  This refers to the detailed individual to individual proximity records.

- ***Aggregate Data Retention***

This refers to records for one individual which have been summarised into total proximity time without the detail of the other individuals involved in the proximity detection.

4.3 Configuring RASOR

You can configure RASOR to suit your business needs.

4.3.1 Configure a RASOR

The RASOR properties should be configured to suit the use of RASOR. The default settings for each configurable parameter are:

- ***Upload Frequency***

  Defines how often the RASOR sends data to Reactec Analytics. The default frequency of data uploads is 15 minutes. The minimum frequency is set to one minute because frequent data transmissions impact the RASOR battery life.

- ***Location Frequency***

  Defines how often RASOR captures GPS location data. The default frequency is 30 seconds. The minimum frequency is set to five seconds because frequent GPS location retrieval impacts the RASOR battery life.

- ***Grace Period***

  This is the time between a Panic Alarm being detected and communication to Reactec Analytics. The default is 30 secs.

- ***Alarm Resend Frequency***

  Defines how often the RASOR resends alarms to Reactec Analytics which have not been cancelled. The default frequency is five minutes.

- ***Panic Button Enabled***

  On

- ***Fall Detection Enabled***

  Off

- ***Location Tracking Enabled***

On. Setting location tracking to OFF within the Reactec Analytics disables all RASOR devices owned on that company account therefore never recording any location information.

Information

RASOR can be configured by individual operators to give maximum flexibility in setting the parameters to suit the use of the device.

4.3.2 Using RASOR in hub mode

RASOR has two modes of working:

- **Operator Mode**

  RASOR is assigned to an individual by signing out using ID cards.

- **Hub Mode**

  RASOR is permanently located in a powered dual charger for the purpose of collecting data for anyone who moves within range of RASOR.

> **Tip**
>
> The default setting is **Operator Mode**.

Companies wishing to operate a RASOR in a fixed location within a powered dual charger should apply the ***Hub Mode*** settings.

To apply the hub mode settings, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***RASOR devices***.
3. For the RASOR that you are placing into Hub Mode, select ***Edit***.
4. Select ***Hub Mode***.
5. Select ***Save***.

4.3.3 Assign a RASOR to a group

A RASOR can be assigned to a group.

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***RASOR Devices***.
3. Select ***Edit*** next to the RASOR you want to assign.
4. Using the Groups drop-down field, select the Group that you want to assign the RASOR to.
5. Select ***Save***.

4.3.4 Assign Reactec Analytics users for RASOR alerts and alarms

To effectively manage the automatic e-mail and text message notifications that can be produced by RASOR devices, the Operators should be assigned to a Group.

In managing the Group setup, it is important to manage the ***RASOR Alerts / Alarms*** section to ensure the correct users receive e-mail and text notifications of the alerts and alarms raised by RASOR.

To assign Reactec Analytics users for RASOR alerts and alarms, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Groups***.
3. Select ***Edit*** for the Groups that will use RASOR devices
4. If the Group has not yet been created, you must first create the Group. Select ***Create New***, enter a name for the Group, and select ***Create***.
5. Select the ***Operator Alerts/Alarms*** tab.
6. Use the search field to find the users.
7. Select ***Update***.

Information

If a user is to receive alarm notifications by text, their mobile phone number must be entered into their user profile.

4.4 Configuring Gateways

You can override the Gateway global settings on a unit by unit basis to change the time-zone in which the Gateway is operational.

To change the global settings, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Gateway Devices***.
3. Select ***Edit*** for the Gateway that you wish to override settings for.
4. From ***Settings*** select ***Override global settings*** and update the time-zone field to suit your requirements.
5. Select ***Update***.

4.5 Configuring Docking Stations

You can override the Docking Station global settings on a unit-by-unit basis. There is the ability to change the upload settings and the social distance settings.

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Docking Stations***.
3. Select ***Edit*** for the docking station that you wish to override settings for.
    - To edit upload settings:
        a. Under ***Settings*** select ***Override global settings***.
        b. Update each field as required.
4. Select ***Save***.

4.6 Configuring Beacons

All Beacons or individual Beacons can be configured for specific warning radius ranging from 2m to 10m.

The default for Global settings for all Beacons is:

- Alert Type - Vibrate and buzz
- Proximity Incursion Distance - 10m

You can change the above Global settings by:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Proximity options*** .
3. Edit the required options
4. Select ***Save***.

You can override the Beacon global settings on a unit by unit basis.

To update these settings, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Beacon Devices*** .
3. Select ***Edit*** for the Beacon you need to override settings for.
4. To edit the settings, from ***Settings*** select ***Override global settings*** and update each field for your requirements.
5. Select ***Save***.

4.7 Creating a User

The ***Users*** page allows user administration. Employees require a Reactec Analytics user account to access the system. The following user account types are available:

- **Report** - View reports and set up own alerts, no ability to add or amend any information within the Reactec Analytics.
- **Group Administrator** – Manage Users, Operators, Asset Administration (Hardware & Tools), Manage Data, Control Measures, and Interventions for specified groups.
- **Administrator** – In addition to the above, manage all Users accounts, all Groups, Permissions, Set Up options and Data.

Tip

A Smart User can be set up with Report, Group Administrator, or Administrator account types. Smart Users have access to TEP and SEP data. Users not set up as Smart Users do not have access to SEP data.

► *For more information, see "Watch exposure points" on page 12.*

Information

User access can be restricted by Reports module and Groups. Only Administrators or Group Administrators can manage users.

To create a new user account, follow these steps:

1. On the toolbar, select ***Users*** **>** ***Create New***.
2. Enter the employee details and select the appropriate user ***Type***.
3. Select the ***Report Modules*** the employee should have access to.
4. From ***Data Access*** specify the ***Groups***, ***Regions***, or ***Divisions*** for which the employee can view data.
5. From ***Is Smart*** select ***View TEP & SEP*** to create Smart Users.
6. From ***Daily Alerts*** select ***on*** or ***off*** to receive alerts if the employee has exceeded their EAV, ELV, or both.
7. From ***Daily Proximity To Danger Alerts*** select ***on*** or ***off*** to receive daily alerts of employee moderate and sustained breached from proximity to watches.

