TRAKAWEB USER GUIDE

UD0018

29/11/22

VERSION 10.9

VERSION HISTORY

Version	Date	Who	Description of Changes	Approved By
1.0	16/11/12	AK	Initial version of document	
2.0	18/05/12	AK	General Updates	
3.0	29/05/13	AK	Rewrote the document to new style of TrakaWEB	
4.0	14/03/14	AK	Added detail on the Curfew section	
5.0	07/11/14	AK	Updated document to reflect current changed to TrakaWEB latest features	
5.1	28/04/15	AK	Amended the supported browsers in section 1.2. Added section on Email notifications.	
5.2	12/05/15	AK	Fixed the footer at the bottom of the document.	
5.3	31/07/15	LN	Added RRSS section	
5.4	18/08/15	GU+OR	Added email notification filter description + minor changes	
5.5	17/09/15	LN	Updated to incorporate the use of Lockers. Rewritten Curfews section. Rewritten Setting Up Email Notifications section. Added USB Charge Status Indication section. Adding more detail to Notes & Reason Logging and Custom Messages. General wording updates.	
5.6	20/10/15	LN	Removed details on obsolete feature – Hide Red LEDs	
5.7	02/12/15	JO	Updated TrakaWEB prerequisites (1.0).	
5.8	21/01/16	RC+LN	Updated Email Notifications in section 3.10.7. Edited 'Enrolment ID' in User Details section to include Card Reader.	
5.9	04/03/16	RC	Included section for Fault Logging (3.10.4)	
6.0	06/04/16	RC	Amendment to Curfew functionality change. (3.10.7)	
6.1	21/04/16	DJW	Updated prerequisites section (1.1).	
6.2	06/05/16	RC	Moved Feature Options to end of document. Created section for Item Booking (section 5.7).	
6.3	03/06/16	RC	Made changes to section 3.4.3, Editing an Item.	
6.4	20/06/16	RC	Added Fuel, Distance & Location Logging feature to section 5.8. Updated screen shot references to the new feature options page throughout the document.	
6.5	11/07/16	RC	Changed 'Current' to 'Curfew' in section 3.5.3 – Status Reports	
6.6	05/08/16	RC	Added TrakaWEB System Viewer Grid to section 3.2	
6.7	26/10/16	LN	Moved 'Item Access Groups' to 'Items' section. Corrected issue with heading levels from 'Feature Options' section onwards.	
6.8	21/11/16	RC	Added Access Schedules – section 3.13	
6.9	21/12/16	RC	Updated item booking. Items removed from system prior to a booking commencing – Section 5.7.8	
7.0	13/01/17	RC	Added information on Grant All/Revoke All in section 2.5.2	
7.1	02/02/17	RC	Added subsection on using the time picker in access schedules-Section 3.16.3. Added details to Fault Logging regarding prompt for info prior to the locker door opening – Section 4.1.6 & 4.1.13. Added new introduction.	
7.2	09/02/17	RC	Change to email notification section. Use a comma to separate email addresses instead of semi-colon. Section 4.5.3.7. Access Schedules icon added to Navigation Toolbar – Section 2.5.3.1	
7.3	07/04/17	RC	Added new section for 16bit support for TrakaWEB – Section 6	
7.4	20/04/17	RC	Updated Filter Builder in section 3.1.1.1 by removing 'When' activity.	
7.5	19/09/17	RC	Updated Authorisers and Curfews in 16bit support section. Added sync information to Access Schedules (Reviewed by OR) – Section 3.13. Added new logon image to Getting Started section. Added note in Email Notification regarding Subject field. Item handover section moved to Feature Options. Removed reference to Korean in the language section. New screen grabs added to email notifications for Fault Logging. Additional note in Fault Logging for email notifications. Added note for adding 5 items	

			to an iFob in section 3.4.5. Changes and additional notes made to 16bit Support – Section 6.	
7.6	06/12/17	RC	Sub-configuration options added to Item Booking, sections 5.7.7, 5.7.8, 5.7.9. Change made to Software Permissions Groups in section 3.6.4	
7.7	24/01/18	RC	Added information for TrakaWEB Admin Job Scheduler to Section 7	
7.8	27/03/18	JO	Updated section 2.2 – TrakaWEB Pre-requisites	
7.9	11/04/18	RC	Updated Job Scheduler images in section 7	
8.0	24/05/18	WT	GDPR Added after contents pages	
8.1	28/06/18	RC	RRMS added to section 5.10. RTUS information added to section 5.11 for V3 release.	
8.2	03/07/18	RC	Change to note in RRMS section 5.10	
8.3	16/07/18	RC	Added information for Authorisation Override to section 4.3.2	
8.4	13/11/18	RC	Updated Software Permissions Groups in section 4.6.4. Updated screen shots throughout document to reflect latest Traka Touch screens. Updated language selection in section 3.1	
8.5	16/01/18	RC	Updated section for updating items in section 4.4.2	
8.6	25/03/19	RC	Added information for clearing auto-fill info from browser to section 3.2 & 8. Changes to section 6.11 with updates of how 16bit Card &/or PIN option works with TrakaWEB. Added information for Emergency Open to section 4.11 FIFO information added to section 6. Edit to 16bit FIFO in section 7.23. Support telephone number updated at start and end of document. Illegal Handover now changed to 'Item Returned by a Different User' in reports – Section 4.5. Job Scheduler updated – Section 8	
8.7	02/04/19	RC	Added Auto Allocation section to 16bit Support for TrakaWEB – Section 7.22	
8.8	03/05/19	JO	Minimum SQL & OS versions supported changed	
8.9	12/06/19	RC	Amended introduction added to RRMS section 5.10.1	
9.0	31/07/19	RC	Clarification on RRMS pre-setup in section 5.10.3	
9.1	10/09/19	RC	Updated software release versions. Catalan added to language settings in section 3.1. Updates made to email notifications email template. Section 5.6.	
9.2	11/10/19	RC	Added 'Attempted System Access Exception Report' – Section 4.5	
9.3	20/11/19	RC	Change to System access screen to reflect user start/expiry date.	
9.4	28/02/20	RC/JO	Update to Software Permission Groups. Added new section for Multi-Select/Multi-Edit. Added section for Authoriser and Authoriser from a Different Group. Added information for accessing Support Log Files.	
9.5	01/05/20	RC	Removed Windows 7 references. Added section for removing fingerprint template. Updated support site link. Added new Distance Reports. Update to MSME for phase 2 release including curfews and filtering for Item Access Groups. Update for Authorisers on Return with additional Authorisation column added to User page.	
9.6	01/07/20	RC	Updated system editing. Added section for TWDI. Updated Item Booking Software Permissions.	
9.7	17/08/20	RC	Update to 'Not Seen In a While Reports' with added timescale filters. Added software permissions information to Item Booking section. Expanded on the Regions section to explain 'rules'. Added information in RRMS for differences between IAG & CIAG.	
9.8	16/09/20	RC	Updated MSME section with information for 'Set User Systems Allowance'. Update to standard Authorisers section.	
9.9	13/01/21	RC	Added 'Book for Yourself' Software Permissions information to Item Booking section. Replaced icons in Fault Logging, Emergency Release and Curfews sections. Removed 32bit support from prerequisites. Added new section for Scheduled Reports.	
10.0	12/02/21	RC	Added Mandatory Fields to Edit Users. Added new section for Temporary Key Store. Added new section to MSME for removal of Grant All/Revoke All buttons.	
10.1	12/05/21	RC	Updated Item Booking section for adding users to existing bookings.	
10.2	04/10/21	RC	Updated documentation with increased granularity in software permissions	
10.3	19/10/21	RC	Added section for Allowance Across Systems Advanced FIFO	
10.4	02/12/21	RC	Added section for Allowance Across Systems Fixed Return	

10.5	10/05/22	RC/LS	Added details for Item Access by Item Access Group Report. Added section for Item Pairing.	
10.6	06/07/22	RC	Updates to sections regarding Unrestricted Software Item Access	
10.7	30/08/22	RC	Note added to report filters for language specifications prior to generating a report.	
10.8	04/11/22	RC	Added new EULA information	
10.9	29/11/22	RC	Added information for Software Permissions Groups. Added information for Remote Release to Item Pairing.	

CONTENTS

1. WELCOME

Welcome to the TrakaWEB User Guide. This guide has been prepared in order to assist you with every aspect of TrakaWEB ranging from logging in, to adding users and running reports.

The guide will assist you with the use of TrakaWEB in conjunction with both Traka Touch Key Cabinets and Traka Touch Locker Systems.

The content of this user guide was documented against the following software versions:

- **TrakaWEB V3.16**
- **Traka Touch V3.1**
- **Integration Engine - For information regarding the latest version, please refer to the relevant Integration documentation**

NOTE: Please refer to the Traka support site for the latest compatibility information of TrakaWEB and Traka Touch products.

https://support.traka.com

GDPR COMPLIANCE INFORMATION

Traka supplies Key Cabinets and intelligent Locker systems. These products keep keys & assets safe from unauthorised access and allow only authorised users to remove and return the keys/assets they are entitled to. Traka systems give full accountability of who has (or had) which keys/assets and at what time and date.

This is usually managed by software that runs on either the Traka product and/or the client's computer network. To achieve all this, the Traka products hold personal information in order to identify individual users as well as the keys/assets. Examples of this are the storage in the Traka products of names, email address, PIN/card numbers and other detailed personal information required by a Data Controller (any organisation using the Traka systems).

Please be aware that under General Data Protection Regulations (GDPR) any Data Controller "shall be responsible for, and be able to demonstrate, compliance with the principles of GDPR". With regards to the personal data held on Traka products, the company or organisation that owns and operates the Traka system is the Data Controller as they are responsible for obtaining that data and for determining the purpose and legal grounds for which it is to be used.

Traka are happy to confirm that its products have the functionality & protection in place for an organisation to meet GDPR obligations including the fulfilment of the following rights to individuals (please note that to fulfil these requirements a process of using the software reporting process and/or exporting screen shots will be required):

- to be informed how their personal data is being used
- to access the personal data that is being held
- to rectify if any of their personal data is inaccurate or incomplete
- to erase and delete personal data
- to restrict processing of their personal data
- to obtain a copy of their personal data
- to object to their personal data being processed

On this basis, operators of Traka systems are reminded that they must take into account their obligations and responsibilities under GDPR when carrying out the following:

- Determining what personal data is to be held within the system and the legal grounds for doing so
- Obtaining the personal data from individuals and inputting it to the system
- Determining the appropriate access controls for the system and the data held on it
- Defining who is able to process the personal data and putting in place the appropriate Data Processor Agreements
- Understanding the requirements for, and implications of, sharing the personal data with other systems that are integrated to the Traka system
- Removing/deleting/erasing personal data from the system (including any backup copies) and dealing with Subject Access Request or Data Breaches

For more information about GDPR in relation to Traka products and systems, please contact GDPR@traka.com

INTRODUCING TRAKA

About Traka

Originally, the manufacturer of one of the world's first electronic key management systems in 1990 - we are now considered as world leaders in innovative technology for sophisticated, intelligent key management systems and lockers solutions to manage and control access to your most important assets. In April 2012 Traka was acquired by ASSA ABLOY, the world leader in door locking solutions.

Traka is used extensively in the UK and in over 30 countries worldwide supported by our network of distributors and resellers. Our market sectors span many industries and include Distribution and MHE Management; Fleet Management in Police, Road Haulage and Car Dealerships; Property Access Control in Prisons, Secure Units, Hospitals, Hotels, Schools, Universities and Managed Accommodation; Equipment, Asset Management and Control in Casinos, Petrochemical, Mining, Airports, Docks, Railways, Quarries, Military and Emergency Services.

Traka Service

Customer satisfaction is our top priority – at Traka we pride ourselves on building long term partnerships from initial hardware installation, through the system software configuration and user training and finally in providing on-going customer support via our helpdesk. Project Management begins from the moment that you decide to place your order with Traka. Our specialist Customer Account Managers work behind the scenes with our sales team to ensure a seamless handover.

The service provision you can expect from Traka will include...

- An experienced engineer to install the system at your site
- A project manager to help you plan your system configuration – your keys, users, their permissions and reports you want to prepare
- Training for your users and administrators
- Aftercare from our account management team
- Telephone assistance using our dedicated help line direct to our UK support center
- Optional 3- and 5-year maintenance contracts are also available

2. TRAKAWEB

2.1 PREREQUISITES

Before attempting to use TrakaWEB, please ensure you have read and completed the most recent versions of the following user guides:

- **TD0013 - TrakaWEB Installation & Configuration Guide**
- **UD0061 - TrakaWEB Getting Started Guide**
- **UD0011 - Traka Touch User Guide (for Key Cabinets)**
- **UD0090 - Traka Touch Locker User Guide (for Locker Systems)**

What is TrakaWEB?

TrakaWEB is a web-based administration suite for centrally managing Traka Touch systems. Developed to support any organisation or industry managing an unlimited number of items.

Prerequisites for TrakaWEB

The following Server specifications are recommended:

- **Windows Server 2019 with IIS10**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows Server 2016 with IIS10**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows Server 2012 R2 with IIS8.5**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows Server 2012 with IIS8**
  (3GHz Xeon, 8GB RAM, 500 GB HD)
- **Windows 10 (Professional or Enterprise editions) with IIS10**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **Windows 8.1 (Professional or Enterprise editions) with IIS8.5**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **Windows 8 (Professional or Enterprise editions) with IIS8**
  (3GHz i3, 8GB RAM, 500 GB HD)
- **64-bit support**
  Physical or Virtual machine support

The following Databases are supported:

- **SQL Server (incl. Express version) may be configured to 'Mixed Mode Authentication' or 'Windows Authentication'.**

The following Client Browsers are supported:

- **Internet Explorer** (latest version recommended, support up to v3.13 TrakaWEB only)
- **Google Chrome** (latest version recommended)
- **Mozilla Firefox** (latest version recommended)
- **Safari** (for Mac only - latest version recommended)
- **Microsoft Edge** (latest version recommended)

2.2 CAUTION

Great care has been taken to ensure that the Traka hardware and software works correctly but it is impossible to guarantee that there are no errors in a computer program or that hardware failures will not occur. Remember also that if someone enters the wrong information errors may also occur and careless use of the hardware can cause damage that no design can withstand.

Only you can check that the system works properly in your particular application both initially and on a regular basis.

We would ask you to consider how you would operate your business should you be unable to access the keys due to a hardware or software failure. We would also recommend you implement some contingency plan to cover such an occurrence.

For these reasons, Traka and their agents and distributors cannot assume liability or responsibility for any consequences under any circumstances arising from the use of the Traka equipment and programs. The product is sold only on the basis of this understanding. If this is not acceptable to you then please return the equipment and software prior to its use for commercial purposes for a complete refund.

2.3 WARRANTY TERMS AND CONDITIONS

Traka UK Warranty and Annual Maintenance and Support Agreement

Traka systems are provided with a 12-month warranty, starting on the day of installation. During this warranty period Traka will provide parts and labour to repair any fault caused though manufacturing defect.

After the expiry of the warranty period, an annual maintenance and support agreement may be purchased, which covers the cost of parts and labour to repair on a planned next working day response any fault caused through normal use of the equipment. In addition, the maintenance and support contract includes an annual system check and free upgrades to the PC software. The annual charge for this will be 15% (subject to distance) of the list price of the equipment covered.

Items covered by the Warranty and Annual Support Agreement
Hardware
All parts provided by Traka during the original installation. Where card or other readers are supplied by the Customer, these parts are specifically excluded from the warranty and maintenance. Items purchased subsequent to the original installation will be subject to an adjustment to the annual support agreement

Software
Traka will also provide free software upgrades as required during the period of the annual maintenance. Furthermore, Traka will provide a login to our technical support web site where information on the latest upgrades is available and where the latest software may be downloaded. Software upgrades are supplied on a self-install basis and requests for Traka to install the software are not included within the warranty or annual support agreement.

Response Times
Traka offer a 9:00 to 5:30 support facility and guarantee a same or next working day response to any reported fault. Where site visits are required, Traka will whenever possible attend on the next working day. Working days are Monday to Friday excluding Bank holidays.

Exclusions
Traka will not be responsible for any fault or damage or configuration change that occurs as a result of:

1. Inadequate user training
2. Software reconfiguration
3. Use of the software on a non-supported version of the Windows operating system
4. Customer re-installation on a different version of the operating system
5. Accidental damage
6. Vandalism, sabotage or terrorism
7. Noncompliance with the Customers responsibilities as detailed below

If a warranty or support visit is required to repair systems damaged as a result of these exclusions, Traka reserve the right to place a lower priority on the call and cannot guarantee the same response times to repair such failures.
If response to repair any fault or to reconfigure any settings is required due to these exclusions Traka will charge at their usual site visit rates.
If as a result of the site visit, the system failure was subsequently found to be caused by these or other exclusions, Traka will charge for both parts and labour at the prevailing rates.

Use of the equipment and Backing up the data
The Customers responsibilities are to: -

1. Ensure that the Traka hardware and software is used in a proper manner by competent trained employees only and in accordance with the Traka User Guides.
2. Provide the Traka support engineer full access to the Traka system and TrakaWEB. This may include making available access keys and passwords.
3. Ensure that all Traka systems are connected to the TrakaWEB database and are regularly backed up.
4. Not alter or modify the hardware or software in any way whatsoever nor permit it to be combined with any other system without the prior written consent of Traka.
5. Not request, permit or authorise anyone other than Traka to provide any maintenance services in respect of the hardware or software while the maintenance agreement is in effect and not subject to notice of termination.
6. Co-operate fully with Traka personnel in the diagnosis of any error or defect.
7. Ensure in the interests of health and safety that Traka personnel while on the Customer's premises for the purpose of this agreement are either at all times accompanied by a member of staff familiar with the premises and safety procedures or trained in respect of the site health and safety procedures.

Limitation of Liability
Traka shall not be liable for any direct, indirect or consequential loss or damage howsoever caused, arising from this agreement, the software, the hardware, its use, application support or otherwise, except to the extent which it is unlawful to exclude such liability.
Database

Traka shall not be liable for any direct, indirect or consequential corruption or loss of data arising from modification to the Traka database not conducted using the proper TrakaWEB tools provided. Any reparation to a Traka database required to be carried out by a Traka Engineer, where the database structure has been tampered with using other software programs (non-Traka software programs) such as Microsoft SQL Server will be charged for accordingly.

Virus
Traka warrants that it will use all reasonable endeavours to ensure that the software is supplied free of computer viruses and has undergone rigorous virus checking procedures prior to delivery in line within current best practices.

2.4 COPYRIGHT

2.5 CONTACT

Should you need assistance with your Traka products, please feel free to contact us by any of the means below. If however you purchased your Traka products through a distributor and you require assistance then please contact your distributor first.

Web Addresses
From our main website you can access our technical support website where you keep up to date with all the latest downloads and information.
Traka Website: **http://www.traka.com**

Email
If you have any questions regarding any aspect of Traka, please feel free to email us.
Enquiries: **info@traka.com**
Support: **support@traka.com**

Telephone and Fax
If you have any questions regarding any aspect of Traka, please feel free to call between the hours of 09:00 and 17:30 GMT/BST.
Telephone: **+44 (0)1234 712345**
Facsimile: **+44 (0)1234 713366**

Technical Support Helpline
Telephone: **0333 355 3641**

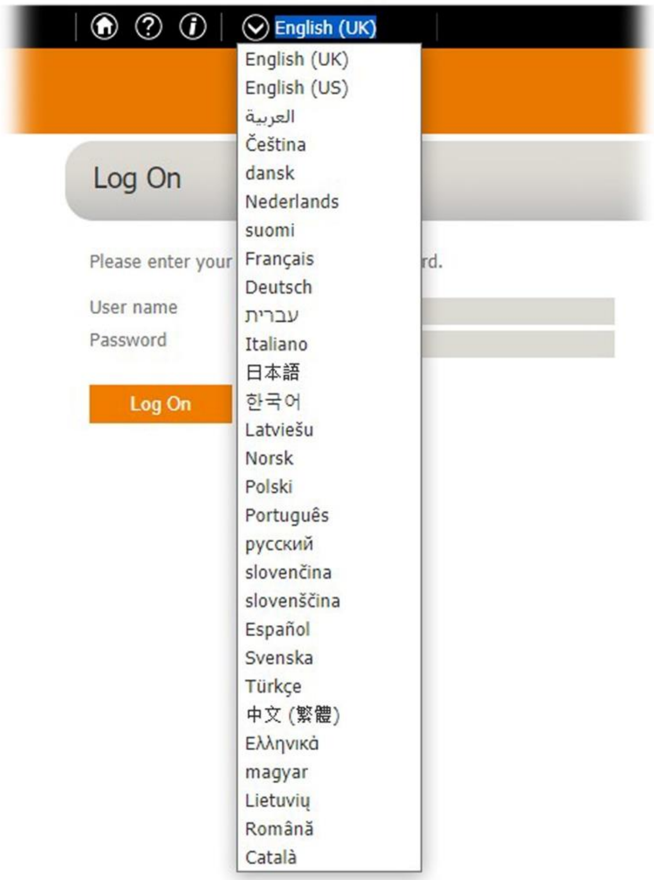
Postal Address
You can also write to us.

Address:
Traka
30 Stilebrook Road
Olney
Buckinghamshire
MK46 5EA
United Kingdom

3. GETTING STARTED

3.1 CHANGING THE LANGUAGE

TrakaWEB along with Traka Touch is multi-lingual and can display the whole web layout in various languages. These can be set on a per user basis so that when each user logs into TrakaWEB it will automatically change to the appropriate language. You can also change the language whilst browsing through TrakaWEB by clicking the small arrow button next to the language name, which will show a list of the currently supported languages. Simply select the desired language.



The page will then quickly refresh with the newly selected language.

NOTE: The language selector is always accessible from the top of the page regardless of where you are in TrakaWEB.

3.2 LOGGING INTO TRAKAWEB

Once you have completed the installation and commissioning of TrakaWEB, open a new window in your web browser and navigate to your TrakaWEB URL and you will be presented with the login screen.

NOTE: Please view the provided user guide - TD0013 - TrakaWEB Installation & Configuration Guide for more information on your TrakaWEB URL.

Enter your user name and password and select the 'Log On' button.

NOTE: If the autofill options have not been disabled in your web-browser, the Username and Password information will be visible when you next access the login screen. To prevent this information from being unintentionally saved or used, it is recommended that you disable the autofill options. For more information, please refer to the Disable & Clear Auto-Fill Information section.

3.3 NO MORE ACCESS LEVELS

Traditionally, Traka have used 'Access Levels' to define whether a user can remove an iFob/item from the system. Historically you would assign each item with an access level from 1-2560. The corresponding access level would then need to be allocated to the user. For example, if items 1-10 had an access level of 1, then any user needing to remove any of those items would also need access level 1 in their user details.

TrakaWEB does not use access levels; instead, you directly grant the user access to the item's position in the system, therefore giving them sufficient access. This bypasses the use for individual access levels. You can select which items the user can remove in the User Details grid under item access tab.

3.4 TRAKA TOUCH SYNCHRONISATION

Once your system has been connected to TrakaWEB, all the items, users and general data from your Traka Touch system will automatically be synchronised when you log in. After the initial Sync, TrakaWEB will communicate with your system every 30 seconds to ensure all information is as up to date as possible.

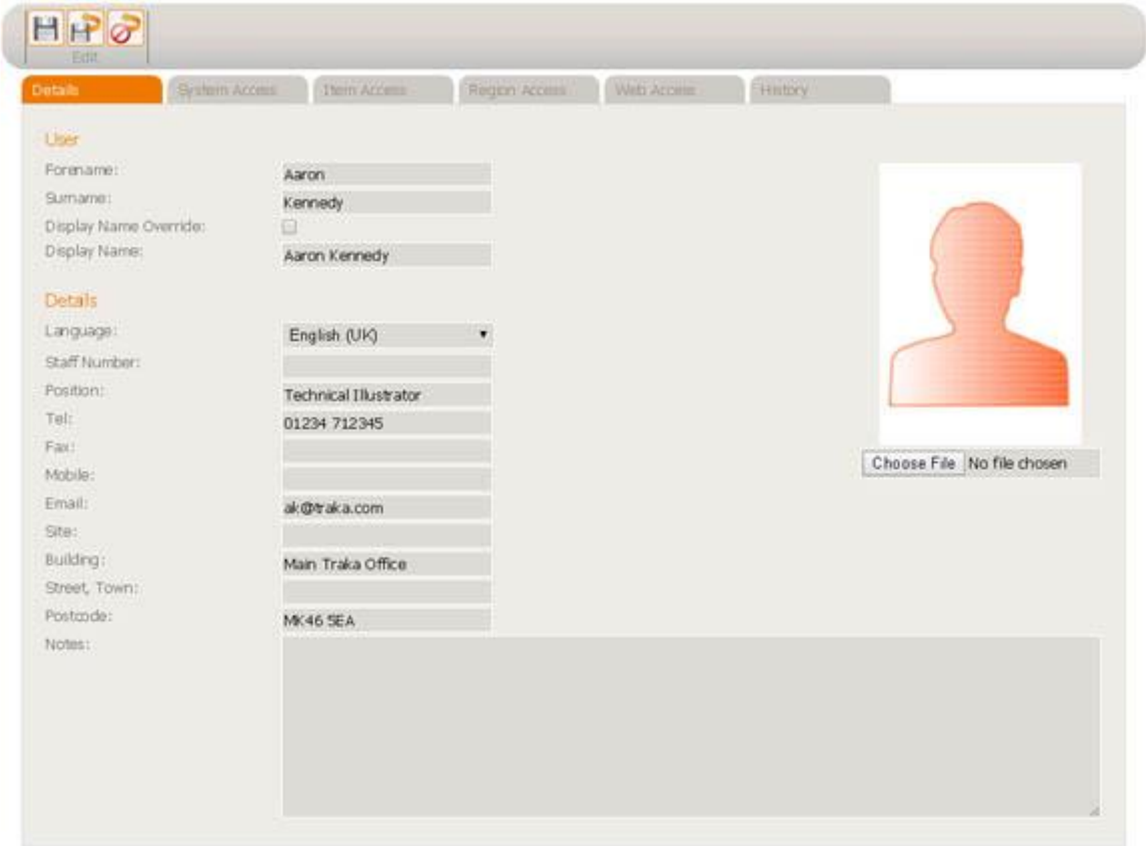
The current status of your system is displayed in the detail panel on the system viewer page.

3.5 HYPERLINKS

Throughout TrakaWEB, there are areas of text that are highlighted orange called hyperlinks. These hyperlinks can be selected to take you from one page to another. This allows you to quickly navigate from one section to another without cycling through different menus or clicking the forward and backward buttons on your browser. An example of a hyperlink in TrakaWEB is shown below.

From the item panel on the system viewer, click the 'previous user' name.

You will automatically be taken to the Edit User page, which holds all the information about the user.



3.6 TRAKAWEB INTERFACE

3.6.1 GENERAL INTERFACE

Each area of TrakaWEB displays different information and therefore varies in layout and style; however, a general interface is maintained consistently throughout TrakaWEB. Located at the top of each page is a black and orange banner which will display certain buttons and information that are used in every aspect of TrakaWEB.

1 - Home Button
When selected, the Home button will take you from the page you are currently viewing back to the system viewer page.

2 - Help Button
Selecting this button launches the built in TrakaWEB User Guide.

3 - Information Button
Clicking this will show a small dialogue box that tells you what version of TrakaWEB you are using along with licencing information and support details such as telephone and email addresses.

4 - Language Selector
Selecting this button will display a list of languages that TrakaWEB currently supports. Selecting one of those languages will automatically change all text on screen to the specified language. This can also be set on a per user basis, ensuring that all text will automatically change when the user logs into TrakaWEB/Traka Touch.

5 - User Name
Here the currently logged in user's name is displayed.

6 - Log Off Button
Clicking this will log you out of TrakaWEB.

7 - Traka Website Link
Clicking traka.com will take you to the main Traka website.

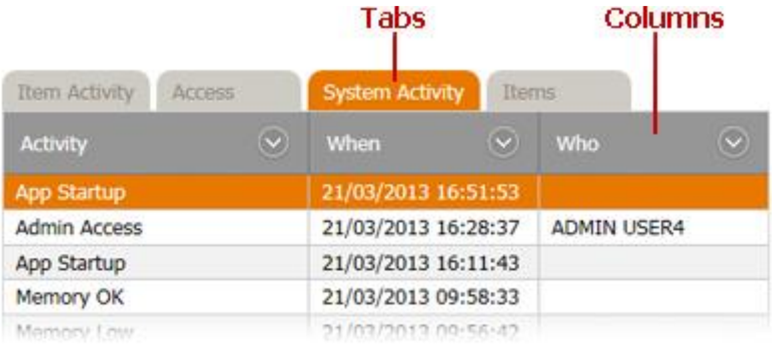
8 - Page Name & Icon
Each page of TrakaWEB will display the title of that page along with an icon.

3.6.2 GRIDS

Throughout TrakaWEB, there are various places that use grids to display important information. Each will vary slightly in what columns are displayed or what size they are. However, the navigation through each grid is the same.

Tabs & Columns

Each grid is made up of one or more columns and often has at least one tab. Columns can be added, moved and deleted from a grid simply by using the Show/Hide Grid Columns tool located at the top of the page in the Ribbon Toolbar.

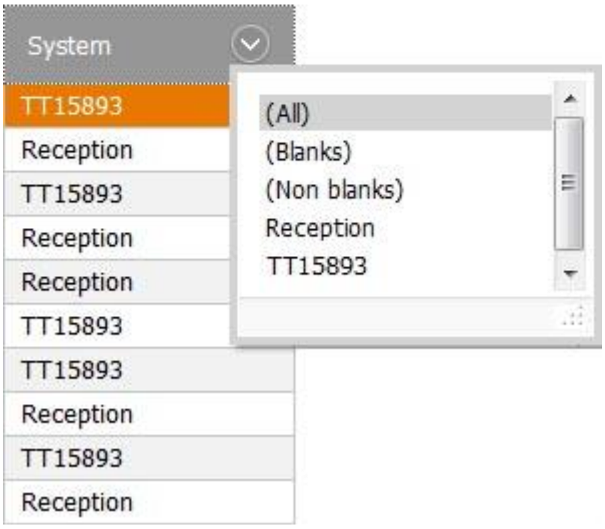


Any combination of columns can be saved and stored for later viewing. These are known as Layouts. Please refer to the Layouts Overview for more details.

Filtering Data

The information in each column of a grid can be sorted by ascending or descending order. To achieve this, simply click on the empty space of a column header to toggle the information from random to ascending first. Click again to sort to descending first.

Often there is a chevron button next to the column name. These also offer different options for filtering information. In the example below, the system chevron has been dropped down to show the names of all systems in the selected region. By default, the column always shows 'All' the system names. Clicking one of these names will automatically display that specific system. The option 'Blank' will display any system without a name whereas; 'Non-Blanks' will show every system that has a name.



It is also possible to sort information on multiple columns. For example, clicking the position column will sort the position number ascending first i.e., 1, 2, 3 etc. Holding the shift key on your keyboard and selecting another column, e.g., system, will then sort the position number by the system name.

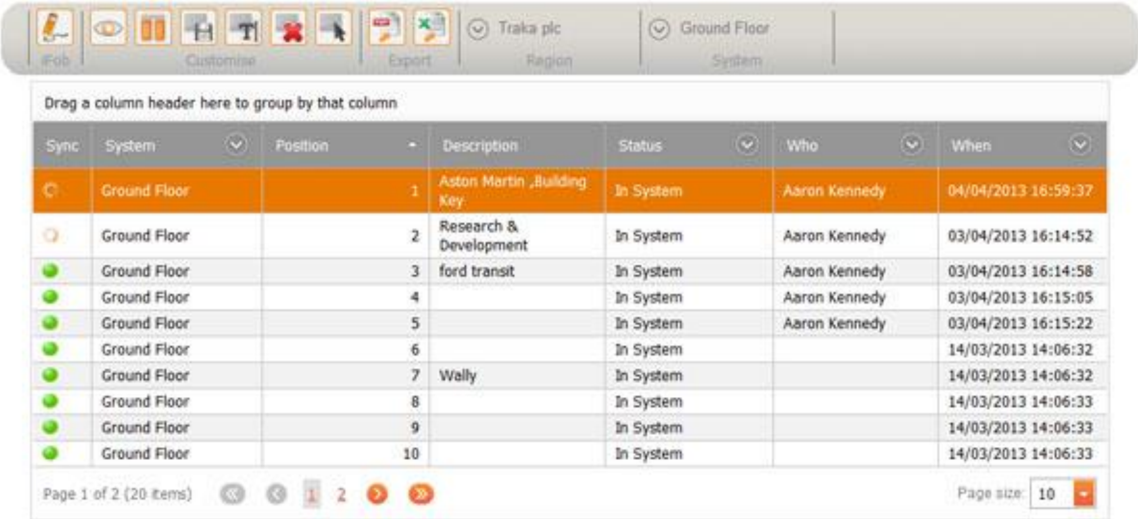
At the bottom of each grid is the page selector. You can click the number of the page you require or alternatively by clicking either of the < > buttons will move the page along one page at a time. To navigate to the very first or last page click the << or >> respectively.

Often there is also the option to select how many lines of data you can view on each page. This is only applicable if you have many lines of data that cannot be shown together. Selecting the drop-down arrow from the Page Size form in the bottom right hand corner will allow you to select how many lines of data will be displayed on each page.

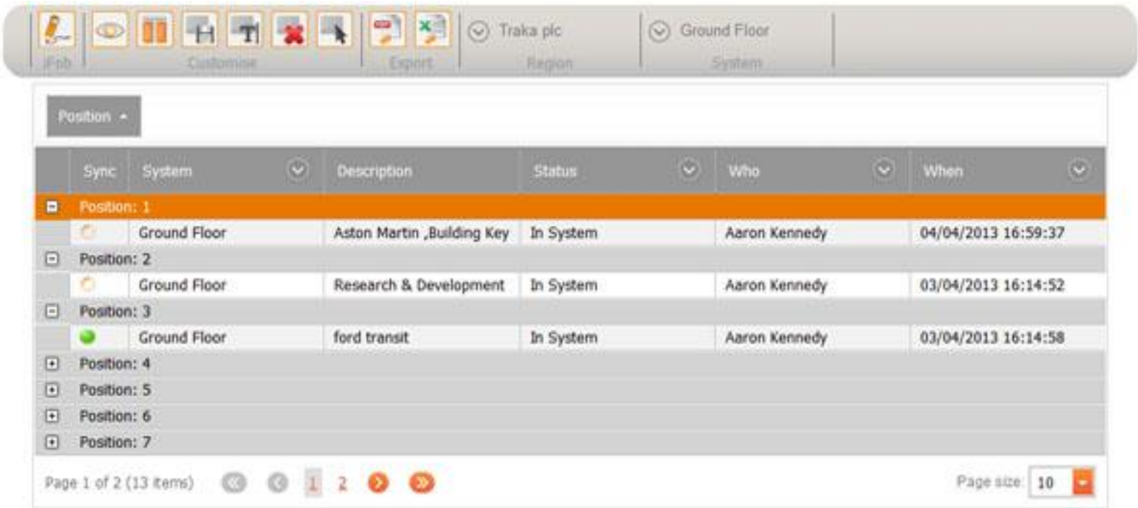
Grouping Information by Column

Most grids in TrakaWEB have the functionality to group information by the column. To tell if the grid you are viewing is able to group by columns, there will be a 'grouping bar' located above the grid just under the ribbon toolbar that displays the message 'Drag a column header here to group by that column'.

NOTE: If the 'grouping bar' is not visible, select the 'search' button in the ribbon toolbar.



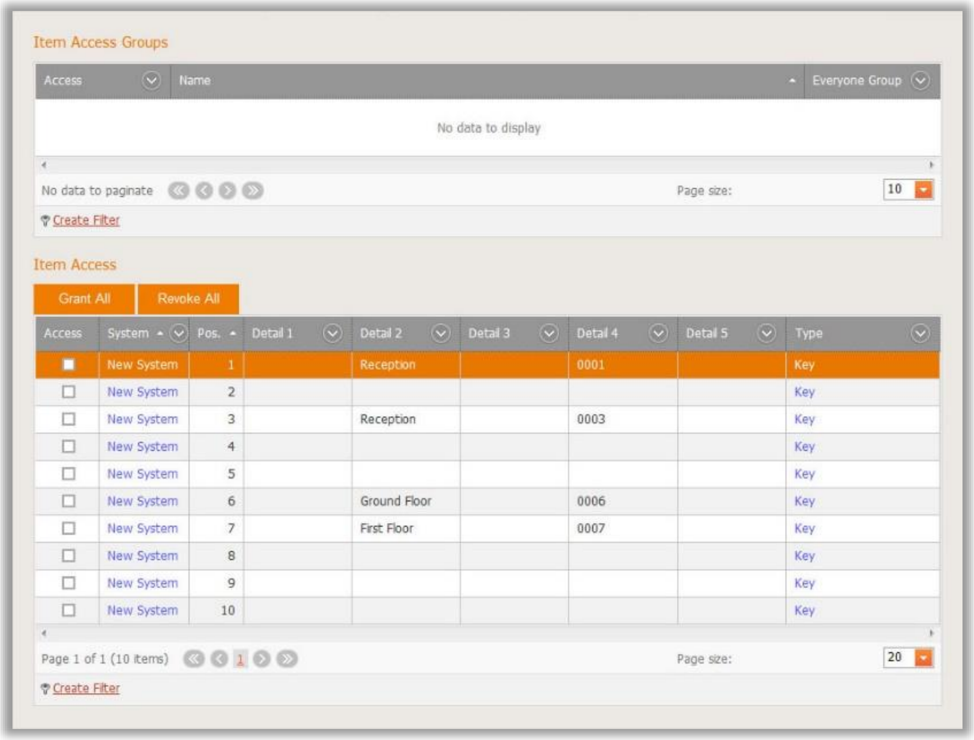
In the grid in the example below, the 'position' column has been added to the grouping bar. This allows you to view each position number individually. By expanding each line, you will see the details for that position number across all systems in the database. If you had three systems, you would see three separate lines with details on that position number in each of the three systems.



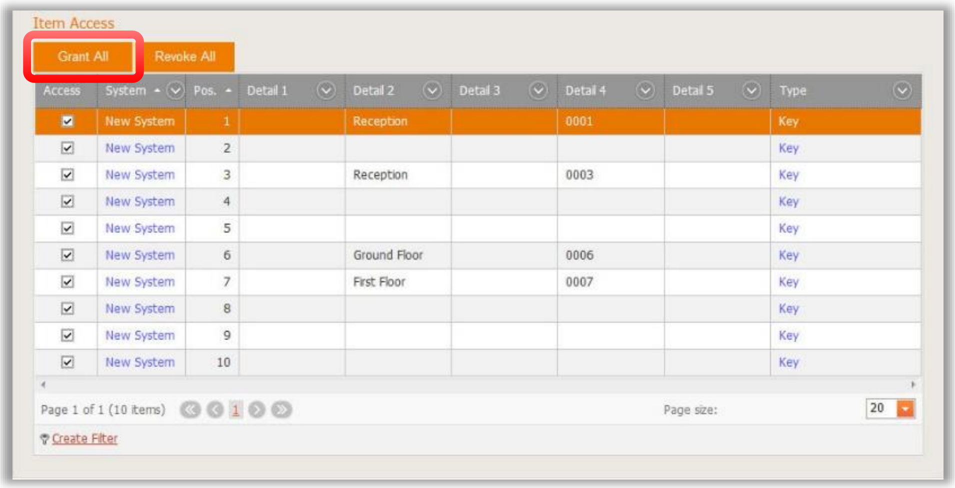
Grant All/Revoke All

The Grant All/Revoke All buttons are a quick way to allocate or deallocate access of all items to a user. They can be used in relation to Item Access Groups and Item Access.

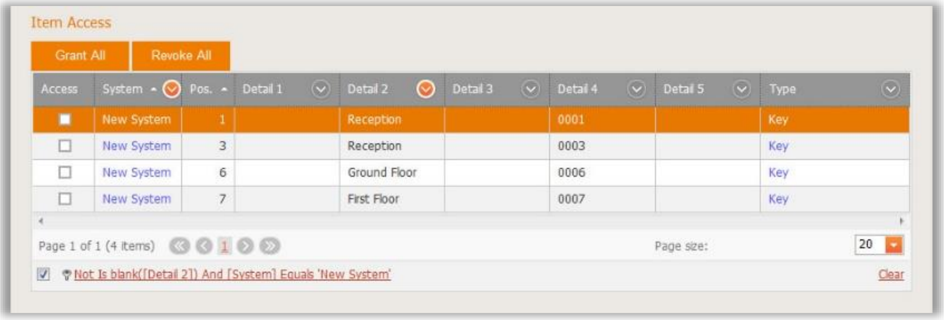
1. At the Edit User screen, click on the **Item Access** tab.



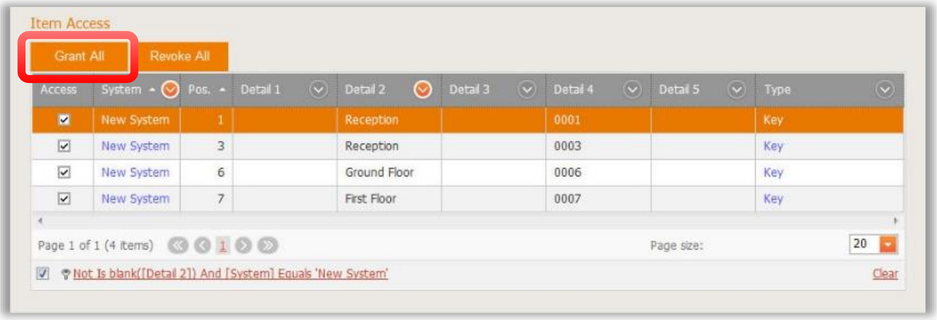
2. Clicking on the **Grant All** button will place a tick in every box in the Access Grid.



The same function can be applied to filtering the information in the grid.



Clicking on **Grant All** with a filter applied will only grant access to the items currently displayed in the grid.



NOTE: A similar process can be applied when setting up Users and Items in Access Schedules by clicking on Select All or Remove All.

3.6.3 TOOLBARS

3.6.3.1 NAVIGATION TOOLBAR

At the bottom of each screen, you will notice the Navigation toolbar. From here, you will be able to navigate to the different pages of TrakaWEB such as the System Viewer, Users and Systems etc. See the diagram below for a breakdown of each area.