8. For Group Administrators and Administrators, you must select at least one of the following options:
    - ***System***: A User manages Users, Data, Groups, Permissions, HAV Options, Export Data, and Control Measures and Interventions.
    - ***Operators***: Management of Operators only.
    - ***Hardware***: Management of Asset Admin (hardware and tools).
    - ***Interventions***: Allows the creation of Interventions only. This option in populated automatically if ***System*** is selected.
9. Select ***Create***.

Tip

Add a mobile phone number if the User is to receive automatic texts from RASOR. Excessive text messages will lead to additional charges to your account.

4.8 Data structure

You can structure data to suit your business needs.

4.8.1 Groups, regions, and divisions

Use groups, regions, and divisions to organise your HAV data.

4.8.1.1 Creating a group

Groups are used to organise collected data for reporting purposes.

Data can be assigned to groups to represent the operational or organisational relationships of the collected data within Reactec Analytics. Data can be assigned to reflect these relationships, for example, by project.

To create a group, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Groups***.
3. Select ***Create New***.
4. Enter the Group name.

5. Assign the new Group to a Region or Division, if necessary.
6. In the ***User Access*** tab, specify which users are permitted to view data for this group.
7. If you select ***Specific Users***, select the search box to choose which users require access.
8. Select ***Create*** to add the Group to the list of groups.

4.8.1.2 Archiving a group

Groups are used to organise exposure data and can be used to represent the operational or organisational relationships of the exposure data within Reactec Analytics.

As operational and organisational relationships change over time, the groups can be altered to reflect that and ensure the reporting is as relevant as possible.

To archive a group, follow these steps:

1. Log in to Reactec Analytics.
2. On the toolbar, select ***Data/Project Manager***.
3. Select ***Groups***.
4. For the Group you want to archive, select ***Archive***.

> **Tip**
>
> To view archived Groups, select ***Show Archived Groups***. The list appears with the option to reactivate.

4.8.1.3 Categorising a group

Use the Region and Division categories to organise Operator exposure data in a way that is meaningful to your organisation. Reports can then be filtered based on these categories.

To categorise a group, follow these steps:

1. Log in to Reactec Analytics.
2. On the toolbar, select ***Data/Project Manager***.
3. Select ***Groups***.
4. Select ***Edit*** for the Group you want to categorise.
5. From the drop-down, select the Region and Division.

6. If a Region or Division has not been created, select ***Create New*** and enter a name in the field.
7. Select ***Update***.

   The new Region or Division is shown in the Group list. You can edit the new Region or Division from the ***Region*** or ***Division*** pages.

4.8.2 Label sets

Labels and label sets are used to group data in Reactec Analytics.

- **Labels** are used to add data for arbitrary grouping purposes. Labels provide a fine-grained method of dynamically grouping Operator's data.
- **Label sets** are used to group Labels. Each label set represents a different type of data.

For example, a label set could identify one of the following pieces of information about a subcontractor:

- The operator that works for them
- The team they belong to
- The Operator's job role
- A particular work flow or process

Reactec Analytics supports three types of label sets:

- **System label sets**: Automatically created by Reactec to support system level functionality such as cohorts.
- **User label sets:** Created by customers to group their operators according to their business needs.
- **Process label sets:** Created by customer to group data by specific workflows and or processes that lead to potential areas of concern.

Label sets that are automatically created by Reactec will have attributes that determine the behaviour of the labels within the label set. For example, to support SAFE-DISTANCE functionality, the Label set named Cohorts is in place. By adding Operators into a Label within this Label set, the social distancing data collected for these devices is stored and reported as cohort data as opposed to social distance data.

As an example, you may want to consider subcontractors who work across a number of projects to be a label set. You would create a label set named

Subcontractors and then create a label for each specific subcontractor. This will allow you to analyse data by project or by subcontractor. You may have different job professions deployed across a number of locations and want to review data by site but also by profession. You would assign your operators by data groups for location but then introduce a label set named ***Profession***. Under the label set for profession you would then create a Label for each profession you wanted to assign individuals to.

4.8.2.1 Creating a label set

At start up, a single cohort label set is in place.

To create additional label sets, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Label Sets***.
3. Select ***Create New*** and enter the name of the new label set.
4. Select **Label Set Type** and choose from the drop down list.
5. Select ***Allow Multi Select*** to allow Operators to be assigned to more than one Label in the label set.
6. Select ***Track Changes*** to track when edits are made to the label set.

   If you select this option, the following data is recorded:

   - New label creation
   - When a label is assigned to an Operator
   - When a label is removed from an Operator
7. If known, add the names of each label that are to be included in the label set in ***Labels***.
8. Select ***Create***.

4.8.2.2 Assign Operators to labels

To assign Operators to created labels:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Label Sets***.
3. Select ***Assign*** for the appropriate label set.
4. Select the label for Operators to be assigned from if they are already in another label.
5. Select the label to move the Operators to.

> **Tip**
>
> Alternatively, Operators can be assigned to a label set within the Operators page when creating or editing an Operator.
>
> ► *For more information, see "Edit an Operator" on page 45.*

4.8.3 Assigning multiple Docking Stations and Operators to a group

It is possible to add multiple Docking Stations or Operators to a group at the same time. This is useful when creating a new group, or re-organising groups.

After Docking Stations or Operators have been assigned to a group, any new HAV exposure data uploaded will be associated with that group. All data previously uploaded remains associated with the group the Docking Stations or Operators were previously assigned to.

► *For more information, see "Correct data assignments" on page 57.*

To assign multiple docking stations or Operators:

1. Log in to Reactec Analytics.
2. On the toolbar, select ***Data/Project Manager***.
3. Select ***Groups***.
4. Select ***Edit***.

   If the group has not been created, you must first create it.

   ► *For more information, see "Groups, regions, and divisions" on page 37.*
5. Select ***Operator*** or ***Hardware***.
6. Search for the communication device or Operator and select it.

4.9 Operator management

You can configure Operators to suit your business needs. Any employee who is required to use a watch, RASOR or supported third-party sensors, must be given an ID Card. Before being able to use an ID card, the employee must first be added to Reactec Analytics as an Operator.