System Viewer | Users | Items | Reports | Software Settings | iFobs | Systems | Realtime Activity

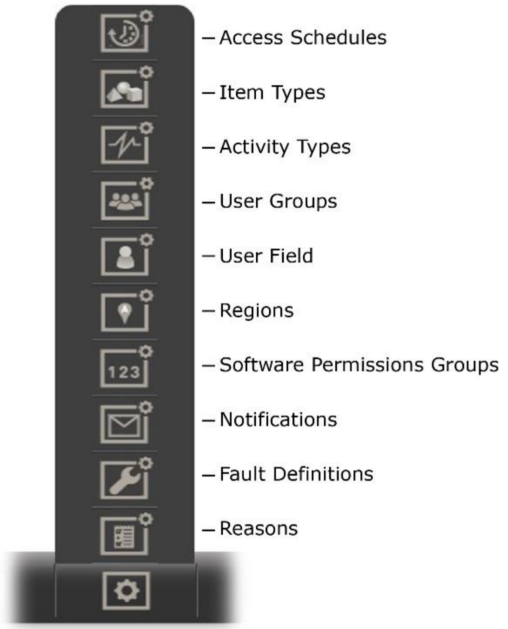
Clicking on these buttons will take you to the corresponding page. However, there are two exceptions to this. Items and Software Settings have sub menus that will appear when they have been clicked once.

-Item Booking

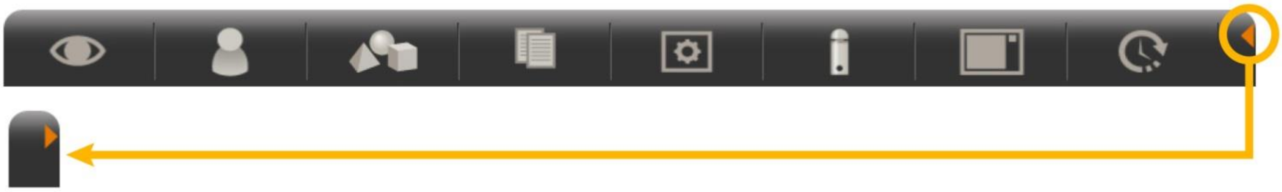
-Outstanding Faults

-Item Access Groups

-Items



Clicking the orange arrow at the end of the toolbar will minimise it to the left-hand side of the screen. Clicking a second time will restore it to its original size.



For more information on the other pages of TrakaWEB, please review the Main User Guide section.

3.6.3.2 RIBBON TOOLBAR

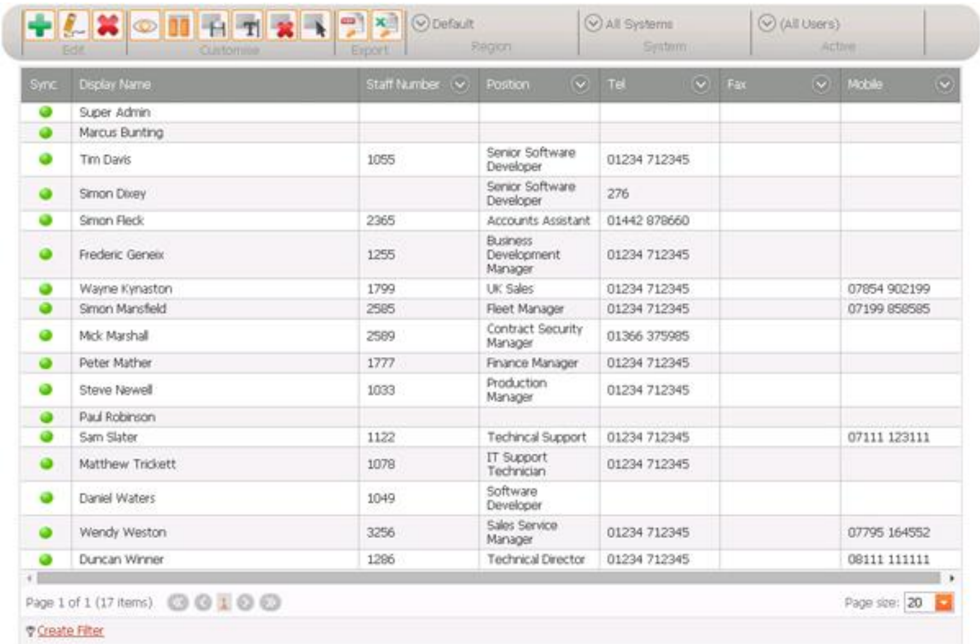
Located at the top of most pages throughout TrakaWEB is the Ribbon Toolbar. From here, you can select various options that are specific to each page e.g., if you were currently viewing the User page you would see the following ribbon toolbar.

The drop-down sections on the toolbar consist of System, Region and Status selection. Clicking the small arrow button next to the system or region name will display a list of the systems/regions that currently exist in your database. For more information, please see the separate topics for Systems and Regions. The status selection will only be found in some areas of TrakaWEB, such as the User List. This allows you to filter the users if they are active or inactive. You can also select an 'All' option to view all users.

Filtering

There are several ways to filter information in TrakaWEB by using the ribbon toolbar. On the right hand side of the toolbar, you will see columns such as Region, System, Status, Type etc. These change throughout TrakaWEB and apply to the page you are currently viewing.

Simply select the drop-down arrow and select one of the supplied options and the corresponding grid will filter the information accordingly. For example, below is an image of the user list. In this instance, the customer has a database with many systems that are also in different regions and many users who have access to various items.

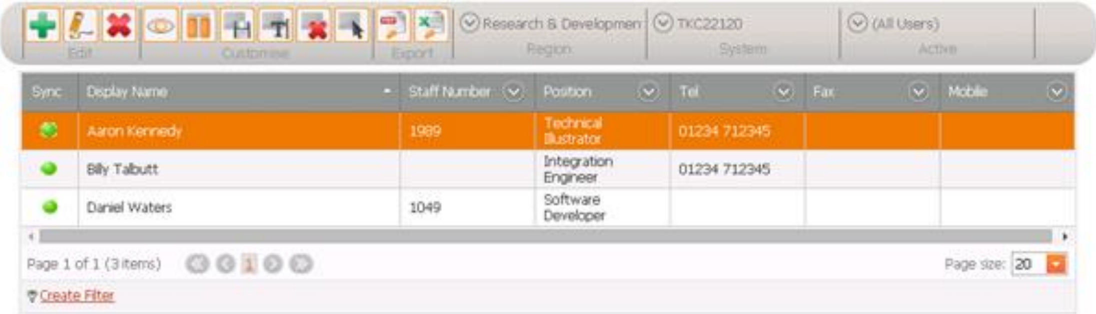


Sync	Display Name	Staff Number	Position	Tel	Fax	Mobile
	Super Admin					
	Marcus Bunting					
	Tim Davis	1055	Senior Software Developer	01234 712345		
	Simon Dixey		Senior Software Developer	276		
	Simon Fleck	2365	Accounts Assistant	01442 878660		
	Frederic Geneix	1255	Business Development Manager	01234 712345		
	Wayne Kynaston	1799	UK Sales	01234 712345		07854 902199
	Simon Mansfield	2585	Fleet Manager	01234 712345		07199 858585
	Mick Marshall	2589	Contract Security Manager	01366 375985		
	Peter Mather	1777	Finance Manager	01234 712345		
	Steve Newell	1033	Production Manager	01234 712345		
	Paul Robinson					
	Sam Slater	1122	Technical Support	01234 712345		07111 123111
	Matthew Trickett	1078	IT Support Technician	01234 712345		
	Daniel Waters	1049	Software Developer			
	Wendy Weston	3256	Sales Service Manager	01234 712345		07795 164552
	Duncan Winner	1286	Technical Director	01234 712345		08111 111111

To find all the users that are in a specific region, simply select the Region drop down selection arrow and choose a region from the pre-configured options.

This will then narrow down the list of users to those who are only in the specified region. You can further strengthen this search by selecting a specific system within the region.

Now the results have been filtered twice making it easier to find the information that is required.



Common Buttons in TrakaWEB

The buttons and options on the ribbon toolbar will change according to the page you are currently working on. Several common buttons appear in many places throughout TrakaWEB. Please see below for button descriptions. Please use the hyperlinks to view more information about the feature the buttons represent.

General Options

 Add

 Edit

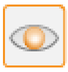
 Delete

 Save

 Save & Return

 Cancel & Return

Customise Options

 Search

 Show/Hide Grid Columns

 Save Layout

 Rename Layout

 Delete Layout

 Select Layout

Export Options

 Export to PDF

 Export to Excel

3.6.3.3 GENERAL OPTIONS

Add

When viewing such pages as users or items, you can click the Add button to add a new user/item/group etc. to the database.

Edit

When viewing such pages as users or items, you can highlight an existing user or item and click the Edit button to edit that particular user/item/group etc.

Delete

When viewing such pages as users or items, you can highlight a line of data and click the Delete button to delete that user/item/group etc.

Save

The Save button can be found in various places throughout TrakaWEB, selecting it will save any changes you have made or are currently making.

Save & Return

The Save & Return button can be found in various places throughout TrakaWEB. Selecting it will save any changes you have made and take you back to the previous page.

Cancel & Return

The Cancel & Return button can be found in various places throughout TrakaWEB. Selecting it will cancel any changes you have made and take you back to the previous page.

4. MAIN USER GUIDE

4.1 RIBBON TOOLBAR

4.1.1 CUSTOMISE OPTIONS

4.1.1.1 SEARCHING

Throughout TrakaWEB, you can Search grids for specific information. Selecting the search button from the ribbon toolbar will enable you to search for a user, activity, item description etc. directly from each column in the grid.

The example below shows the search feature being used on the Activity grid from the system viewer. Although the grids throughout TrakaWEB are different, the principle of the search tool remains the same.

1. Click the search button from the ribbon toolbar.

2. Each column in the grid will have its own search field. If you want to know what activities transpired between two dates, then you would search those dates in the 'When' column. In the example below the name Duncan has been entered into the 'Who' column of the Item Activity grid.

Item Activity | Access | System Activity | Items

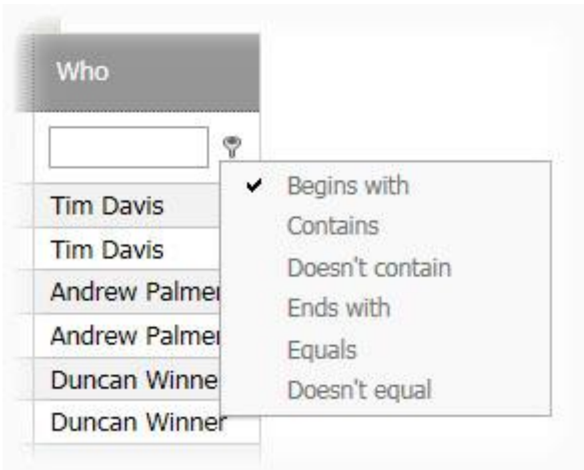
Activity	When	Who
		Duncan
Item Returned	15/03/2013 16:44:40	Tim Davis
Item Removed	15/03/2013 16:44:16	Tim Davis
Item Returned	15/03/2013 16:44:03	Andrew Palmer
Item Removed	15/03/2013 16:40:35	Andrew Palmer
Item Returned	15/03/2013 16:37:55	Duncan Winner
Item Removed	15/03/2013 16:37:43	Duncan Winner
Unauthorised Item Returned	15/03/2013 15:56:09	
Item Removed	15/03/2013 15:56:02	Aaron Kennedy
Item Returned	15/03/2013 15:55:59	Aaron Kennedy
Item Removed	15/03/2013 15:55:57	Aaron Kennedy
Item Returned	15/03/2013 15:55:55	Aaron Kennedy
Item Removed	15/03/2013 15:55:53	Aaron Kennedy

TrakaWEB will now search for any activities that have transpired against anyone with the name Duncan.

TIP: As you can see in the example above, there are two users with the same first name. Therefore, to find the specific data' add as much information as possible into your searches. In this example, adding a second name would narrow the search down to a particular user rather than a group of users who share a first name.

Search Filters

When the search feature is enabled, a small grey icon will appear at the right-hand side of the search field. Clicking this will display a small drop-down box with several filtering terms that can be applied to your search. For example, selecting the term 'begins with' is useful when searching a user's first name.



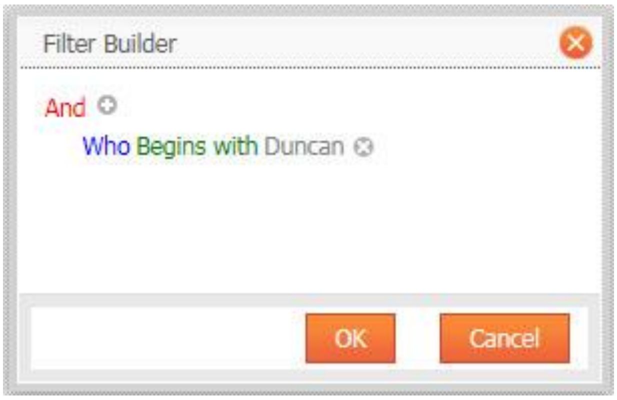
Clearing Searches

Clicking 'Clear' in the bottom right-hand corner of the grid will clear the current search and the grid of all information before the search took place.

Filter Builder

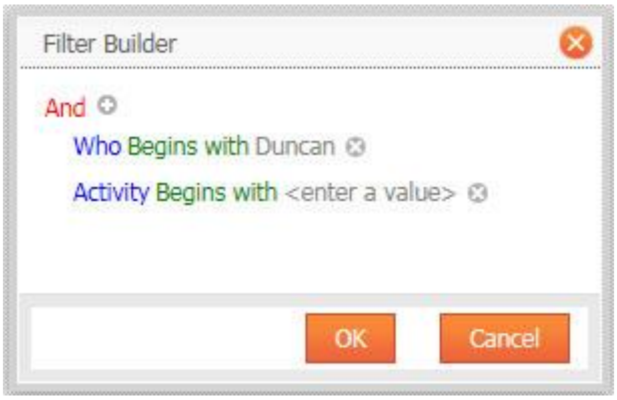
The Filter Builder allows you to add multiple filters to each search. After you have entered a search term, such as the name Duncan into the 'Who' column, the bottom left of the grid will display the current filter setting. In the image below, the filter was set to 'Begins with Who' and the search term was 'Duncan'. Which means any activities generated by anyone named Duncan will be displayed in the activity grid. At the bottom left-hand side of the grid in red text are the details of the current search. Clicking that text will open a new window that will allow you to add multiple filters to one search, narrowing your results and making it easier to find the information you are looking for.

The Filter Builder will list the filters used to generate the last search. In this case, the filter was set to the column 'Who' (highlighted blue), the value searched against was 'Begins With' (highlighted green) and the search term was 'Duncan' (highlighted grey).



Clicking 'And' will add another filter to the list. Each filter is split into three definable sections. The first is the column section highlighted in blue, the second is the filter value highlighted green and third is the search term highlighted in grey.

NOTE: Each definable section such as columns (highlighted in blue) will be different for each page of TrakaWEB you are viewing, e.g., using the Filter Builder to search in Item Types, there will only be one option for the columns section as you can only search by the name of the item type.



4.1.1.2 LAYOUTS OVERVIEW

A Layout is a combination of columns you can apply to most of the grids across TrakaWEB. After you have added or removed columns from a particular grid, you can save that particular selection which is known as a 'Layout'. Once saved, the layout will keep the columns in the order which you left them when it was saved.

In the example below, the user is currently on the System Viewer page with position two highlighted and is now looking at the Access tab on the Activity & Access grid. By selecting a layout that has already been saved, you can see that two extra columns have appeared providing more information about the users who have access to position two.

NOTE: All layouts are exclusive to the grids or tabs, which they are made for. For example, you cannot create a layout for the grid on the User List page and then apply it to the grid on the Items page. Each grid contains different information concerning the data it represents. Layouts from other grids may not be applicable to the information on other pages.

NOTE: If you are viewing or creating a new layout and leave the page and return, the grid will automatically switch to the default layout, and you will need to Select a Layout.

 Creating a layout - Show/Hide Grid Columns

 How to Save a Layout

 How to Rename a Layout

 How to Delete a Layout

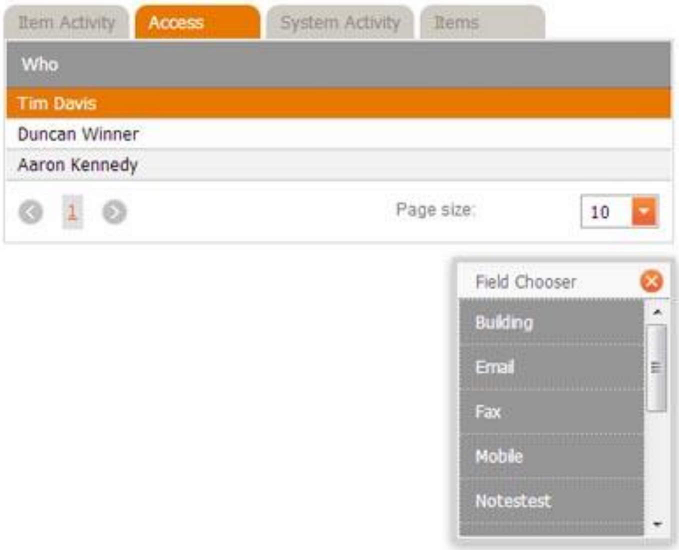
 How to Select a Layout

4.1.1.3 SHOW/HIDE GRID COLUMNS

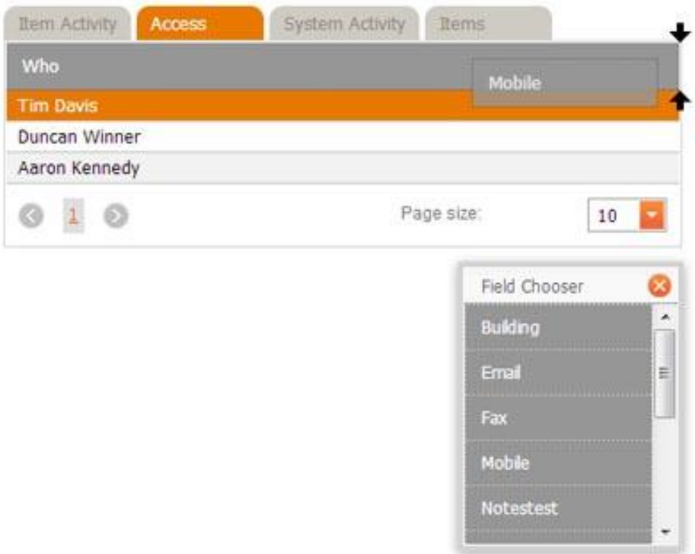
Throughout TrakaWEB, there are many grids that display important information for the page you are currently viewing. For example, the System Viewer has the Activity & Access Grid, which has four different tabs that display all the information for the currently selected position. The Show/Hide Grid Columns button allows you to add or remove fields of your choice to the tab you are currently viewing. Once you have added a field to the grid, it becomes a column that you can move or remove.

When adding extra fields to a grid, it is important to remember that each tab is different and the fields that can be placed and taken away will vary from grid to grid. In the example below, we have selected the field 'Mobile' to be added to the grid.

1. From the ribbon toolbar, select the Show/Hide Grid Columns button. A small window will appear with a number of different fields to add to your existing columns. Depending on the page you are viewing and the current data on screen, each grid or tab will have a different selection of columns for you to select and customise. In the example below, the fields you can select from are relevant to user i.e., mobile number, fax, email etc. These fields are definable in the User Fields.



2. To add a column to your grid, simply drag and drop the desired field between the other columns. The black arrows will indicate where the new field will fit into the grid.



3. Once the field is placed, the grid will show the data that field represents. In this case, the 'mobile' field was added, therefore, if the users listed in the grid have a mobile number entered into their user details page, it will now be displayed here.

4. You can add multiple fields to a grid by simply following steps 1-3.

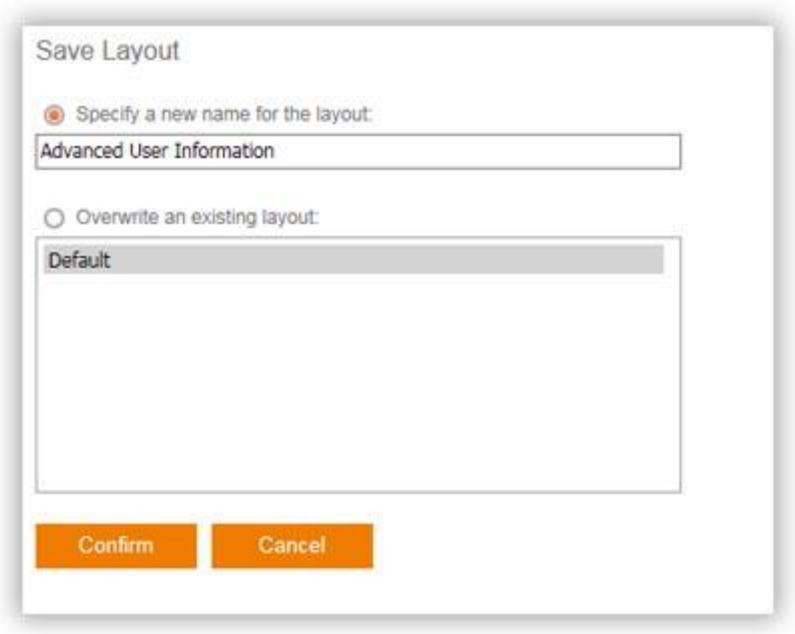
5. If you have a specific set of columns that you may wish to view again, you can save them and give them a unique name. This is known as a Layout. Please review the following topic to Save a Layout.

4.1.1.4 SAVE LAYOUT

After you have customised a grid by adding, moving or deleting columns/fields, you have the option to save that selection so that you can later return to the same grid and select a pre-configured layout without having to select different columns/fields.

1. Click the 'Save Layout' button at the top of the page in the Ribbon Toolbar.

2. The following window will appear prompting you to assign a name to the layout. You have the option of saving a new layout or overwriting an existing one.