4.9.1 Operator pre-upload considerations

For employees who will use watches and/or Pambry or Cirrus devices, consider what applications the devices are being used for, for example, HAV monitoring, Proximity, Noise, or all three.

Reactec Analytics requires the following mandatory information:

- **External Operator ID number**: Up to 16 letters and numbers. This is a unique number used to identify the employee in Reactec Analytics.
- **Name**
- **EAV** and **ELV** of the employee If being used for HAV monitoring

Additional fields available:

- ***DOB, CSCS ID and NI numbers***

  These can be used to confirm the identity of the Operator. These are discretionary fields and should be taken into consideration along with your company's GDPR policy. These fields can be disabled from use within the**Operator Options** set up page.

- ***Ear Defenders (SNR)***

  The PED 0828 includes the ability to adjust the reported noise level for any hearing protection to be worn by the Operator. Using the SNR (Single Number Rating) of the ear defenders supplied to the Operator, use the drop-down list to choose the SNR noise reduction effect.

  > **Caution**
  >
  > Entering a SNR value for an Operator within Reactec Analytics means that whenever they are assigned a PED 0828 all noise measurements are reduced by the SNR value of the expected hearing defenders. This facility should only be used when the use of the ear defenders is robustly controlled.

- ***Working days per week and Working weeks per year***

  To allow the effective reporting or days monitored in the Operator Average Exposure report, update the Operator's working days per week and working weeks per year. By default this is set to 5 and 45 respectively.

- ***R-Link Options***

By default the fields below are checked as per the functionality that the watches were purchased for. The functionality can be edited on an Operator by Operator basis:

- ***HAVS Enabled*** - if an Operator is to be supplied with a watch for HAV risk monitoring.
- ***PPI Enabled*** - select if an Operator is being supplied with a watch for Proximity monitoring.

4.9.2 Add an operator - to use a watch

To add an operator:

1. From the toolbar, select ***Data/Project Manager***.
2. Select **Operators**.
3. On the ***Operators List*** page, select ***Create New***.
4. Enter the operator details.
5. Select ***Create***.

Caution

Before Reactec Analytics can provide information to the Reactec communication devices to enable an employee to use Reactec equipment, Reactec Analytics must also obtain the in-built RFID identity number for the ID card.

The RFID identity number is obtained during the assignment process using ID Card Manager.

Tip

For a company's own existing RFID cards, the same data can also be obtained during the assignment process using ID Card Manager.

However, if the inbuilt RFID identity number is available in an excel format from another software package, using the Card ID field to associate the inbuilt RFID identity number with the Operators unique Operator ID number at the point of uploading or adding Operators to Reactec Analytics avoids the need for an additional assignment process using ID Card Manager.

4.9.3 RASOR Users

You need to create an Operator to use RASOR Then consider if the Operator using a RASOR is to be assigned a RASOR to allow them to view live data from colleagues or to be provided with Lone Worker protection.

4.9.3.1 Add an Operator to view live data

If an Operator is to be supplied with a RASOR to view data of other Operators, follow these steps:

1. Select ***Is Supervisor*** in the Operator page.
2. Select the Groups that the Operator will be allowed to see data from.

   This can include unassigned.

4.9.3.2 Add an Operator for Lone Worker protection

If an Operator is to be supplied a RASOR for Lone Worker protection, select the Check-In Check-Out settings that suit their work pattern. By default, when creating an Operator, the ***Use global settings*** option will be checked.

Global settings can be edited by in the **Operator Options** set up page.

RASOR default communication settings can be altered per Operator by selecting ***Override global settings*** in ***Check-In Options***.

The Check-In feature by Operator can be set to:

- ***Active***: Always on
- ***Available***: Activated by the Operator on the device
- **Disabled**: Not available to the Operator

Information

Reducing the settings from the default impacts the battery operational life and therefore has pre-set minimums.

4.9.4 Assigning Operators to labels

Operators can be added to a label for the following purposes:

- System functionality behaviour, such as cohorts
- Data reporting purposes, to suit business needs

To assign an Operator to a label, follow these steps:

1. Open the Operator record.
2. Select ***Labels*** and select the label to add the Operator to.
3. If the label doesn't exist, select ***New Label***.
    a. Select a label set to add the label to.
    b. Enter the name of the new label and select ***Add***.
4. Select ***Update***.

Tip

Alternatively, Operators can be assigned to a label set when managing labels.

► *For more information, see "Label sets" on page 39.*

4.9.5 Edit an Operator

To edit an Operator, follow these steps:

1. On the ***Operators*** page, select ***Edit*** for the Operator.
2. Enter the Operator details.
3. Select ***Update***.

4.9.6 Bulk upload of Operators

To upload multiple Operators, follow these steps:

1. On the ***Operators*** page, select ***Bulk Upload***.
2. Select ***Download template*** to access a spreadsheet to populate.
3. Populate the spreadsheet, entering the Operator details, and save the file to a known location.
4. Select ***Choose File*** and select the populated spreadsheet.

5. From the drop-down next to ***Group***, select a ***Group*** that these Operators have to be associated with.
6. Select ***Import***.

4.10 Reports management

You can configure reports to suit your business needs.

4.10.1 Scheduling a report

Scheduled reports can be sent to one or more email addresses on a predefined schedule. These reports can be sent as PDFs or as links to the report in Reactec Analytics. These are useful to ensure key stakeholders are kept informed.

To schedule a report, follow these steps:

1. On the toolbar, navigate to the report that you want to schedule.

   For example, ***HAV > Exposure Levels Reached***.
2. Using the ***Filter*** panel, filter the report data as required, then select ***Email***.

   The ***Email PDF report*** window opens.
3. Within the ***Recipients*** box, select each person you want to receive a PDF copy of the report and select ***Add***.
4. Select ***Periodically***.

   The Schedule options are displayed.
5. Select the frequency that the report should be sent.
6. Select ***OK***.

   The window closes and the scheduled report is added to the list on the ***Report Emails*** page.

> **Tip**
>
> You can edit scheduled reports on the ***Report Emails*** page.