3. Enter a name for the layout and click Confirm.

4. The layout is now saved and can be renamed, deleted or selected from the Ribbon Toolbar.


How to Rename a Layout

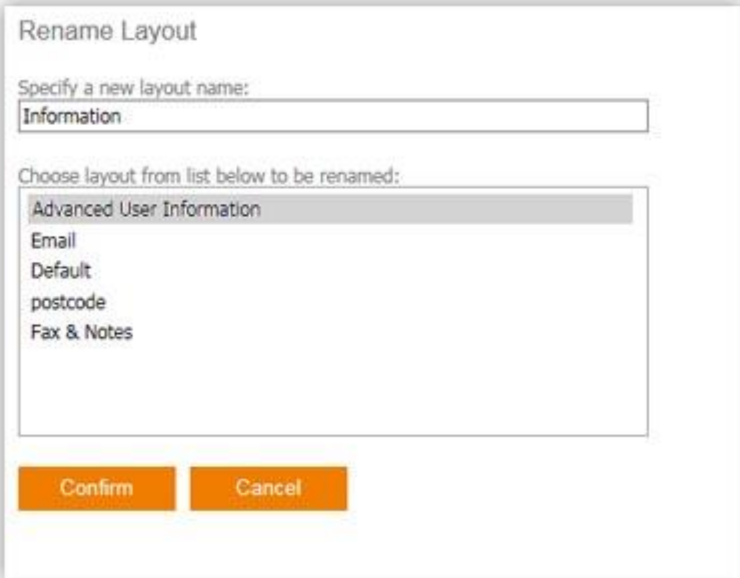

How to Delete a Layout


How to Select a Layout

4.1.1.5 RENAME LAYOUT

After a layout has been saved, you can rename it at any time if you wish to do so.

1. Click the Rename Layout button at the top of the page in the Ribbon Toolbar.
2. The following window will appear prompting you to select a layout and enter a new name.



3. Once you have selected the desired layout and typed in its new name, click the Confirm button.
4. The layout is now saved against its new name. You can delete or select it from the Ribbon Toolbar.

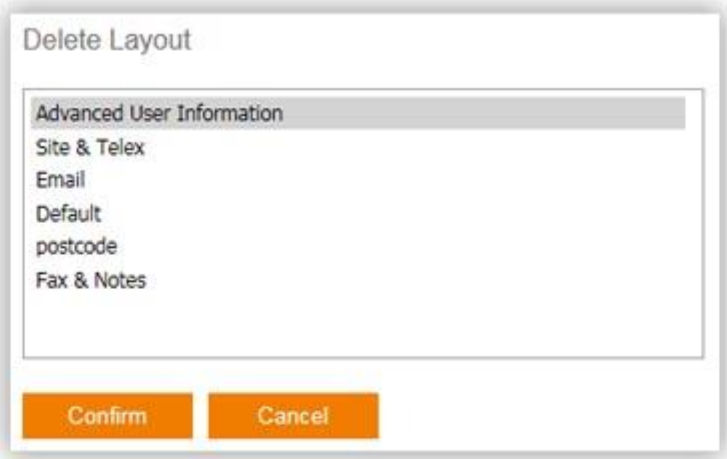
 How to Delete a Layout

 How to Select a Layout

4.1.1.6 DELETE LAYOUT

After a layout has been saved, you can delete it at any time if you wish to do so.

1. Click the Delete Layout button at the top of the page in the Ribbon Toolbar.
2. The following window will appear prompting you to select a layout to delete.



3. Once you have selected the desired layout click the Confirm button.
4. The layout has been deleted and is no longer selectable or editable.

 Creating a layout - Show/Hide Grid Columns

 How to Save a Layout

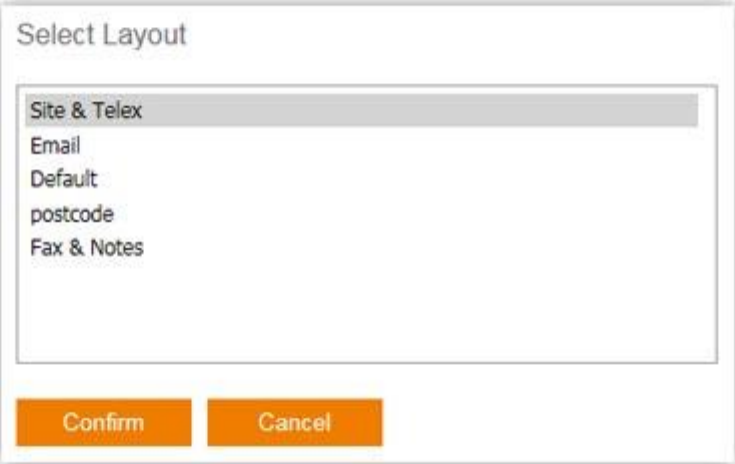
 How to Rename a Layout

 How to Select a Layout

4.1.1.7 SELECT LAYOUT

After a layout has been saved, you can select it and any other layouts at any time.

1. Click the Select Layout button at the top of the page in the Ribbon Toolbar.
2. The following window will appear prompting you to select a layout to view.



3. Once you have selected the desired layout click the Confirm button.
4. The previous layout being displayed on the grid will now change to the newly selected layout.

 Creating a layout - Show/Hide Grid Columns

 How to Save a Layout

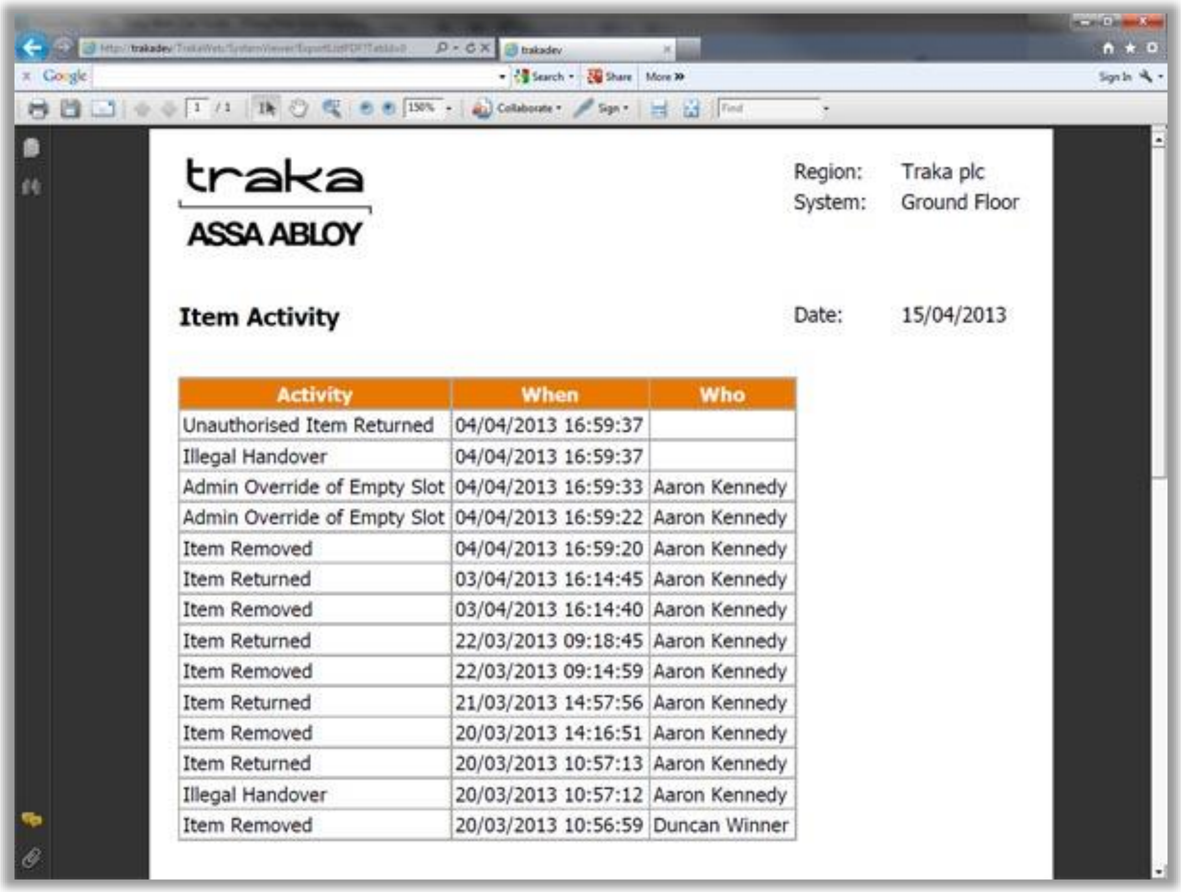
 How to Rename a Layout

 How to Delete a Layout

4.1.2 EXPORT OPTIONS

4.1.2.1 EXPORT TO PDF

In TrakaWEB, it is possible to export the data from whatever grid you are viewing into PDF format. Simply select the Export to PDF button from the ribbon toolbar and TrakaWEB will open a new tab in your browser with the currently viewed data into a PDF.



traka
ASSA ABLOY

Region: Traka plc
System: Ground Floor

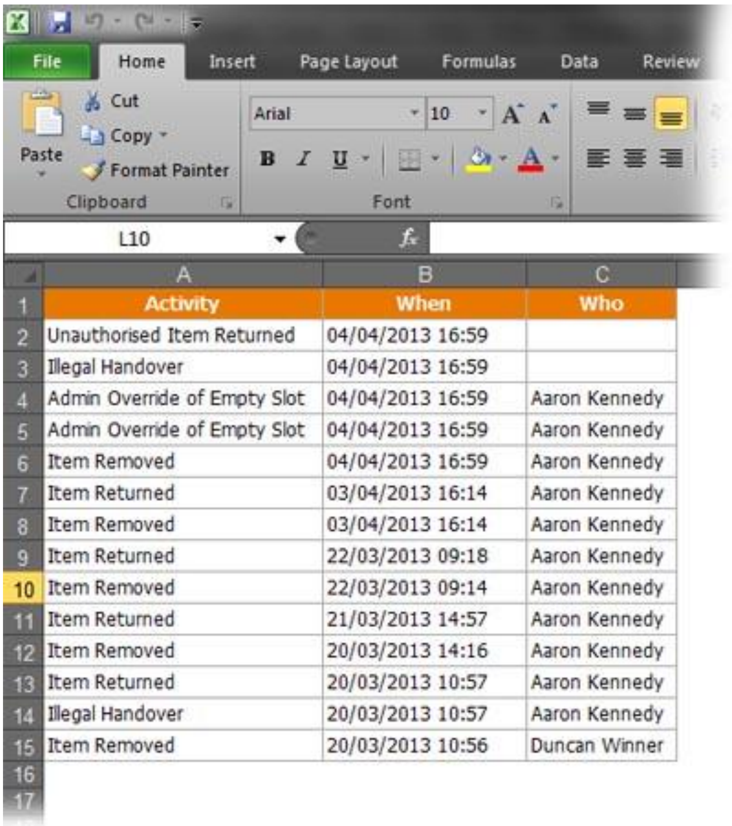
Item Activity

Date: 15/04/2013

Activity	When	Who
Unauthorised Item Returned	04/04/2013 16:59:37	
Illegal Handover	04/04/2013 16:59:37	
Admin Override of Empty Slot	04/04/2013 16:59:33	Aaron Kennedy
Admin Override of Empty Slot	04/04/2013 16:59:22	Aaron Kennedy
Item Removed	04/04/2013 16:59:20	Aaron Kennedy
Item Returned	03/04/2013 16:14:45	Aaron Kennedy
Item Removed	03/04/2013 16:14:40	Aaron Kennedy
Item Returned	22/03/2013 09:18:45	Aaron Kennedy
Item Removed	22/03/2013 09:14:59	Aaron Kennedy
Item Returned	21/03/2013 14:57:56	Aaron Kennedy
Item Removed	20/03/2013 14:16:51	Aaron Kennedy
Item Returned	20/03/2013 10:57:13	Aaron Kennedy
Illegal Handover	20/03/2013 10:57:12	Aaron Kennedy
Item Removed	20/03/2013 10:56:59	Duncan Winner

4.1.2.1 EXPORT TO EXCEL

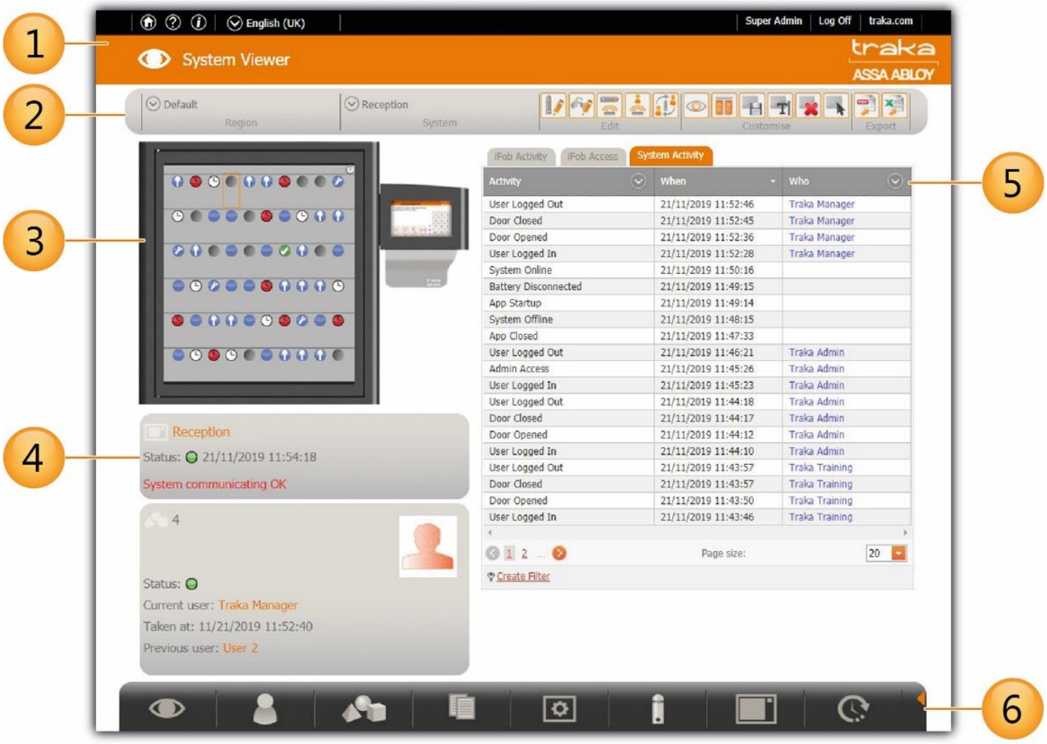
In TrakaWEB, it is possible to export the data from whatever grid you are viewing into a Microsoft Excel format. Simply select the Export to Excel button from the ribbon toolbar and TrakaWEB will generate a new tab in your browser with the currently viewed data into an Excel Spreadsheet.



Activity	When	Who
Unauthorised Item Returned	04/04/2013 16:59	
Illegal Handover	04/04/2013 16:59	
Admin Override of Empty Slot	04/04/2013 16:59	Aaron Kennedy
Admin Override of Empty Slot	04/04/2013 16:59	Aaron Kennedy
Item Removed	04/04/2013 16:59	Aaron Kennedy
Item Returned	03/04/2013 16:14	Aaron Kennedy
Item Removed	03/04/2013 16:14	Aaron Kennedy
Item Returned	22/03/2013 09:18	Aaron Kennedy
Item Removed	22/03/2013 09:14	Aaron Kennedy
Item Returned	21/03/2013 14:57	Aaron Kennedy
Item Removed	20/03/2013 14:16	Aaron Kennedy
Item Returned	20/03/2013 10:57	Aaron Kennedy
Illegal Handover	20/03/2013 10:57	Aaron Kennedy
Item Removed	20/03/2013 10:56	Duncan Winner

4.2 SYSTEM VIEWER

The System Viewer allows you to see a representation of your Traka Touch system on your PC. This is the 'Home' screen of TrakaWEB that will appear each time you log in. From here, you can view all the activity of each system in the database. Only one system can be viewed at a time.



1 - General Interface

The General Interface is the buttons and options located at the top of each page in the black and orange banner. This interface will display certain buttons and information that are used in every aspect of TrakaWEB no matter where you navigate to. Please follow the link for more details about the TrakaWEB Interface.

2 - Ribbon Toolbar

The Ribbon Toolbar is located at the top of most pages throughout TrakaWEB and contains buttons and drop down menus relevant to each section.

The drop down section to the left of the ribbon toolbar is for System and Region selection. Clicking the small arrow button next to the system or region name will display a list of the systems /regions that currently exist in your database. For more information, please see the separate topics for Systems and Regions.

The buttons on the right in the 'Tool' section are only relevant to the system viewer page. Other buttons in the 'Customise' & 'Export' sections can be found in other places in TrakaWEB. Please see below descriptions of each 'Tool' button and Hyperlinks to the relevant topics.

[Edit iFob](#) [Edit Items](#) [Remote Release](#) [Remote User Login](#) [Transfer Ownership](#)

For more information on the 'Customise' & 'Export' buttons, please review the ribbon toolbar topic.

3 - System Display

The System Viewer displays an interactive image that represents the type of Traka Touch system you have. The colours and icons of the iFobs/Items in the system viewer change depending on their current status. These icons also differ between Key Cabinets and Locker Systems.

The drop-down sections to the left of the Ribbon Toolbar are the System and Region selection. Clicking the small arrow button next to the System or Region name will display a list of the Systems/Regions that currently exist in your database.

Key Cabinet Status Icons

No iFob defined

iFob currently in the system with no items attached

iFob currently in the system with items attached

iFob with no items currently out of the system

iFob with items currently out of the system

iFob currently out of the system and under a curfew

iFob currently out of the system and is overdue

iFob currently in the system and has a fault logged against it

iFob currently in the system and has a repaired fault logged against it

iFob in the wrong slot. The X shows the where the iFob has been incorrectly located

iFob in the wrong slot. The ✓ shows the where the iFob should be correctly located

No information available on the related iFob and/or item

Locker System Status Icons

- Asset currently in the system with no item defined

- Asset currently in the system with item defined

- Asset with no item defined currently out of the system

- Asset with item defined currently out of the system

- Asset currently out of the system and under a curfew

- Asset currently out of the system and is overdue

- Asset in wrong compartment. The X shows where the asset has been incorrectly located

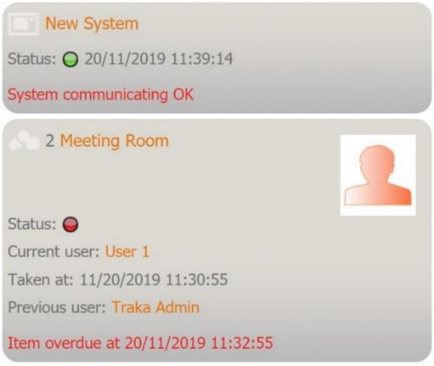
- Asset in wrong compartment. The ✓ shows where the asset should be correctly located

- Asset has become undetectable

NOTE: The Locker System status icons will not update for Non-RFID Locker Systems as it is not possible to detect if an asset is present in the system.

4 - System & Item Detail Panels

The system & Item Detail Panels will be located either below the cabinet image (if the system is a Key cabinet) or to the right of the Locker/System Viewer Grid (if the system is a Locker). The first panel shows the status of the system and the second shows the status of the item for the currently selected position.



System Detail Panel
The System Detail Panel shows the status of the Traka Touch system. It will display the system title, date & time at the system, and the connection status. If the status LED is green, that indicates the system is currently connected to TrakaWEB. If the LED turns red, this will mean there has been a disconnection, check the network cable has not been removed and ensure the system is switched on.

Item Detail Panel
The Item Detail panel shows the iFob or item description, the user who currently has the item, when it was taken, the previous user who removed the item and if the iFob/item has a curfew. In the image above, position 2 is highlighted; therefore, the Item Detail Panel is showing a red LED indicating that a curfew has been placed on the item and is overdue. In this case, the iFob/item had a curfew and should have been returned to the system at 11:32 on the 20/11/19 but has not been returned. Therefore, a message has appeared at the bottom of the panel stating that the item is overdue.

5 - Item Activity & Access Grid

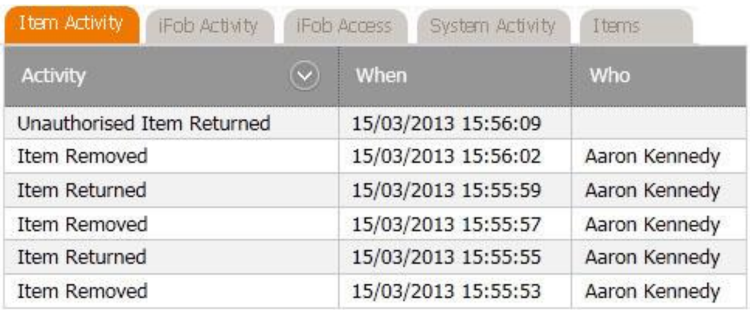
To the right of the cabinet image is the Item Activity & Access grid. This grid will display...

- The last 30 days of activities for the items in the selected position.
- The last 30 days of activities for the iFob (RFID Tag if it is a locker system) in the selected position.
- All users who have access to the iFob/item in the selected position.
- The last 30 days of system activity.
- The items defined for the selected position.

Item Activity

The item activity tab displays the last 30 days of activities for the item(s) in the selected position. This grid will show you who removed and returned the item and what time it was removed/returned. You can run various reports for a more in depth look at these activities.

In a Traka Touch Key Cabinet, multiple items can be attached to an iFob; therefore, the item activity tab will display individual lines for each of the items attached to that iFob when it is removed/returned.



Activity	When	Who
Unauthorised Item Returned	15/03/2013 15:56:09	
Item Removed	15/03/2013 15:56:02	Aaron Kennedy
Item Returned	15/03/2013 15:55:59	Aaron Kennedy
Item Removed	15/03/2013 15:55:57	Aaron Kennedy
Item Returned	15/03/2013 15:55:55	Aaron Kennedy
Item Removed	15/03/2013 15:55:53	Aaron Kennedy

iFob Activity

The iFob activity tab displays the last 30 days of activities for the iFob in the selected position.

If your system is an RFID Locker System, it will not contain iFobs. Therefore, the term 'iFob' is referring to the 'RFID Tag'. It is not possible to attach more than one item to an RFID Tag. Therefore, once an item has been defined, the Item Activity and iFob Activity tabs will display the same events.

Item Activity | iFob Activity | iFob Access | System Activity | Items

Activity	When	Who
Return Notes Not Entered	01/09/2014 09:50:21	Aaron Kennedy
Item Returned	01/09/2014 09:50:16	Aaron Kennedy
Item Removed	01/09/2014 09:50:14	Aaron Kennedy
Return Notes Not Entered	29/08/2014 11:35:46	Aaron Kennedy
Item Returned	29/08/2014 11:35:42	Aaron Kennedy
Item Removed	29/08/2014 11:35:41	Aaron Kennedy
Unauthorised Item Returned	29/08/2014 11:06:44	

iFob Access

This tab lists the users who currently have access to the selected position.

Item Activity | iFob Activity | iFob Access | System Activity | Items

Who
Duncan Winner
Aaron Kennedy

System Activity

This table is very similar to the 'Item Activity'. It displays the last 30 days of activities that have occurred at the system, e.g., Door Opened, Door Closed, Admin Access etc.

Item Activity | iFob Activity | iFob Access | System Activity | Items

Activity	When	Who
Door Closed	15/03/2013 15:56:03	Aaron Kennedy
Door Opened	15/03/2013 15:55:39	Aaron Kennedy
Admin Access	15/03/2013 11:40:18	
Admin Access	15/03/2013 09:58:11	
Memory Low	14/03/2013 17:21:03	
Memory OK	14/03/2013 17:20:23	

Items

This tab displays the details of the items currently attached to the iFob/RFID Tag. These description details are definable from the Edit Item Type section.

Item Activity | iFob Activity | iFob Access | System Activity | Items

iFob Description
red car 2,Safe Key
red car 2,Safe Key

6 - Navigation Bar

At the bottom of each page in TrakaWEB, you will notice the Navigation toolbar. From here, you will be able to navigate to the different pages of TrakaWEB such as the System Viewer, Users, and Systems etc.

4.2.1 TRAKAWEB SYSTEM VIEWER GRID

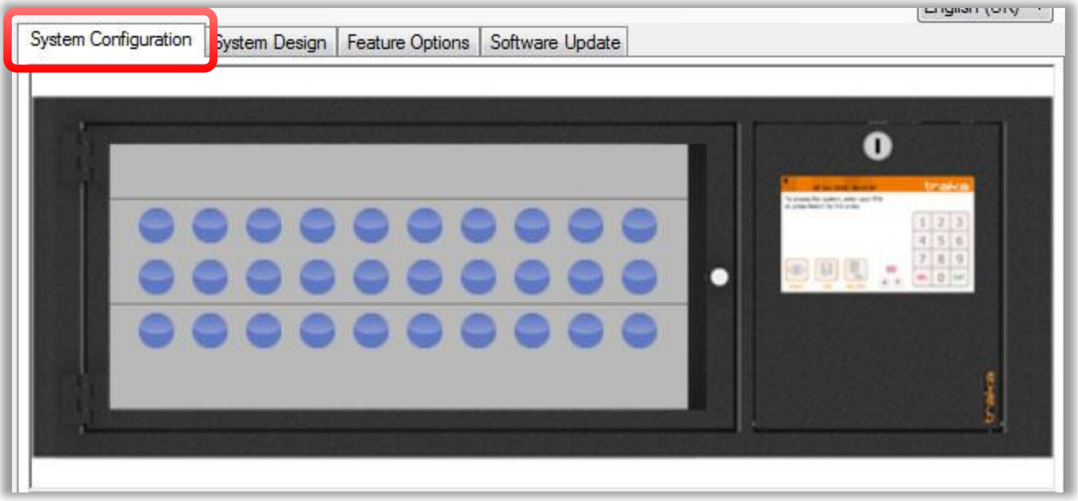
Due to the many permutations of physical locker designs, it is not always possible to display the interactive image of the locker within the TrakaWEB system viewer. Currently, there are only a subset of locker images available to use and so to resolve the issue, a System Viewer Grid is used. The System Viewer Grid shows the status of the physical system within TrakaWEB without having to display an image of the actual locker or cabinet.

Configuration of the System Viewer Grid is done within TrakaWEB Admin on a per-system basis. Although the option is available for both cabinets and lockers, the option to customise the TrakaWEB System Viewer Grid is specific to lockers only.

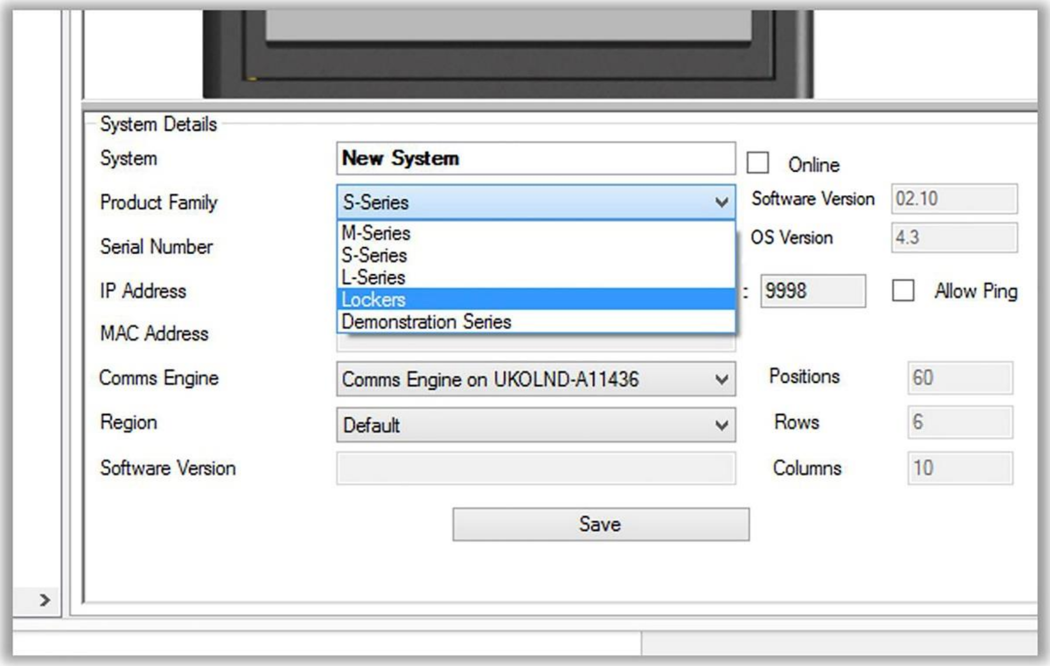
NOTE: When configuring cabinets, a user has the option to either view the system viewer grid or the interactive image within the system viewer in TrakaWEB.

System View Option and Custom Product Type

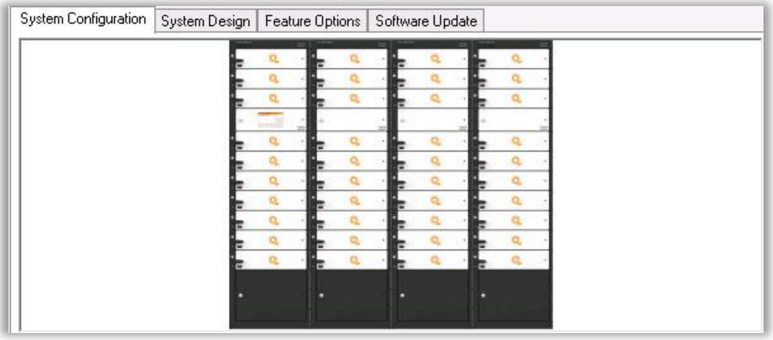
After launching the TrakaWEB Admin Application, the System Configuration screen will be displayed.



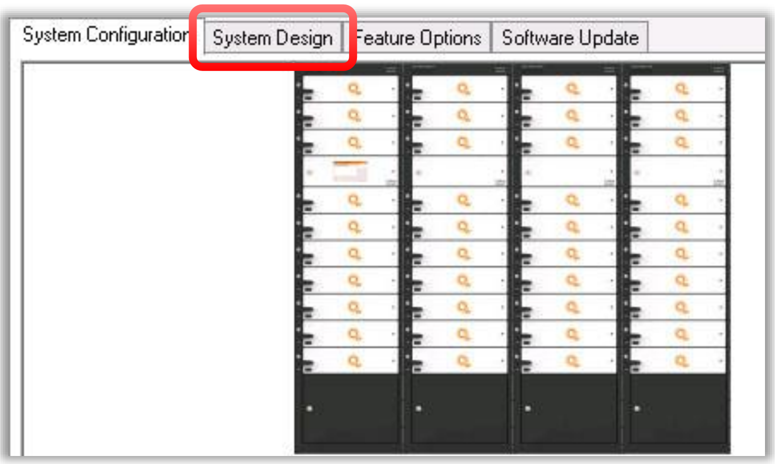
1. Locate the Product Family drop down menu to choose a specific system type.



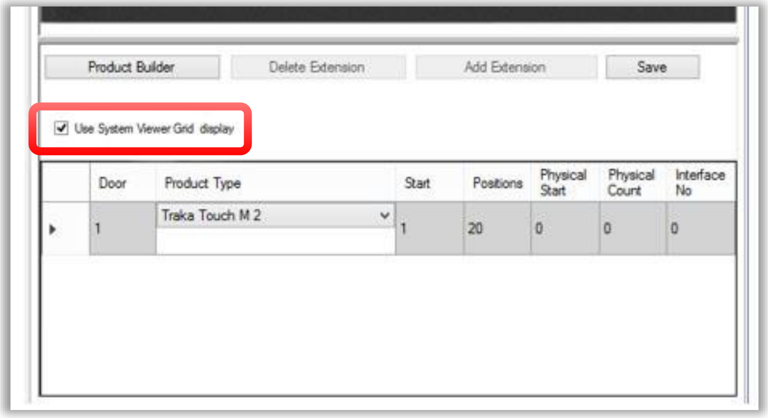
The screen will change to display the default locker image.



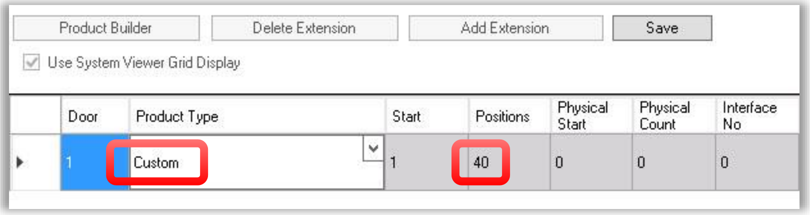
2. Click on the 'System Design' tab to edit the selected system type.



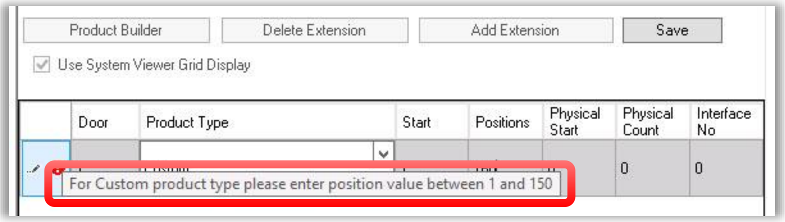
3. Within the System Design tab, click on the 'Use System Viewer Grid display' tick box.



If the system to be configured is a locker, the 'Custom' option will be made available from the Product Type drop down menu. The custom product type is a product type that should be used when there is no system image available for the locker. When using the custom product type the user will be required to manually enter a number into the 'Positions' field for this system. The maximum value that can be entered will be 150.

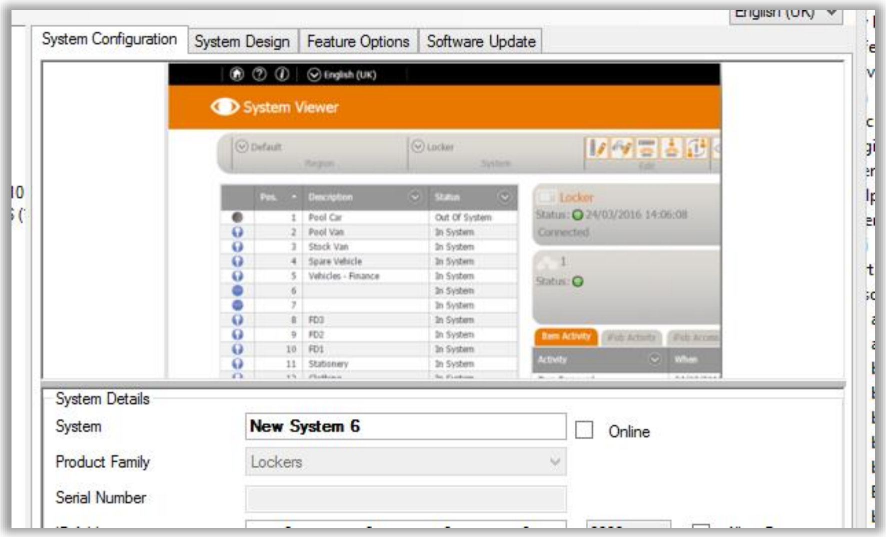


NOTE: The maximum value that can be entered within the 'Positions' field is 150. If this value is exceeded, an icon will appear in the left-hand box. Hovering the mouse cursor over the icon will display a message informing the user of this.



NOTE: If 'Custom' has been selected, the 'System Viewer Grid' must be used with that particular system. The tick box to select the 'Use System Viewer Grid Display' will be ticked and greyed out and the Product Builder will also be disabled.

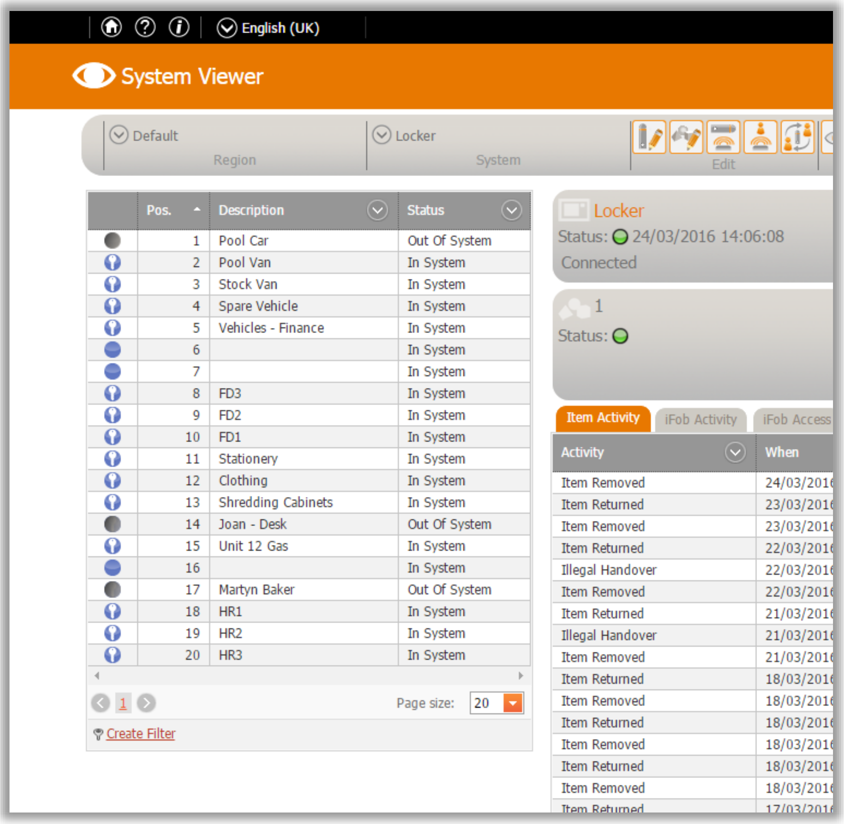
With the 'Custom' option enabled, a generic image will be displayed in place of the usual system image to indicate that this system is a custom type and that no image is currently available.



TrakaWEB System Viewer

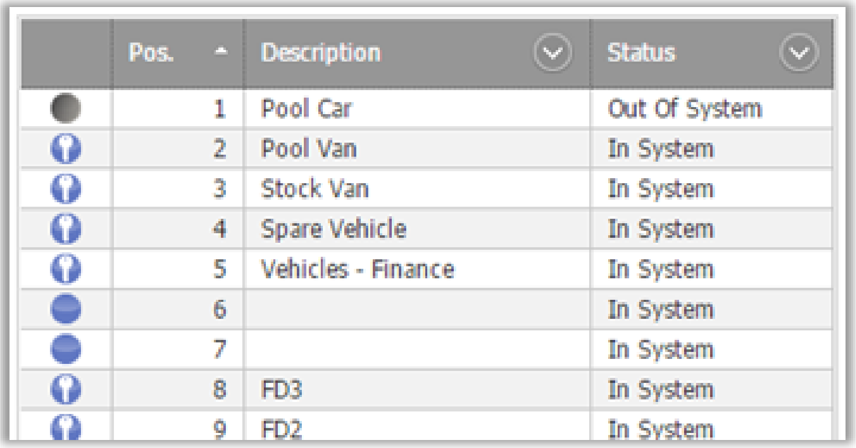
When TrakaWEB is launched, the System Viewer page will check to see if the current system should be displayed by an image or a System Viewer Grid as it loads. If the System Viewer Grid display is to be used, then the status information will relocate from the bottom left of the page to the top right of the page above the activity grids location.

The System Viewer Grid layout will change depending on which return type the system has been assigned. A typical System Viewer Grid may appear as shown below:



Fixed Return

For a fixed return system, each physical position will be represented by a row within the System Viewer Grid. Each row will be divided into columns as shown below.



Random Return to Single System

For a Random Return to Single System, each physical position in the system will be represented by a row in the System Viewer Grid. A row will also be displayed for each iFob that is not in the system.

When an iFob is removed from the system, its position will remain but its icon will turn grey to show that the iFob is not in the system. A new row will then be added to the bottom of the grid to show which particular iFob has been removed. Its Index, Description and Status will also be displayed. This is shown in the example below.

The iFob's in position 6 and 7 have been removed from the system. Two new rows are created at the bottom of the grid reflecting their current status.

	Pos.	Index	Description	Status
	1	1	Silver Ford Focus	In System
	2	2	Red Ford Focus	In System
	3	3	Silver Ford Focus	In System
	4	4	Silver Mercedes	In System
	5	5	Grey Audi	In System
	6			Out Of System
	7			Out Of System
	8	8		In System
	9	9		In System
	10	10		In System
		6	Transit Van 2	Out Of System
		7	Transit Van 1	Out Of System

4.2.2 RIBBON TOOLBAR BUTTONS

4.2.2.1 REMOTE RELEASE

This option allows you to remotely release an iFob/Item or open a locker compartment door from the system for a user. Clicking the Remote Release button will open a small window, which will prompt you to select a user to release an item to. Simply highlight the desired user and select Remote Release. Alternatively, you can select the 'unknown user' tick box if you wish to release the iFob/item to a user who is not in the database.

You have the choice to release it to both users who do have access to the iFob/item, and users who do not.

The pop-up window will now give a real time update of the removal process. The door on the Traka Touch system or Locker System will now open and prompt the user to remove the iFob/item.

4.2.2.2 REMOTE USER LOGIN

This option allows someone using TrakaWEB to remotely log another user into the system. Selecting this icon from the ribbon toolbar will present the Web user with a pop-up box allowing them to select a user to allow access to the system.

If the user has access to only items, the system will display the item selection screen and automatically open the system door (on Key Cabinets). If the user has admin/report permissions, they will be given an option to remove items or enter the admin/reports menu etc.

4.2.2.3 TRANSFER OWNERSHIP

This option allows you to transfer the ownership of the item(s) in the selected position to another user whilst the item(s) is/are already out of the system. Clicking the Transfer Ownership button will open a small window, which will prompt you to select a user to transfer to. Simply highlight the desired user and select Transfer.

You have the choice to transfer it to both users who do have access to the item, and users who do not.

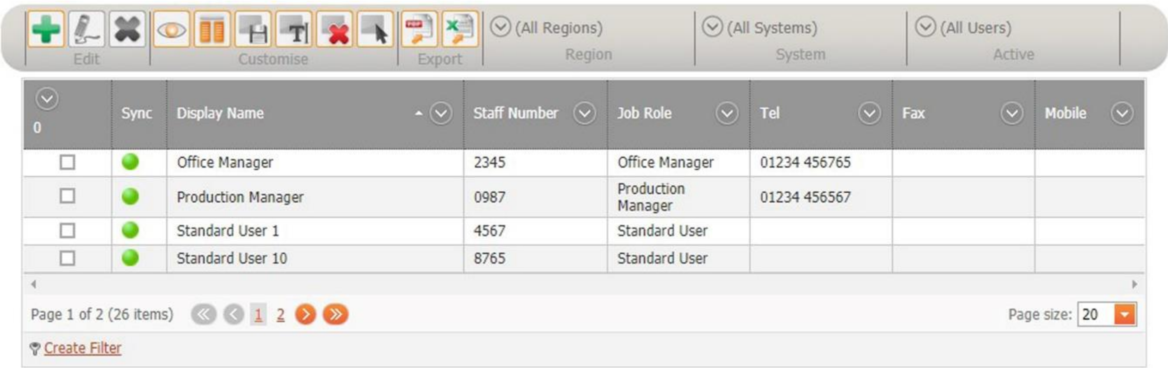
The pop-up window will now display the details of the transfer process. TrakaWEB will now show that the user who currently has the item out of the system has changed.