4.10.2 View or manage scheduled reports

Administrators and Group Administrators can view a list of scheduled reports.

To view or manage scheduled reports, follow these steps:

1. On the toolbar, select ***Report Emails***.

   A full list of scheduled reports is displayed.

2. Use the drop-down options to search for scheduled reports by a specific report, region, division, group or recipient.
3. Select ***Filter***.
4. Select the report to be deleted or edited.

   If you select ***Edit***, all the report parameters, including label filters, can be changed.

5. Select ***Save***.

4.10.3 Configuring the HAV risk flag dashboard report

A HAV risk report can be configured to your organisations expectations.

Only Administrators have editing permissions for this report.

To configure the HAV risk report, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***HAV Options***.
3. In ***HAV Risk Dashboard Settings***, edit the ***Risk Level*** and ***Monitoring Level*** by selecting one of the drop-down options.
4. Select ***Save***.

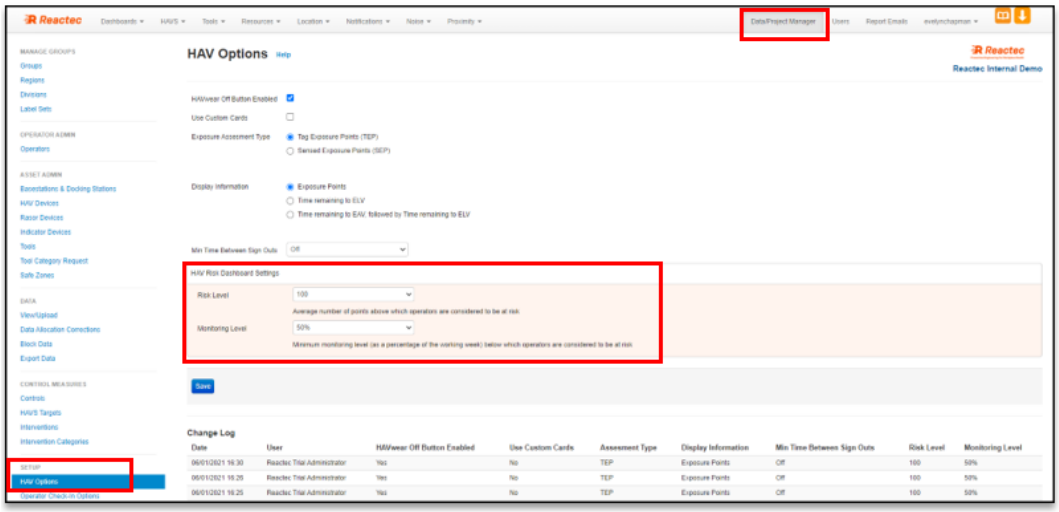

Figure 5 - HAV Options page

4.11 Control measures

A Customer Administrator can record control measures and interventions taken to improve exposure risk management and set targets for daily exposure levels at a company and group level. Reports are then available to assess the effectiveness of these measures.

4.11.1 Control measures management

You can configure control measures to suit your business needs.

4.11.1.1 Create control measures

Control measures can be introduced company-wide and at a specific project or group level with implementation dates and a traffic light status tracker.

To create a control measure, follow these steps:

1. On the toolbar, select ***Data/project manager***.
2. Select ***Controls***.
3. Select ***Create New***.
    - For company-wide control, leave ***Group*** blank
    - For controlling a specific project or group, select a group from the drop-down
4. Enter the detail of the control measure.
5. Enter the benefit of the control measure.
6. Enter the date that the control was implemented.

    This can be left blank if the control hasn't been implemented yet.
7. Select a status from the drop-down.

    If you select ***Completed***, enter a completion date.
8. Select ***Create***.

4.11.1.2 Create HAV daily average exposure targets

HAV daily average exposure level targets can be set company-wide and at a specific project or group level with target dates. Companies can choose whether or not to enable target values. This functionality is only available to company-wide Administrators.

To create HAV daily average exposure targets, follow these steps:

1. On the toolbar, select ***Data/project manager***.
2. Select ***HAVS Targets***.
3. Select ***Create New***.
    - For a company-wide target, leave **Group** blank.
    - For a target specific to a Project or Group, select a Group from the drop-down.
4. Enter the ***Start Date*** of the target.

    When a target is created, the end date will be blank until the target has been hit. When the target has been hit, the user should log back in and enter the ***End Date***.
5. Enter the **Target Value**.

    This is the average percentage of ELV target.
6. Select **Create**.

Information

You cannot create a second entry for the company or group if there is already an existing entry with no end date.

4.11.2 Interventions

Interventions can be created in one of the four reports below by selecting **+** to open the ***Add an Intervention*** dialog.

- HAV - Operator Daily Exposure report.
- Noise - Operator Daily Noise Exposure.
- Proximity to Danger – Workforce Incursion Report.
- Social Distancing - Workforce Contact report.

Interventions can also be viewed, created and edited by selecting ***Data/Project Manager > Interventions***

Interventions are recorded against individual operators. Within the ***Interventions management*** page, filtering is available to associate Interventions with groups or labels of Operators. The filters show the Operators within groups or labels at the time the Intervention is to be applied.

All these forms allow the user to categorise the type of intervention and select either a single group or one or more Operators as the target of the Intervention.

4.11.2.1 Create intervention Categories

Interventions can be categorised into types of intervention. This allows data to be assessed to view the most common types of Interventions needed.

By default, all accounts have a category named ***General***.

To create a new intervention category, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Intervention Categories***.
3. Select ***Create New***.
4. Enter the name of the intervention category.
5. Select ***HAV Interventions***, ***SAFE-DISTANCE Interventions*** or both.
6. Select ***Create***.

An analysis of interventions by category can be reviewed by adding a reporting component to your configurable dashboard.