4.3 USERS

Within TrakaWEB, users can be added, edited and deleted. This may be achieved on a user-by-user basis as outlined in this section, or multiple users can be edited at once by using the Multi-Select/Multi-Edit feature.

4.3.1 USERS LIST

From the Navigation Toolbar select the 'Users' icon. If you already have users set up in your Traka Touch system, then this list will be populated with all of those users along with all the other users in the database. If you have not added any users to your system, you will need to Add Users.



Region, System & Active Filters

When looking at the user list, you can filter which users are displayed by using the Region, System and Active drop-down filters located on the right-hand side of the Ribbon Toolbar. Clicking the arrow button next to each field will show you a list of selectable filter types, depending on what has been configured. For more information, please refer to the Regions and Systems topics.

Sync Column

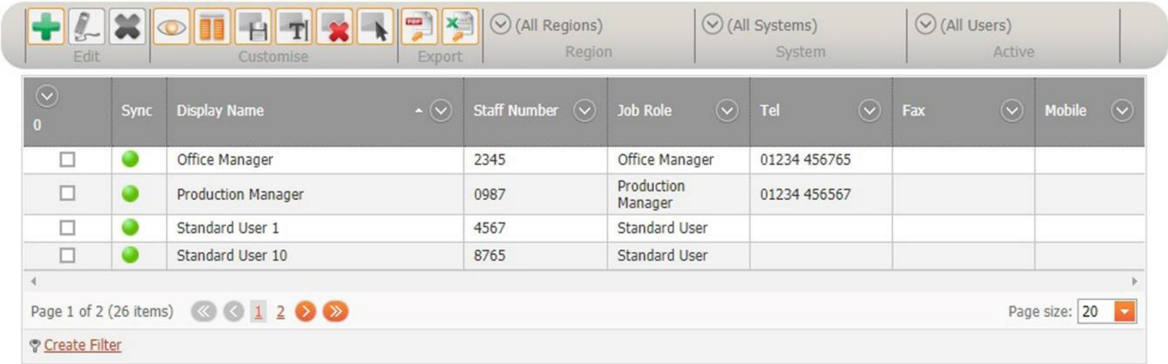
This column shows the current synchronisation status of the user to the currently selected system. There are three main icons that indicate what state the synchronisation is in. A green LED indicates that the user is fully synchronised with all Traka Touch systems they should be. A red LED indicates a sync failure, check that the system is switched on and can communicate with TrakaWEB. Lastly, a rotating loading graphic shows that TrakaWEB is attempting to synchronise the user with the Traka Touch System.

Show/Hide Grid Columns

Throughout TrakaWEB, there are many grids that display important information for the page you are currently viewing. For example, the user list will automatically display the default user fields e.g., staff position, telephone number, fax number etc. The Show/Hide Grid Columns button allows you to add or remove fields/columns of your choice to the grid. Every grid is different and will provide different fields to add to the grid. The user list will allow you to add any or all of the eleven user detail fields.

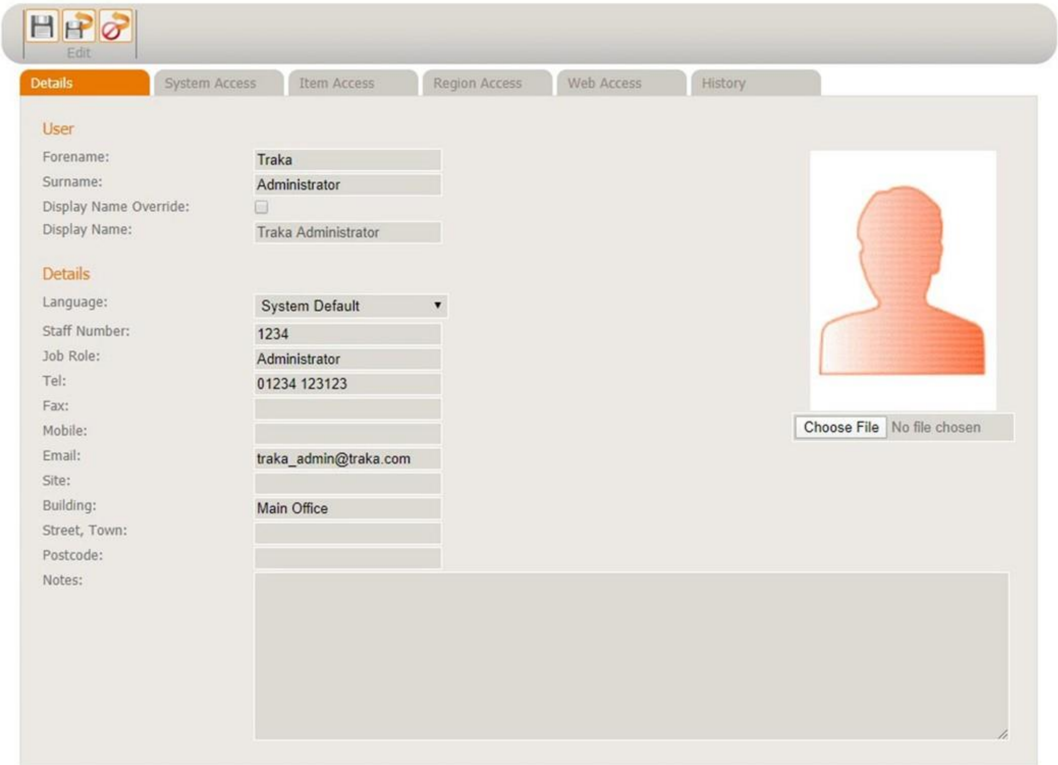
4.3.2 USER DETAILS

The user details window allows you to add and edit user details. From the ribbon toolbar, select the user's icon. If you have already got users set up in your Traka Touch system, then this list will already be populated with all those users.



Details

Here you enter general information about the user such as name, mobile number, language etc.



Forename & Surname
Enter the name of the user. It is essential that these fields be completed.

Display Name Override
If this option is enabled, then you can add/change how the user's name is displayed on screen at the Traka Touch. E.g., if the Forename & Surname fields have your full name 'Duncan Winner', you could enable Display Name Override and enter 'Duncan Winner - Technical Director'.

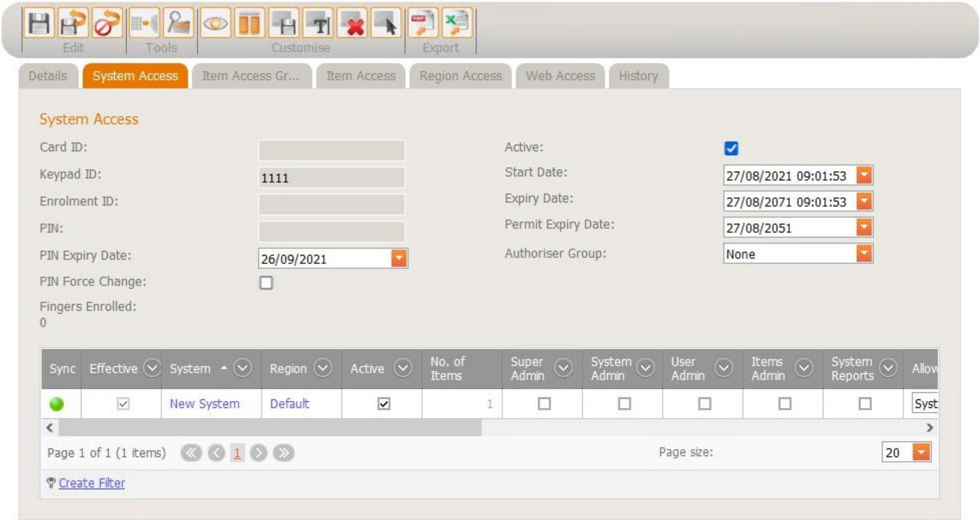
Language
When users identify themselves to the System, the instructions on the touch screen will be displayed in the selected language. If the default language is selected, then the default language of the Traka Touch System will be displayed.

User Details
There are eleven detail fields available to store details about the user. Each field will have a default heading that is assigned when you install TrakaWEB, for example, email. You can change the headings of each field from the User Fields page.

User Picture
Here you can add a picture of the user. Once selected, this image will display next to their name.

System Access

Here you define the systems the user has access to along with other settings such as Keypad/Card ID, PIN expiry date, Authorisation etc.



NOTE: There are two levels of access when using a Traka Touch system: Primary and Secondary. A primary level of access can be one of the following: Card ID, Keypad ID or Fingerprint ID. This means any one of those forms of ID will allow you access to the system. The secondary level of access is an optional PIN (Personal Identification Number). If a user has a PIN, they will be required to enter this at the system following the input of their primary access (Card ID, Keypad ID or Fingerprint).

Card ID
Here you can input your swipe card ID number. Alternatively, you can swipe your card at the reader, click the Read Last Card Swipe button from the Ribbon Toolbar and have TrakaWEB automatically fill in the field for you.

Keypad ID
Here you can input your keypad ID number. This is the primary ID number that will grant the user access to the system.

Enrolment ID
Enrolment ID is used in conjunction with either a Card Reader or the Sagem Fingerprint reader. This feature allows you to set a temporary enrolment number that can be emailed to a user so that when he or she enters this enrolment number at the system they will immediately be prompted to swipe their card or enrol their fingerprint. Clicking the 'Random Enrolment ID' button from the ribbon toolbar will automatically fill this field with a random six-digit number.

NOTE: The user will need to have been setup for email notifications in the Admin App.

PIN
Here you can input your PIN (Personal Identification Number). This is a secondary level of access that can be used in addition to a Keypad ID, Card ID or Fingerprint. E.g., if you have a card ID as your primary level of access, when you log into the system you will be prompted for your PIN after swiping your card.

PIN Expiry Date
This field allows you to enter a date for when the user's PIN will expire. After this date, the user will be required to change their PIN the next time they access the system. If you wish the PIN to forever remain active, leave this area blank.

PIN Force Change
Select this option to force the user to have to change their PIN. If selected, the user will need to change their PIN the next time they access the system.

Fingers Enrolled
Here it will display how many fingers the user currently has enrolled to the system. This is only valid for systems using the Sagem Fingerprint reader.

Active
Tick this selection box on or off to make the user active or not active in all systems and regions.

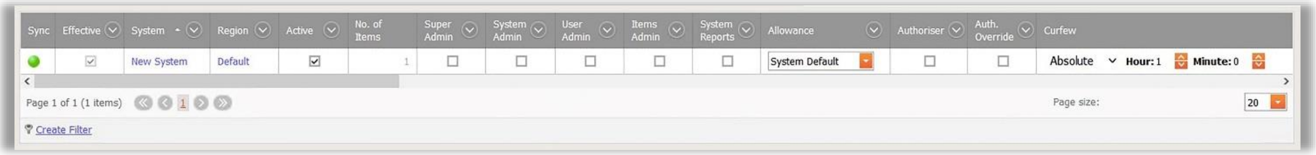
Start & Expiry Date
Select the start & end date and time for the when the user is active.

Permit Expiry Date
Certain users may have licences, certificates or permits that require being kept up to date. Setting an expiry date in this field will show you when the users permit(s) will expire.

Authoriser Group
When using Authorisers, they may be added to different groups depending on authorisation requirement. You may then select from the drop-down menu, the Authoriser Group that you wish to assign the user to.

System Access Grid
The system access grid will display all systems across every region within the database. From here, you can select which systems the user has access to, admin & report permissions etc. These options may be refined by assigning roles to users through software permissions groups. This will in turn reflect the user's roles on Traka Touch. For more information on User Roles for Traka Touch, refer to **UD0011 – Traka Touch User Guide.**

NOTE: The System Access Grid will display different options depending on which feature options are enabled on the system. The example below is typical of a grid with no feature options enabled.



System Access Grid

Effective
Simply select the tick box named Effective to allow the user to access the system.

System
This column will display the name of the system.

Region
This column will display the region to which the system belongs.

Active
Check this box to make the user active and allow them to use the Traka Touch system. E.g. access the system, remove items, run reports etc (anything the user is permitted to do).

No. of Items
This column will show how many items the selected user currently has access to.

Super Admin
The Super Admin role will grant/revoke the user with all the Admin roles regardless of any of them being selected or deselected.

System Admin
The System Admin Role will provide a grant/revoke ability to administer Systems settings, including doors admin if the system is a locker, but will not eanble to ability to edit user records.

User Admin
Selecting this option will provide an Admin role to grant/revoke the ability to edit User records such as adding or removing users or assigning items to users.

Items Admin
Selecting this option will add an Item admin role which will grant/revoke the ability to administer Item records, enabling a user to access items or replace damaged or broken iFobs.

System Reports
Selecting this tick box will allow the user to view & run reports at the Traka Touch system.

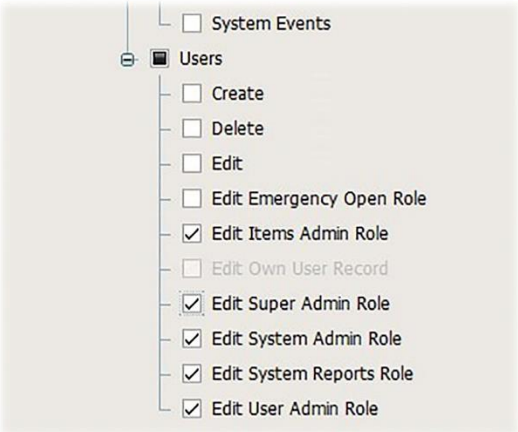
Allowance
Allowance can restrict the total number of iFobs/items users can have out of the system at any one time. Using the drop down selection box, you are able to select a quantity or alternatively, select unlimited for no restriction. The maximum will be however many iFobs/items you have in the selected system.

Authoriser
Selecting this option will enable the user to authorise certain activities such as another user removing items. Please refer to the Authoriser section for more information.

Authorisation Override
Selecting this option will enable an admin user to self-authorise. If an item requires authorisation, a user with this option ticked will bypass the authorisation process.

Curfew
Curfews are used to reduce the amount of time an iFob/item is out of a system, or how long a user can have an iFob/item in their possession. There are two different types of curfew; Relative & Absolute. You can set these curfews against both users and iFobs/items. This is a very useful feature within businesses that have shift patterns and users taking many iFobs/items from various systems, as it will highlight if they are not returned to the system by the end of a users' shift. Please refer to the Curfews section for specific details.

Each of the Admin Roles on the System Access Grid can be enabled or disabled for different users through Software Permissions Groups as shown below.

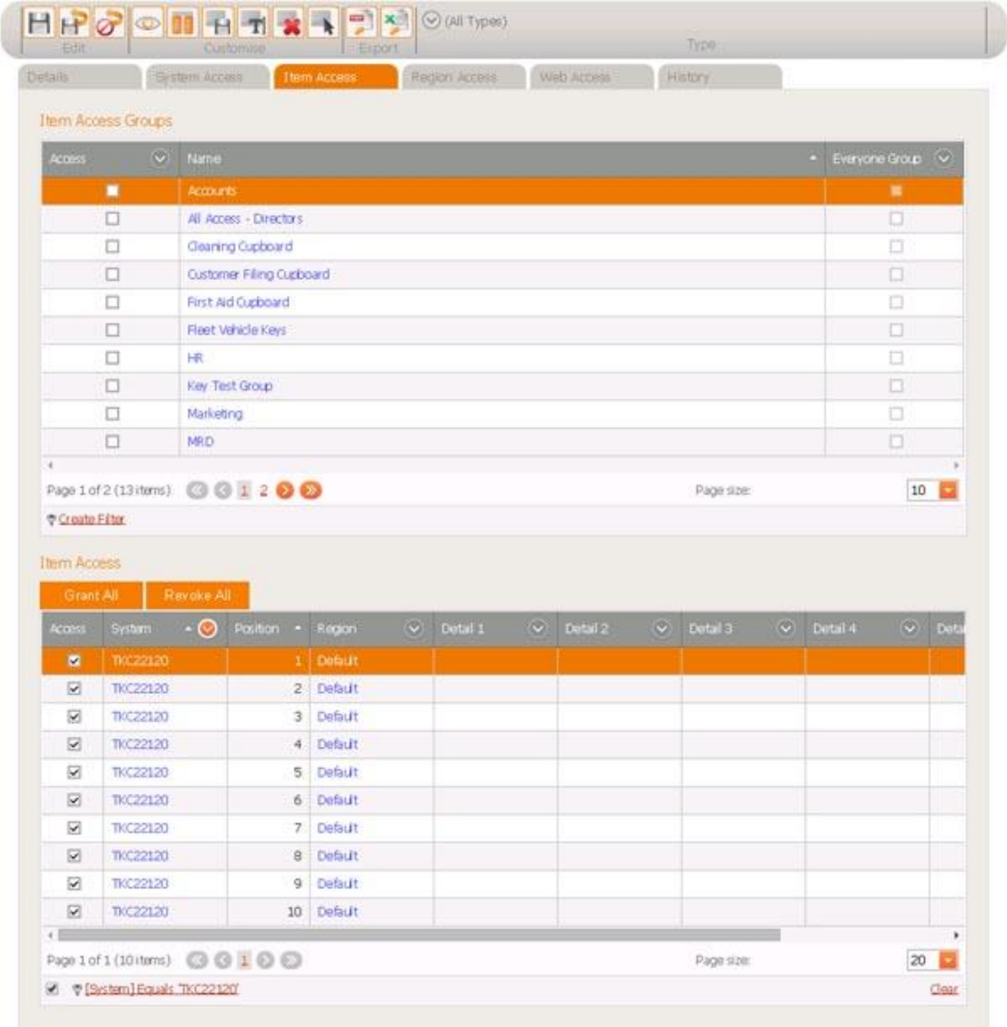


Item Access

Here you can grant/revoke access to items across all systems and regions.

Item Access Groups
You can also grant or revoke access to an entire group of items by using the Item Access Groups section.

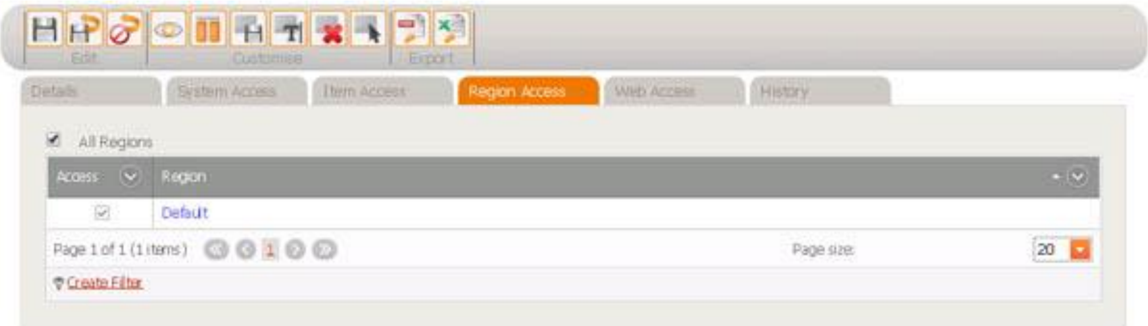
Item Access Grid
Simply checking the Access box next to the desired position will allow the user to remove that item from the system. Selecting the Grant All button will tick all the access boxes allowing the user access to everything. Selecting 'Revoke All' will untick everything removing all access respectively.



NOTE: For more information on Software Item Access Restrictions, refer to the Software Permissions Groups section.

Region

Here you can place the user into a Region. Simply tick the access box on the left of the region you wish the user to belong to.



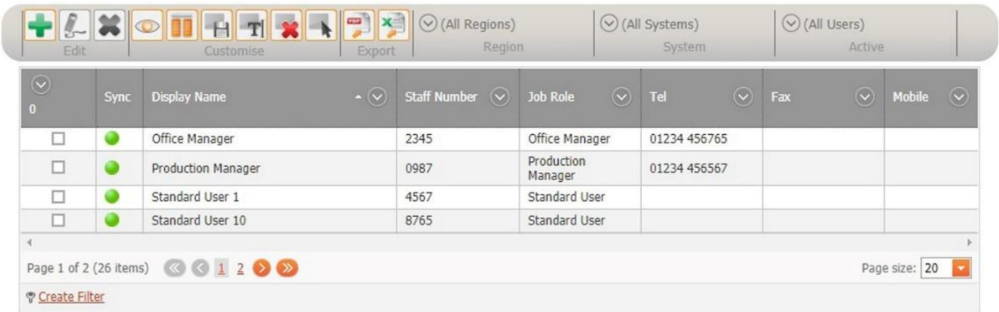
Selecting the **All Regions** tick box will put the user in all regions automatically.

Web Access

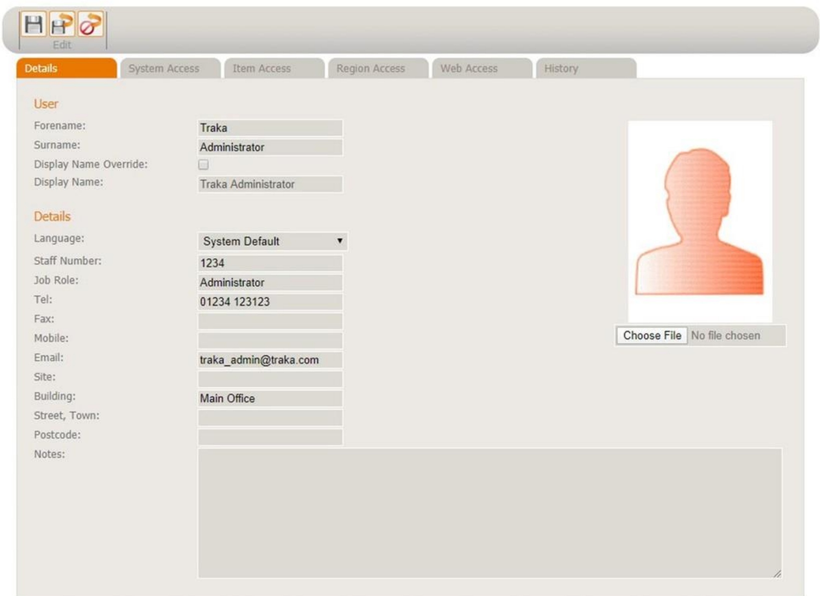
In the Web access tab, a user can be given a separate username and password that will allow them to log into TrakaWEB. It is possible to assign a user to a software access group here as well. For more information on Web Access groups, please see the Groups section.

4.3.3 ADDING USERS

1. From the Navigation Toolbar select the Users icon. If you already have users set up in your Traka Touch system or they have been added here before, then this list will already be populated.



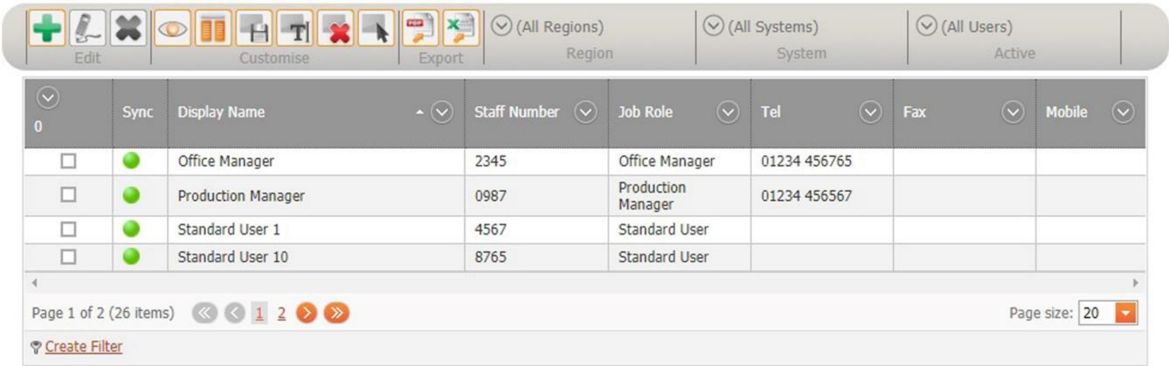
2. To create a new user, click the Add button.



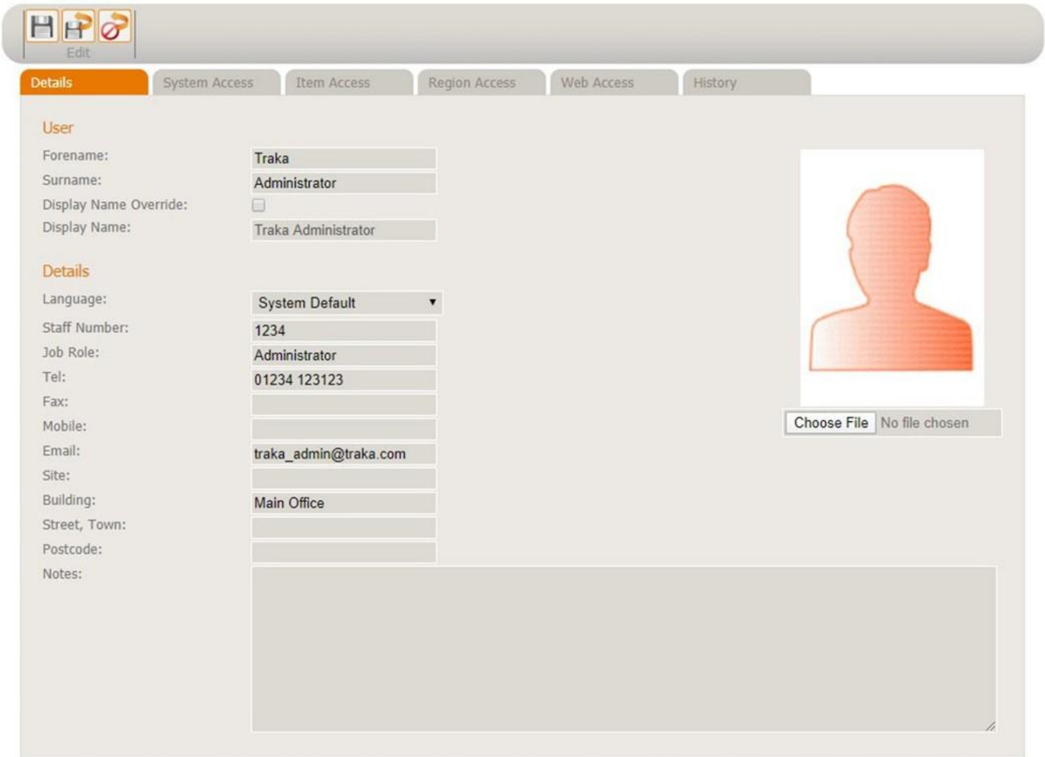
3. The new user record will now open. Input the appropriate details. For more information, please review the User Details section.
4. When you are finished, click the Save & Return button to go back to the user list. To add more users repeat this process from step 2.

4.3.4 EDITING USERS

1. From the ribbon toolbar, click the Users icon. If you already have users set up in your Traka Touch system or they have been added here before, then this list will already be populated.



2. Highlight the desired user and click the Edit button. Alternatively, you can double click the desired user.



3. The selected user record will now open. Edit the appropriate details. For more information, please review the User Details section.

4. When you are finished, click the Save & Return button to go back to the user list. To edit more users, repeat this process from step 2.

NOTE: A User with the edit User Permission will be able to access the History tab to view an audit trail.

4.3.5 DELETING USERS

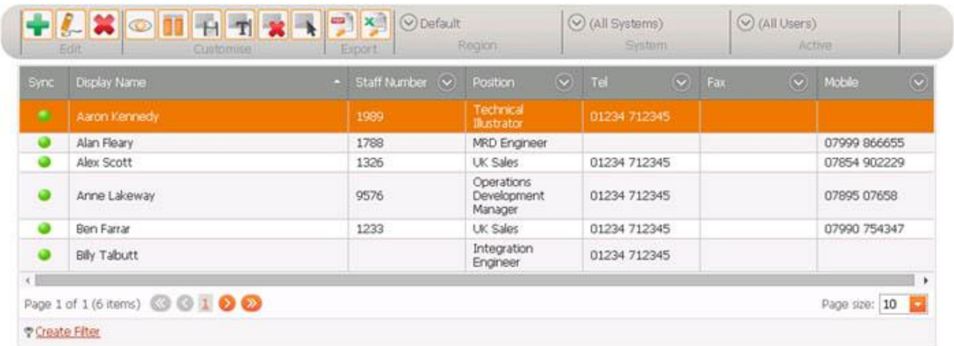
GDPR Statement: To retain the audit history, such as a sequence of activity that has affected a specific operation, procedure or event. It is recommended that the User details are maintained & not fully deleted from the database. With this in mind, the preferred option to remove a User from a Traka system is as follows:

- **Define the user as inactive so that the user cannot use the Traka system(s) any more**
- **Replace the User 'Forename' & 'Surname' with non-specific details such as 'Former employee#1'**

It is also recommended that a backup of the database be made after the above changes are completed & all previous database back-ups destroyed.

This process also maintains compliance with the 'General Data Protection Regulations' (GDPR).

1. From the ribbon toolbar, click the Users icon. If you already have users set up in your Traka Touch system or they have been added here before, then this list will already be populated.



2. Highlight the desired user and click the Delete button.

3. A message window will appear asking you to confirm the deletion of the selected user. Click Delete.

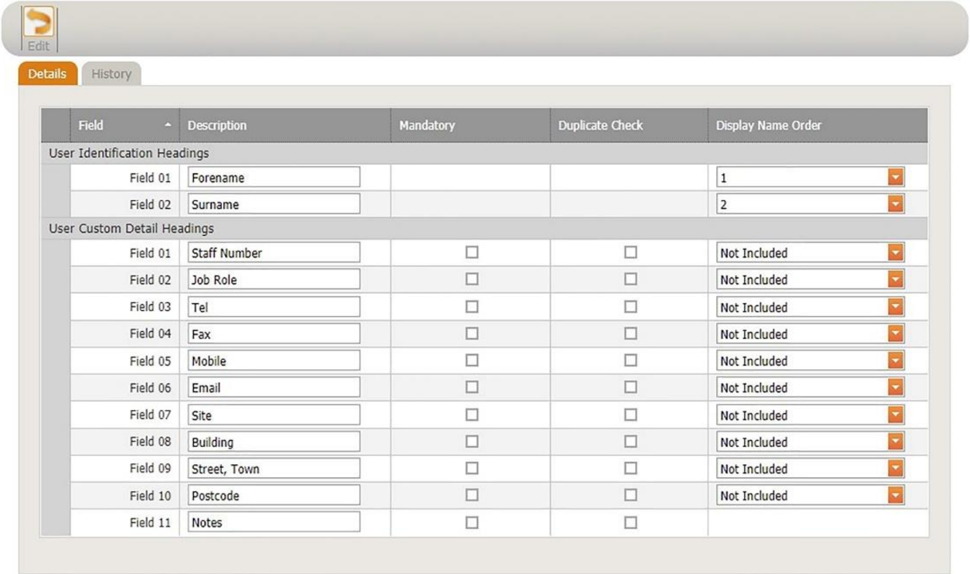
4. The user will now be permanently deleted and disappear from the user list.

4.3.6 USER FIELDS

User Fields are the title headings of the personal credentials in the user details page. Instead of the default staff number, position etc. you can customise them to suit your business requirements.

1. To change these, simply click the Software Settings icon from the Navigation toolbar and select the User Fields button.

2. The User Fields page will then be displayed.



User Identification Headings

Here, you can define the two fields that are by default used for the forename and surname. Simply enter the new text into the corresponding text boxes.

- **Display Name Order**

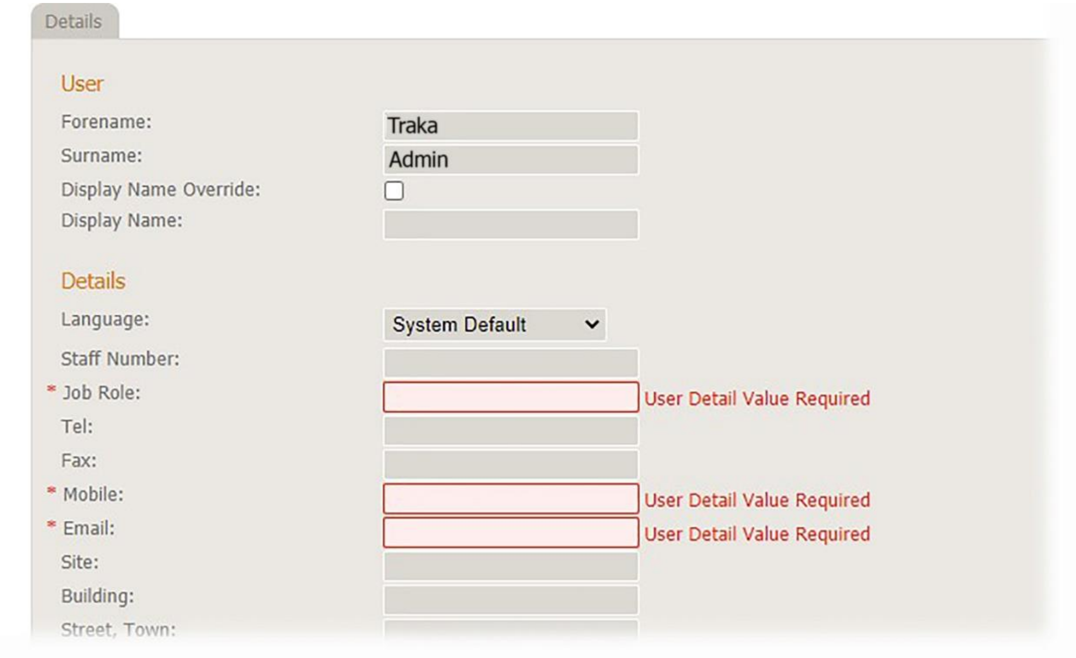
The display name drop-down selection boxes allow you to change which order the fields appear. e.g. If you rearrange forename -2 and surname -1 the Traka Touch will display 'Winner Duncan' instead of the default 'Duncan Winner'.

User Custom Detail Headings

These are the eleven definable fields that appear on the first tab on the user details. Simply enter the new text into the corresponding text boxes.

- **Mandatory Tick Box**

Checking this box will force the logged in TrakaWEB administrator to populate that particular field when creating a new user. E.g. if the mandatory check boxes were selected for the fields 'Job Role', 'Email' and 'Mobile', when the TrakaWEB administrator next creates a new user, they will be forced to enter data into those fields which will be marked by a red asterisk (*) before they are allowed to continue as shown in the example below.



- **Duplicate Check Tick Box**

Checking this box will allow TrakaWEB to search if the identical credentials have been entered against the same field to another user before the details are saved. E.g. if the duplicate check box was ticked for the field 'Mobile' and a TrakaWEB administrator is creating a new user and attempts to enter a mobile number that is already assigned to another user, TrakaWEB will inform you and will not allow you to continue.

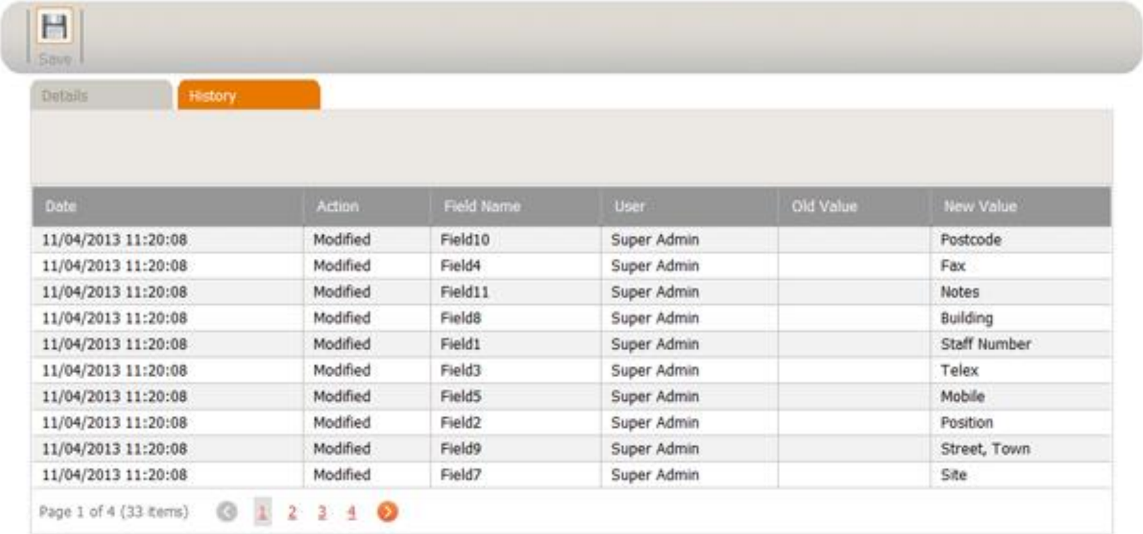
- **Display Name Order**

The display name drop-down selection boxes allow you to change which order the fields appear. E.g. if you rearrange forename -2 and surname -1 and mobile -3 the Traka Touch will read 'Winner Duncan 07896852148' instead of the default 'Duncan Winner'.

3. Once you have selected the desired options, click the Return button to go back or click the history tab to view past records of changes you have made to each field.

History Tab

This tab keeps a record of all the changes made to each field name and the user who made them. This is useful if you ever want to know what the field titles used to be.

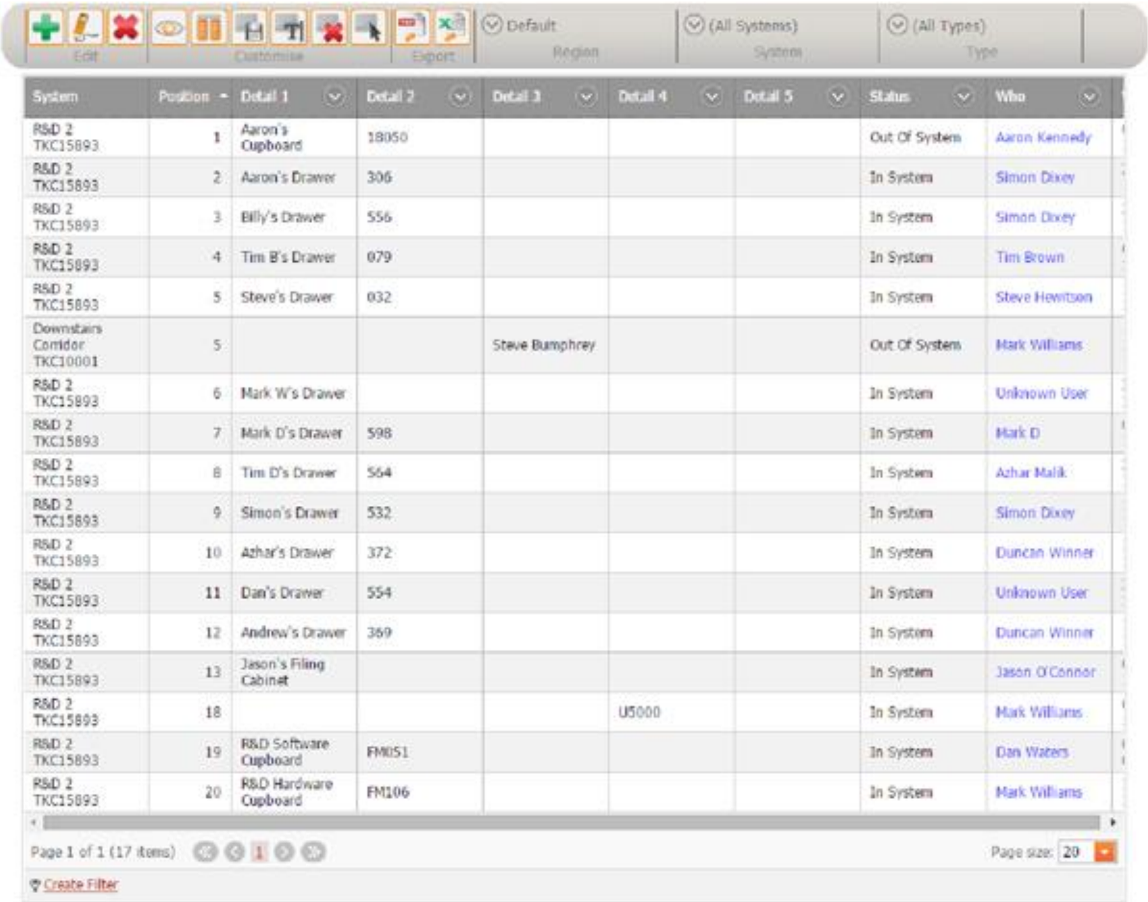


Date	Action	Field Name	User	Old Value	New Value
11/04/2013 11:20:08	Modified	Field10	Super Admin		Postcode
11/04/2013 11:20:08	Modified	Field4	Super Admin		Fax
11/04/2013 11:20:08	Modified	Field11	Super Admin		Notes
11/04/2013 11:20:08	Modified	Field8	Super Admin		Building
11/04/2013 11:20:08	Modified	Field1	Super Admin		Staff Number
11/04/2013 11:20:08	Modified	Field3	Super Admin		Telex
11/04/2013 11:20:08	Modified	Field5	Super Admin		Mobile
11/04/2013 11:20:08	Modified	Field2	Super Admin		Position
11/04/2013 11:20:08	Modified	Field9	Super Admin		Street, Town
11/04/2013 11:20:08	Modified	Field7	Super Admin		Site

4.4 ITEMS

4.4.1 ITEM LIST

From the Navigation Toolbar, click the Items icon. You will then be taken to the Items list. All the items in your Traka Touch system will automatically synchronise when you log into TrakaWEB (providing you enabled communications from your Traka Touch system).