► *For more information, refer to our Reports User Guide.*

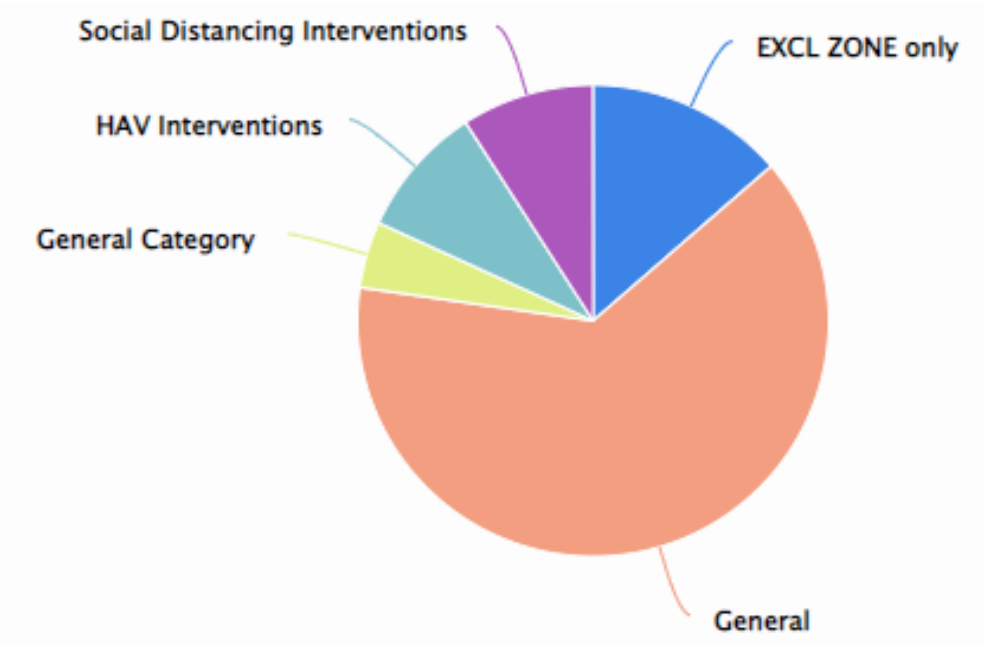

Figure 6 - Intervention By Category Report - Dashboard page

4.11.2.2 HAV exposure Interventions

Interventions can be added within the Operator Daily Exposure report.

1. On the toolbar, select ***HAVS > Operator Daily Exposure***.
2. Enter the required filter criteria from the filter options if required.
3. Select **+** (add) next to the Operator that you wish to apply the Intervention to.

   The following is shown:

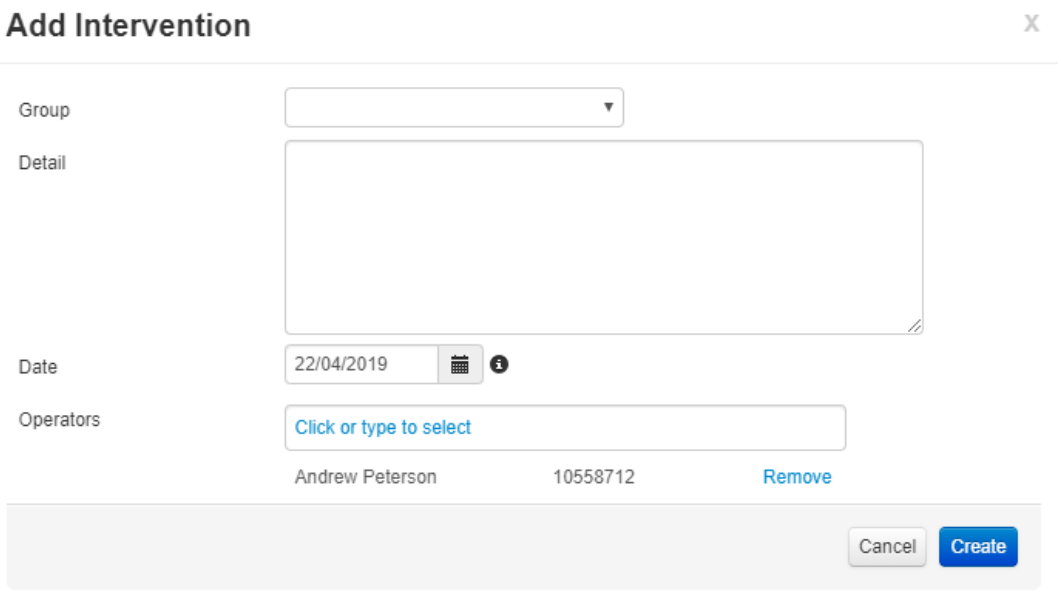

Figure 7 - Create intervention page

4. Select the ***Category*** type from the drop down list.
5. Enter the ***Detail*** of the intervention.
6. Enter the ***Date*** of the intervention notification.
7. Select ***Create***.

4.11.2.3 SAFE-DISTANCE Interventions

Interventions can be added within the ***Workforce Contact*** report.

1. On the toolbar, select ***Social Distancing > Workforce Contact***.
2. Enter the required filter criteria from the filter options if required.
3. Select **+** (add) next to the Operator that you wish to apply the Intervention to.
4. Choose the ***Category*** type from the drop down list.
5. Enter the ***Detail*** of the intervention.

6. Enter the ***Date*** of the intervention notification.
7. Select ***Create***.

4.11.2.4 Manage Interventions

Creating and managing interventions can be achieved from a specific menu within the administration forms.

To create an intervention, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Interventions*** from ***Control Measures***.
3. Select ***Create New***.
4. Enter the ***Details*** of the intervention.

   Provide as much detail as required.
5. Enter the ***Date*** of the intervention notification.
6. Select operators to be included in the intervention.
7. Select ***Create***.

Interventions can also be managed from the main ***Interventions*** page. Select ***Edit***, ***View Details*** or ***Archive*** the Intervention.

You can also view the history of the Intervention for auditing purposes.

4.11.3 Collecting signatures

4.11.3.1 Gather signatures for Interventions and HAV exposure

Signatures against interventions and HAV exposure can be gathered in three places:

- The ***Operator Exposure Action*** report

  For interventions added against HAV exposure data.
- The ***Intervention List*** report

  For interventions added against HAV exposure data.
- The ***Operator Contact Exposure Action*** report

  For interventions added against SAFE-DISTANCE social distancing data.

4.11.3.2 HAV exposure signatures

Signatures against HAV exposure can be gathered in the **Operator Exposure Action** report.

To gather HAV exposure signatures, follow these steps:

1. On the toolbar, select **HAVS > Operator Exposure Action**.
2. Enter the required filter criteria from the filter options.
3. Sign ***Signature*** for the HAV exposure.

   Sign using a touch screen or mouse. Once created, the signature is automatically stored. The date the signature is created is captured and ***Signed Off*** will change from a red cross to a green tick for the points that are associated with that signature.

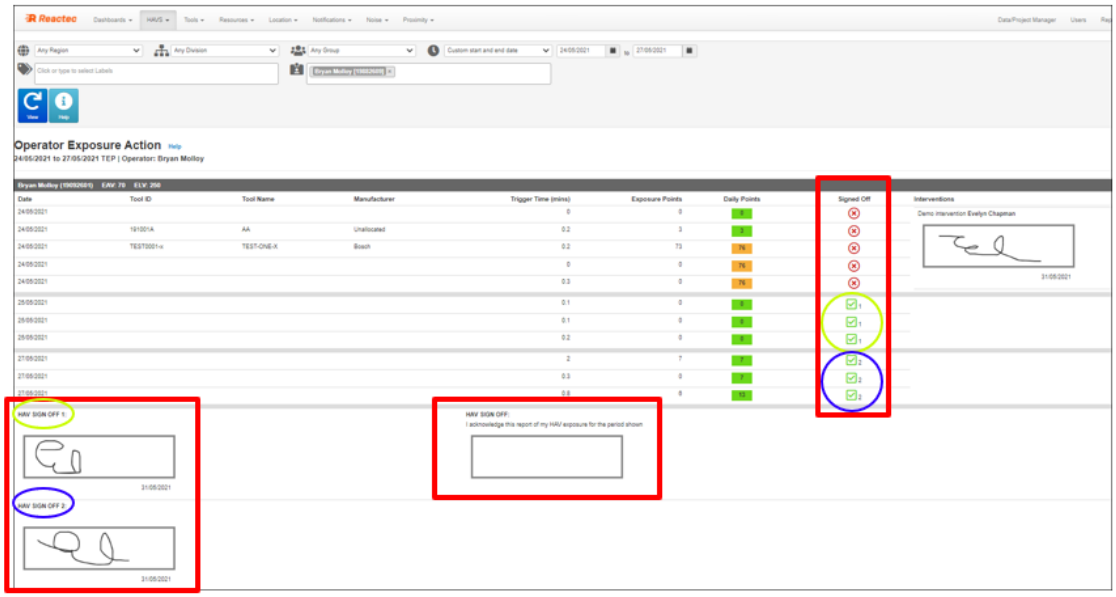

Figure 8 - Operator Exposure Action page

4.11.3.3 Intervention list report

To sign an intervention list, follow these steps:

1. On the toolbar, select **HAVS > Intervention List**.
2. Enter the required filter criteria from the filter options.
3. Select **Details** for the Intervention to be signed.
4. Sign in the ***Signature*** area for the required Intervention.

Sign using a touch screen or mouse. Once created, the signature is automatically stored. The date the signature is created is captured. Two buttons are available to clear or reset the signature.

4.11.3.4 Operator Contact Exposure Action report

To sign an Operator exposure action report, follow these steps:

1. On the toolbar, select **HAVS > Operator Exposure Action**.
2. Enter the required filter criteria from the filter options.
3. Sign in the ***Signature*** area for the required intervention.

   Sign using a touch screen or mouse. Once created, the signature is automatically stored. The date the signature is created is captured. Two buttons are available to clear or reset the signature.

4.11.3.5 Gather signatures for HAV interventions and HAV exposure with one single-point signature

Signatures against interventions and HAV exposure can be gathered by completing one single point signature input.

To gather signatures for HAV interventions and HAV exposure, follow these steps:

1. On the toolbar, select ***HAVS > Operator Exposure Action***.
2. Enter the required filter criteria from the filter options.
3. Identify the Operator for which you require the interventions or HAV exposure to be signed off.
4. Select ***Sign All***.

   A window appears detailing all the interventions which are being signed off and the HAV exposure sign off.
5. Sign ***Signature*** for the interventions and HAV exposure.

   Sign using a touch screen or mouse. Once created, the signature is automatically stored. The date the signature is created is captured and ***Signed Off*** will change from a red cross to a green tick for the points that are associated with that signature.

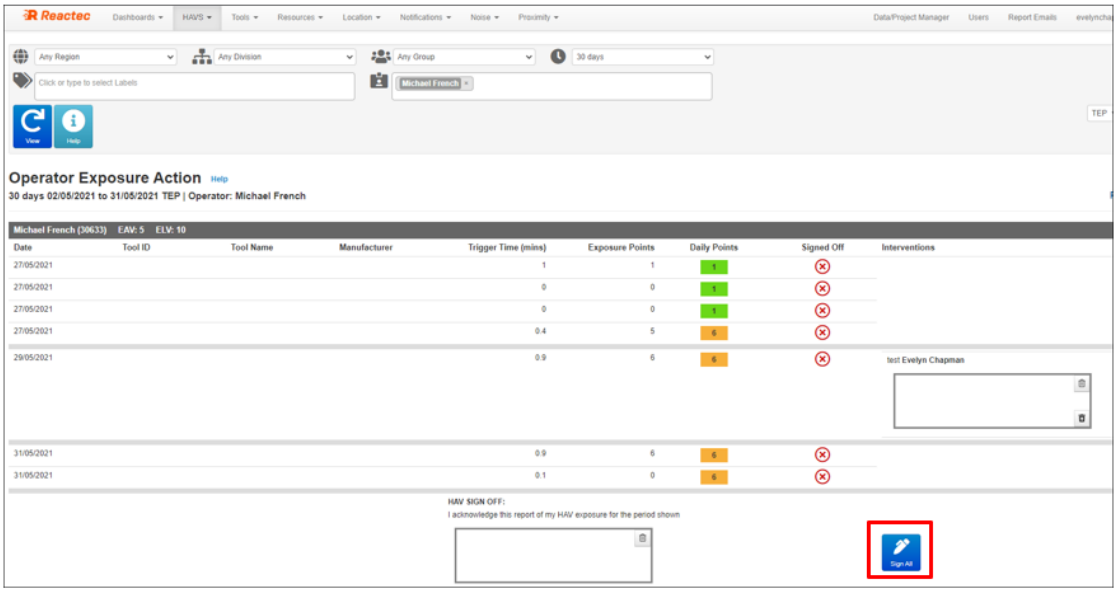

Figure 9 - Operator Exposure Action page

4.11.3.6 SAFE-DISTANCE Intervention signatures

Signatures against Social Distancing Interventions can be gathered individually or by completing one single point signature input when there are two or more Interventions associated with the data set.

1. On the toolbar, select ***Social Distancing > Operator Contact Exposure Action***.
2. Enter the required filter criteria from the filter options if required.
3. If signing off just one Intervention, identify the intervention to be signed.

   A box is shown which can be **signed** using a touch screen or mouse movements. after this is signed it is automatically stored.

   The date the signature is created is captured.

   You have the option to clear or reset the signature.
4. If signing off all Interventions, select ***Sign All***.

   Sign as required.

   Signed boxes change from a red cross to a green tick for the points that are associated with that signature.

Information

The details of an intervention can be viewed within the Intervention Admin page. When reviewing intervention details from within this page, if a signature has been gathered this is shown.

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Interventions*** from ***Control Measures***.
3. For any Interventions recorded, select ***Details***.

4.12 SAFE-ZONES

SAFE-ZONES are used to indicate areas where an individual is at not at risk from being in contact with germs as the area has physical barriers to prevent transmission. While such physical barriers may prevent virus transmission, they may allow radio signals to pass through and hence create a false proximity detection. An Operator tags onto a SAFE-ZONE tag to indicate that they are in a protected area. Tagging in to a SAFE-ZONE tag has the effect of preventing a proximity detection.

The SAFE-ZONE tag is programmed with the following information:

- The zone type

  Open or enclosed.
- The name of the location of the tag

  Up to 32 characters.
- The number of minutes after which the Operator will be automatically tagged out of the SAFE-ZONE

  Defaults to ten minutes. Can be set to zero if no timeout is required.
- Optionally the latitude and longitude of the location of the tag

When tagged to an **Enclosed** SAFE-ZONE proximity with another watch or RASOR will not be detected and the user will not be alerted.

When tagged to an **Open** SAFE-ZONE proximity with another watch or RASOR will not be detected and the user will not be alerted if they are also tagged into a SAFE-ZONE. If the approaching individuals has not been tagged into any type of SAFE-ZONE, their proximity will be detected and the user will be alerted.

Programming of SAFE-ZONE tags requires Tool Tag Manager. Within Reactec Analytics, SAFE-ZONE tags can be viewed and a sub-set of attributes can be managed. SAFE-ZONES will be automatically shown in Reactec Analytics after they are first used by a User.

To edit a SAFE-ZONE, follow these steps:

1. Log in to Reactec Analytics.
2. On the toolbar, select ***Data/Project Manager***.
3. Select ***Safe Zones***.
4. Select ***Edit*** for the required SAFE-ZONE.

   Only the location description and latitude and longitude of the location may be edited. If the zone has latitude and longitude coordinates, then a map icon is displayed to allow the user to view the location of the tag on Google Maps.
5. Select **Save**.

4.13 Data management

You can configure data management to suit your business needs.

4.13.1 Correct data assignments

Where HAV exposure data has been assigned to a Group incorrectly, you can re-assign the data to the correct group. This ensures that the Reports are accurate. Correcting data does not alter the data in any way.

1. On the toolbar, select ***Data/Project Manager***.

   The ***Groups*** page opens.
2. Select ***Data allocation corrections***.
3. Enter ***Filter Criteria*** to search for the data set you need to re-assign.
4. Select ***Show Results***.
5. Use the check boxes on the left of the data record list to select the data sets to re-assign.
6. Select the group to re-assign using the drop-down option from ***Move selected***, and select ***Move***.

Move changes to ***Please wait***. When the re-assigning is complete, the button returns to normal.

Caution

Data correction only re-assigns the HAV exposure data already available in Reactec Analytics. To ensure future data is assigned correctly, you must also assign the docking station or Operator to the correct group.

4.13.2 Block data

If, after investigation, exposure data is found to not be representative of the task undertaken, you can block individual data records from appearing in reports. This ensures the reports are more representative.

There are two methods of blocking:

- **Fully block the data**

  Used, for example, if the watch was placed on a vibrating surface which was not a tool that the Operator was using.

- **Block SEP data only**

  TEP data will be used to populate the SEP record for the tool use. Used, for example, if the watch was in direct contact with the tool under use. If the watch comes in direct contact with a tool then the SEP data will be inappropriately high as the watch algorithms are based on vibration entering the watch through the hand. Data from a watch in direct contact with the tool is extremely unusual but is identifiable. Blocking only SEP data and copying TEP data into the SEP reporting for the incident ensures that there is a record of the tools use in the reporting.

To block data, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.

   The ***Groups*** page opens.

2. Select ***Block Data***.
3. Enter ***Filter Criteria*** to search for the data set you need to block or unblock.
4. Select ***Search***.
5. To fully block the data, select ***Block***.

6. To block SEP data only, select ***Override***.
7. Select ***Restore*** if you wish to restore blocked data.

Information

A notification symbol is shown on each report to highlight that data has been blocked.

4.13.3 Data permissions

Reactec staff cannot view personal data without the customer's permission. Permission can be given temporarily or permanently and can be revoked at any time. Permission is granted via the ***Data Permissions*** page.

To set data permissions, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.

   The ***Groups*** page opens.
2. Select ***Permissions***.
3. Select one of the three options.
4. Select ***Save***.

Information

After granting permission to access your data, you can view their activity by selecting ***Data Processor Audit Log***.

4.13.4 Upload Dust Data

Where data has been collected from a Trolex dust monitor, the data needs manually uploaded to the Reactec Analytics

1. On the toolbar, select ***Data/Project Manager***.

   The ***Groups*** page opens.
2. Select ***View/upload***.
3. Enter ***Choose files*** to search for the data set you need to upload and ***Open***
4. Select ***Upload***.

The Assign Operators & Process page opens

5. Using the available fields;
    - Choose an **Operator** to assign the data to
    - Select **Add Assignment** to split the dates and time if different processes undertaken in a day and data being uploaded over a longer period.
    - Choose a **Process** from the dropdown list For more information, see "Label sets" on page 39
6. Select **Confirm Allocations**

4.13.5 Export data

Administrators can export data from Reactec Analytics. Exporting data can be done in two ways:

- Download all relevant reports in PDF format
- Extract the data in CSV format

Information

Extracting data in CSV format results in a raw data set. This requires a good understanding of the Reactec system to usefully interrogate.

Caution

Exported data is not protected.

4.13.5.1 PDF reports format

To export data in PDF format, follow these steps:

1. On the toolbar, select the report to download.
2. Set the filters.
3. Select ***View Results***.
4. Select ***Download PDF***.

   The PDF report downloads locally to your PC.

4.13.5.2 CSV format

To export data in CSV format, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Export Data***.
3. To select a specific time period, select ***Custom*** and set the start and end dates.

   The default setting is to extract all data.
4. Select ***Export***.

   The CSV file automatically downloads to your PC.

4.14 Tool management

You can configure tools to suit your business needs.

A Customer Administrator can categorise tools into tool families and tool types to improve the analysis of tool information. The categorisation can be done individually or in bulk.

4.14.1 Tool filtering

A Customer Administrator can view and categorise all the tools that have been seen by the system.

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Tools***.

   The ***Tool List*** opens.
3. Filter the list using one of the following methods:
   - Use the drop-down in the ***Tool Search*** filter area to select ***Filter***
   - Use the filter text box to only show results that contain the text entered

4.14.2 Bulk updating

The following properties can be updated in bulk from the ***Tool List*** page:

- Group
- Manufacturer

- Tool Family
- Tool Type
- Model Name
- Vib Source
- Retired
- Date Retired

To update multiple tools at the same time, follow these steps:

1. Select the check box at the end of the row for every tool you want to update.

> **Tip**
>
> Use the text filter to isolate the rows that you want to update and the Select ***All*** at the top of the ***Checkbox*** column to select all the rows to be updated.

2. Select the new values to apply using the drop-down from the ***Update*** section.
3. Select ***Update***.

4.14.3 Edit a single tool

The following properties can be updated individually from the ***Tool List*** page:

- Group
- Manufacturer
- Tool Family
- Tool Type
- Model Name
- Vib Source
- Retired
- Date Retired

To update an individual tool, follow these steps:

1. Select ***Tool Detail*** at the end of the tool row in the ***Tool List*** page.
2. Select ***Edit Tool***.

3. Select the new values to apply using the drop-downs.
4. Select **Update**.

Information

If ***Date Retired*** is selected, the tool will be ignored for reporting purposes after the date specified,

4.14.4 Tool vibration overrides

Tool tag programmed vibration levels can be overridden for any tool for any time period required, for example should it be identified that a tool tag was programmed with information. When a tool vibration override is in place, the report vibration exposure points will be adjusted based on the vibration magnitude specified. Any reports where the data has been overridden will be indicated with a pencil icon.

To add a tool vibration override, follow these steps:

1. From the ***Tool List*** page, select ***Tool Detail*** for a tool.

   The ***Tool Detail*** page for the tool opens.
2. Select ***Add Override*** in the ***Vibration Level Overrides*** section.
3. Enter a start date, end date, and new vibration level.

   Leave the end date blank if the override is to apply forever.
4. Select ***Create***.

Tip

Existing overrides can be edited and deleted by selecting ***Edit*** and ***Delete*** at the end of each vibration level override row.

4.14.5 Export Tool List

A Customer Administrator can download a list of tools in the system.

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Tools***.

The ***Tool List*** opens.

3. Select the Download Tools button

   The tool list wil be downloaded in .csv format

4.14.6 Tool category request

A Customer Administrator can request new manufacturers, tool families and tool types to be added to Reactec Analytics.

To make a tool category request, follow these steps:

1. Select ***Data/Project Manager*** on the top menu.
2. Select ***Tool Category Request***.
3. Enter details of the new category to be added.
4. Select ***Send Request***.

   The request is emailed to Reactec.

4.14.7 Tool servicing

Tools that have been configured for service management can be reported in the Tool Servicing Report to show the following:

- Dates of the last and next service
- The trigger or hours remaining until the next service
- The percentage of service period that has been used.

Tools can be updated to track service management either individually or in bulk.

4.14.8 Track service history for an individual tool

To update an individual tool to track in service management, follow these steps:

1. On the toolbar, select ***Data/project manager***.
2. Select ***Tools***.
3. Select ***Tool Detail Button*** for the tool.
4. Select ***Edit Tool***.
5. Select ***Track Service History***.

6. Select a method of tracking:
    - ***Time Period*** - Tools are serviced based on the number of days since the last service
    - ***Trigger Time*** - Tools are serviced based on the recorded trigger time since the last service
7. Select the ***Service Interval*** period.
8. Select ***Update***.

4.14.9 Track service history for tools in bulk

To update tools in bulk for track Service Management, follow these steps:

1. On the toolbar, select ***Data/project manager***.
2. Select ***Tools***.
3. Select ***Update*** next to each of the tools to be tracked.
4. From the options at the bottom of the page, select the type of ***Service History*** and ***Interval Period*** to be tracked.
5. Select ***Update***.

4.15 Subscriptions

Subscription renewal alerts are displayed in banner form within Reactec Analytics. Renewal email alerts are also sent to Administrators in advance of the subscription expiry date. By default, the email alert is sent to all Administrators. However, this can be configured for specific users.

To manage subscription alerts, follow these steps:

1. On the toolbar, select ***Data/Project Manager***.
2. Select ***Groups***.
3. Select ***Edit*** for the groups you want to receive subscription renewal emails.
4. Select the ***Subscription Alerts*** tab and select ***Specific Administrators***.
5. Use the search field to select the User.
6. Select ***Update***.