System	Position	Detail 1	Detail 2	Detail 3	Detail 4	Detail 5	Status	Who
R&D 2 TKC15893	1	Aaron's Cupboard	18050				Out Of System	Aaron Kennedy
R&D 2 TKC15893	2	Aaron's Drawer	306				In System	Simon Dixey
R&D 2 TKC15893	3	Billy's Drawer	556				In System	Simon Dixey
R&D 2 TKC15893	4	Tim B's Drawer	079				In System	Tim Brown
R&D 2 TKC15893	5	Steve's Drawer	032				In System	Steve Hewitson
Downstairs Corridor TKC10001	5			Steve Bumphrey			Out Of System	Mark Williams
R&D 2 TKC15893	6	Mark W's Drawer					In System	Unknown User
R&D 2 TKC15893	7	Mark D's Drawer	598				In System	Mark D
R&D 2 TKC15893	8	Tim D's Drawer	564				In System	Azhar Malik
R&D 2 TKC15893	9	Simon's Drawer	532				In System	Simon Dixey
R&D 2 TKC15893	10	Azhar's Drawer	372				In System	Duncan Winner
R&D 2 TKC15893	11	Dan's Drawer	554				In System	Unknown User
R&D 2 TKC15893	12	Andrew's Drawer	369				In System	Duncan Winner
R&D 2 TKC15893	13	Jason's Filing Cabinet					In System	Jason O'Connor
R&D 2 TKC15893	18				U5000		In System	Mark Williams
R&D 2 TKC15893	19	R&D Software Cupboard	FM051				In System	Dan Waters
R&D 2 TKC15893	20	R&D Hardware Cupboard	FM106				In System	Mark Williams

Page 1 of 1 (17 items) 1 Page size: 20

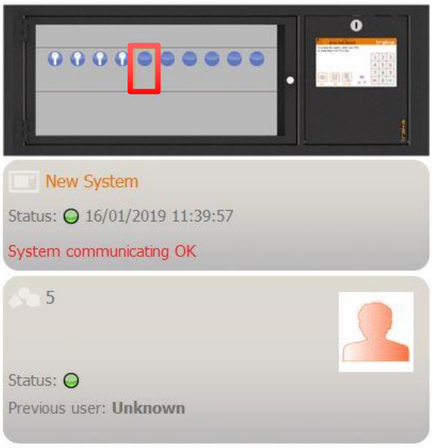
Create Filter

The list shows all the items that are currently in your Traka Touch system, their current status & various definable detail columns. The list that is displayed will depend on the Region, System & Item Type filters that are currently selected on the Ribbon Toolbar. To view only items that are from a specific region/system or are of a specific type, you must select the appropriate filter.

4.4.2 ADDING A NEW ITEM

Adding a new item to the system can be achieved in two ways. You can either:

1. From the System Viewer, select the position for the new Item.



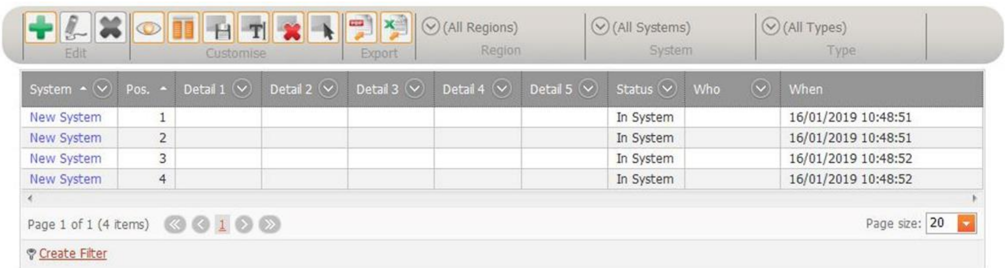
2. From the Ribbon toolbar, select the **Edit Items**  button.

You will now be taken to the **New Item** page.

Or:

3. From the Navigation Toolbar, select Items.

You will now be taken to the Items page, showing a list of all the items currently in the system.



System	Pos.	Detail 1	Detail 2	Detail 3	Detail 4	Detail 5	Status	Who	When
New System	1						In System		16/01/2019 10:48:51
New System	2						In System		16/01/2019 10:48:51
New System	3						In System		16/01/2019 10:48:52
New System	4						In System		16/01/2019 10:48:52

4. From the Ribbon Toolbar, click on the **Add**  button.

You will now be taken to the **New Item** page.

At the **New Item** page, you can enter specific details for the Item in the Details section.

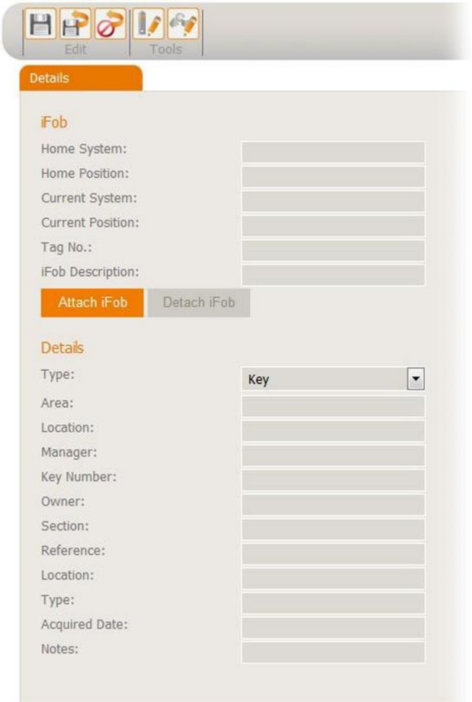
Details

Type

Here you can assign the Item Type e.g. a locker key, car key, door key etc.

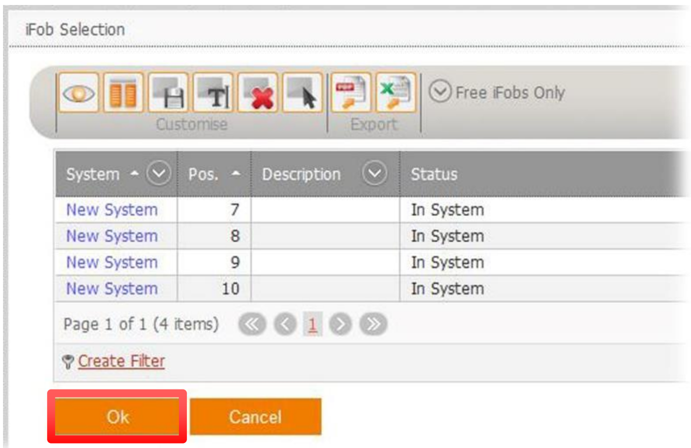
Details Fields

The detail fields that follow will change depending on the selected item type. Please refer to Adding New Item Types or Editing an Item Type for further details. Or alternately you can edit the selected item type by selecting the 'Edit item' button from the ribbon toolbar under tools.



Selecting the **Attach iFob** button from the Details page will direct you to the iFob Selection window. Here, you will see a list of available positions that remain available in the system.

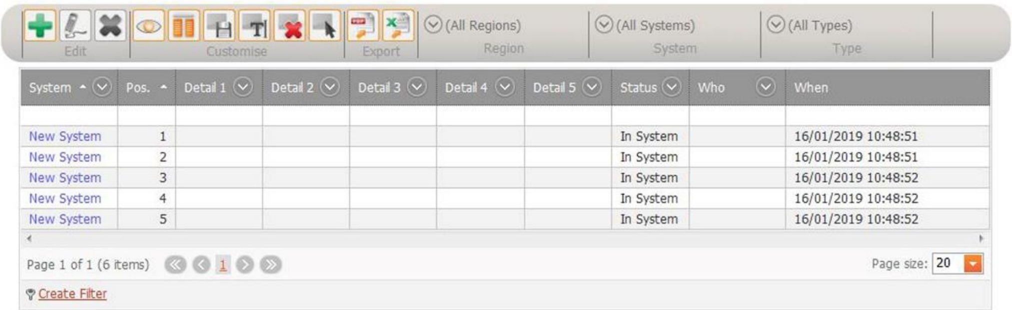
5. Select an available position and then click on **OK.**



You will now be directed back to the Details page.

NOTE: With an item selected, you may also use the 'Detach iFob' button to remove an item from the selected position.

Once completed, click on **Save & Return** from the Ribbon Toolbar. This will take you to the Items list page, showing the newly added Item in the existing list.

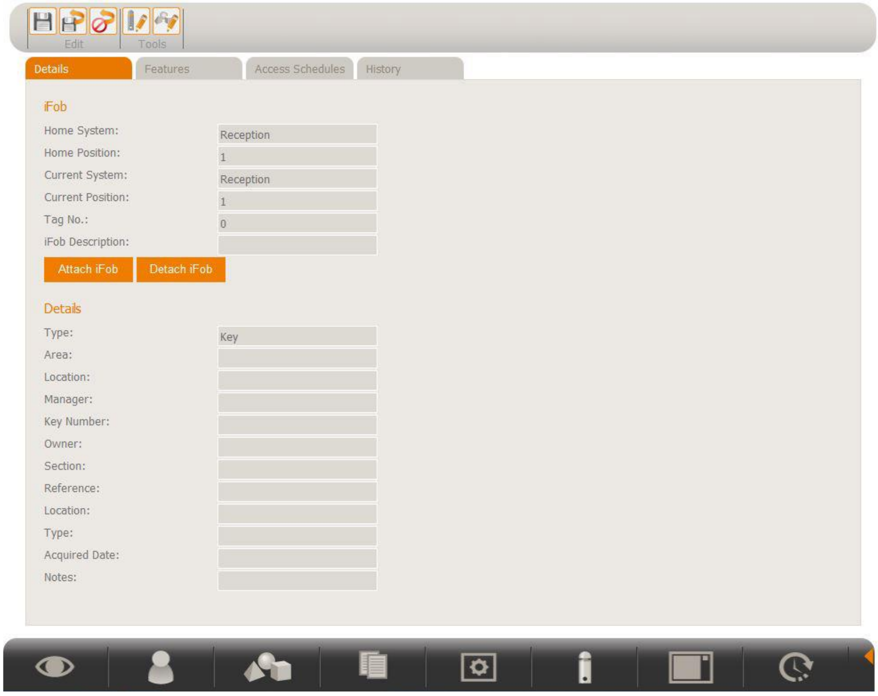


The process can be repeated to add more new items.

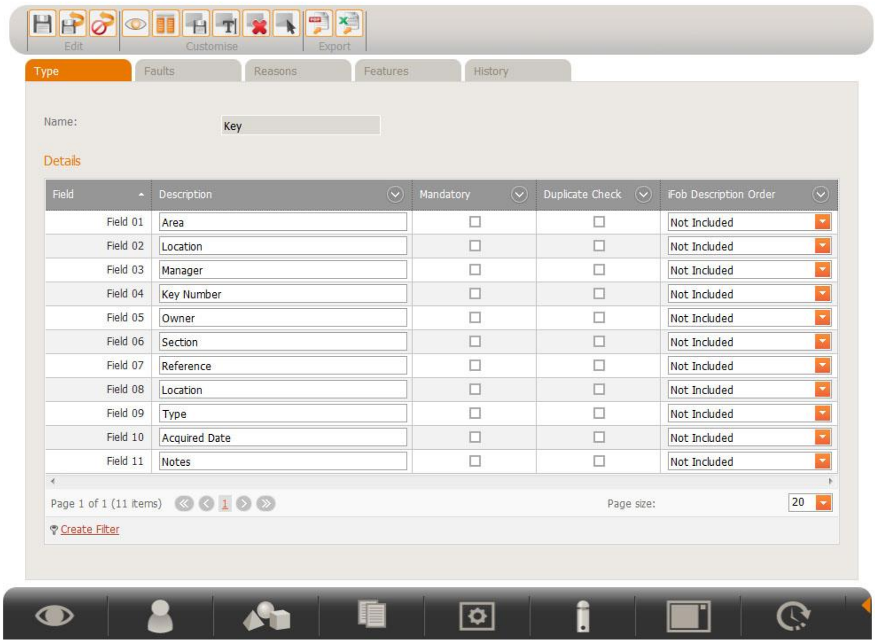
4.4.3 EDITING AN ITEM

1. From the system viewer, highlight an iFob or locker compartment with an item defined and then select the **Edit Items** button from the ribbon toolbar. Alternatively, using the navigation toolbar at the bottom of the screen, click the Item button. From the item list, highlight the desired item and click the Edit button from the ribbon toolbar.

2. If you clicked **Edit Item** from the system viewer page, you will be presented with the Details tab on the New Item details page. You will be able to see the details currently defined for that position. From here, you can edit the system details in the Details section as shown below.

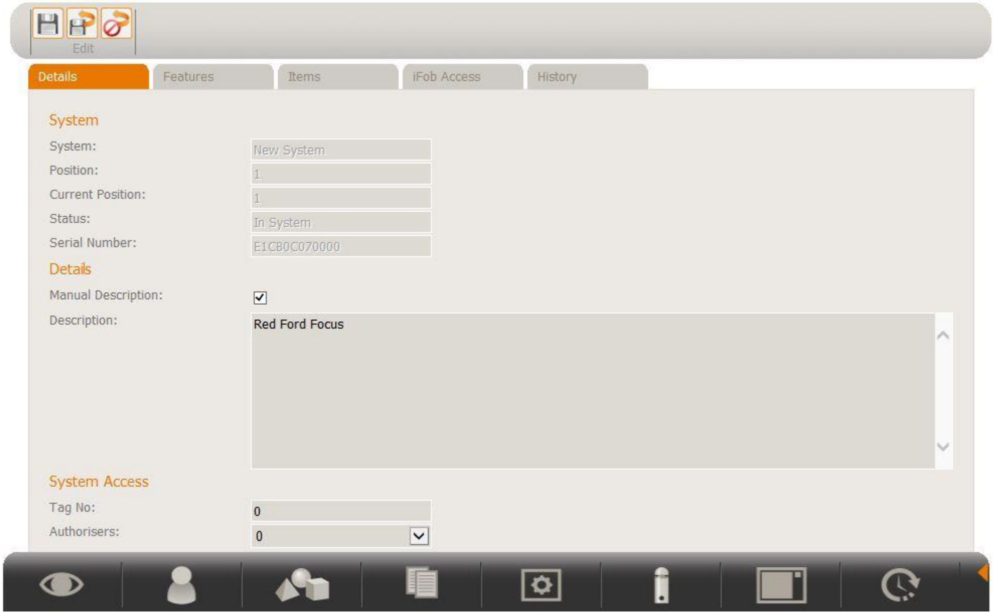


Clicking **Edit Item Type** will take you to the Edit Item Type detail page where you can redefine all the item's details and descriptions.

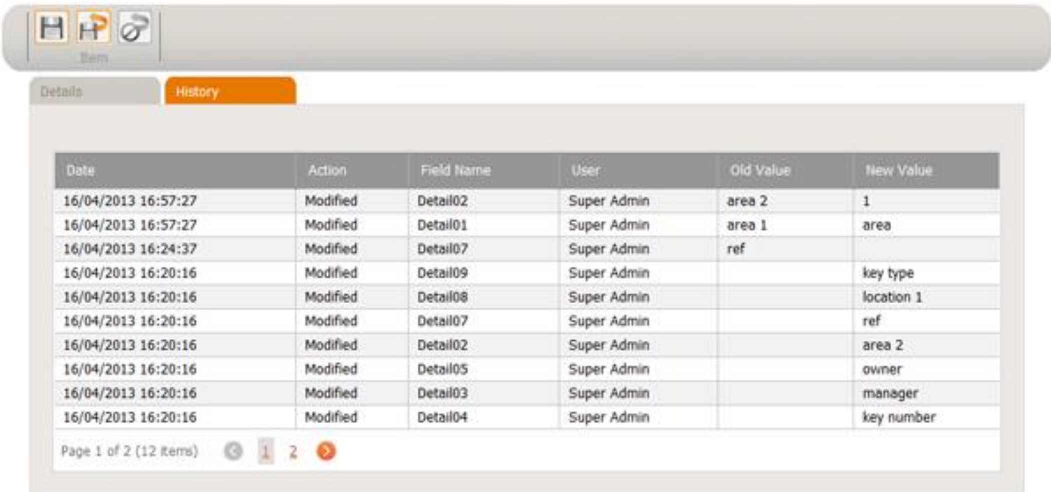


3. If you navigated directly to the Item Page, then you will currently be looking at the Item list. This list will have every item defined for any position in the database. Highlight the item you wish to edit and click the **Edit Item** button. You will then be directed back to the Edit Item page.

As well as being able to Edit Item Type, at the New Item page, you can also select **Edit iFob**. This page enables you to edit the details of an iFob. It also contains the Items tab, which again will allow you to add or edit items. This page also contains the Features tab, iFob access and History tab.



4. The history tab keeps a record of all the changes made to the data in each field and who made the changes. This is useful if you ever want to know what the field details used to be.

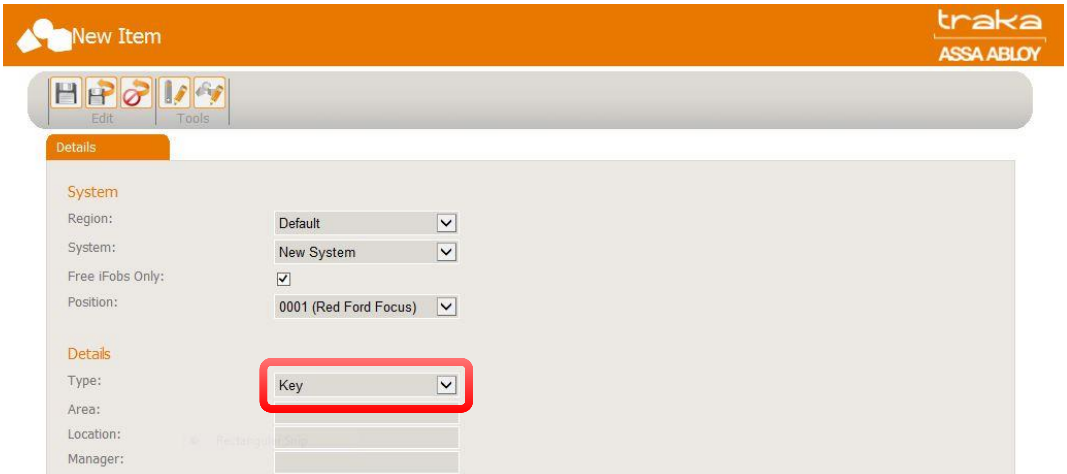


Date	Action	Field Name	User	Old Value	New Value
16/04/2013 16:57:27	Modified	Detail02	Super Admin	area 2	1
16/04/2013 16:57:27	Modified	Detail01	Super Admin	area 1	area
16/04/2013 16:24:37	Modified	Detail07	Super Admin	ref	
16/04/2013 16:20:16	Modified	Detail09	Super Admin		key type
16/04/2013 16:20:16	Modified	Detail08	Super Admin		location 1
16/04/2013 16:20:16	Modified	Detail07	Super Admin		ref
16/04/2013 16:20:16	Modified	Detail02	Super Admin		area 2
16/04/2013 16:20:16	Modified	Detail05	Super Admin		owner
16/04/2013 16:20:16	Modified	Detail03	Super Admin		manager
16/04/2013 16:20:16	Modified	Detail04	Super Admin		key number

Page 1 of 2 (12 items) 1 2

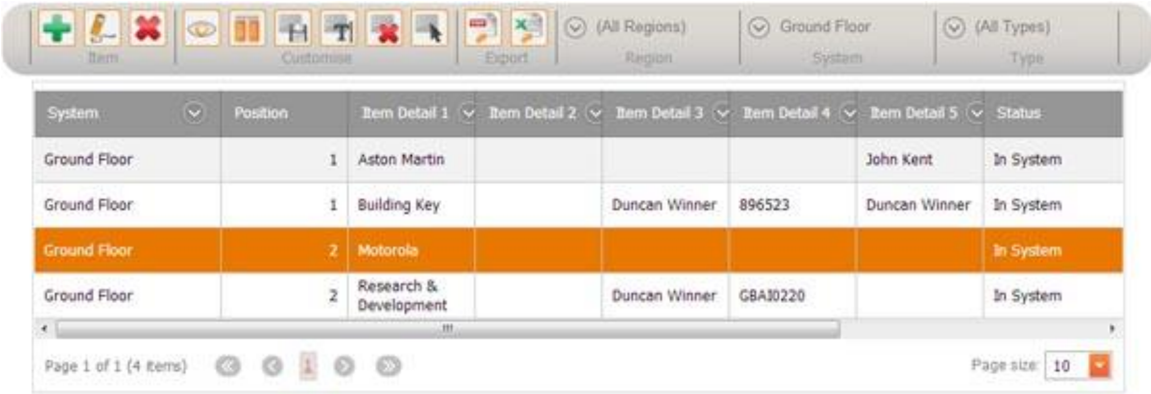
5. When you have completed editing the item, click the Save button or click **Save & Return** to be taken back to the Item List.

If an iFob does not have an item assigned to it and you click **Edit Items**, you will be taken to the 'New Item' page. Here, you can assign a new Item Type, such as a key, to an iFob.

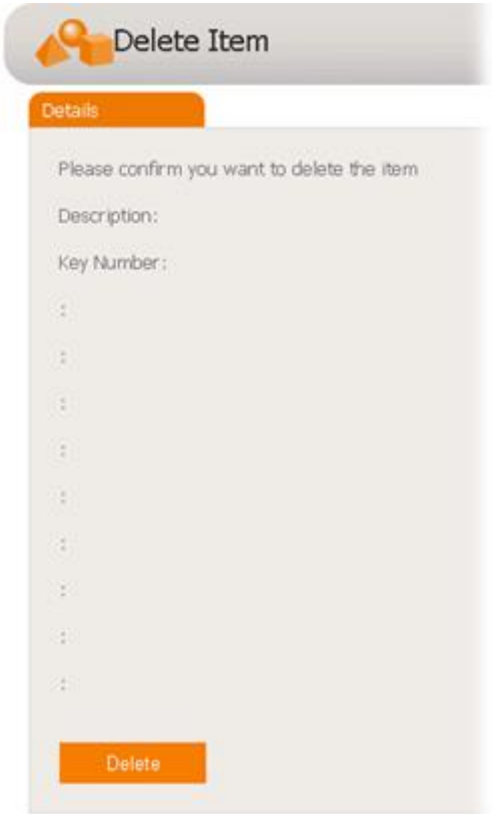


4.4.4 DELETING AN ITEM

1. From the Item List, select the desired item and click the **Delete** button.



2. A window will appear asking for confirmation to delete the item.



3. Once deleted, the item will no longer be in the items list.

4.4.5 ADDING AN ITEM TO AN IFOB

NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' in a Locker System.

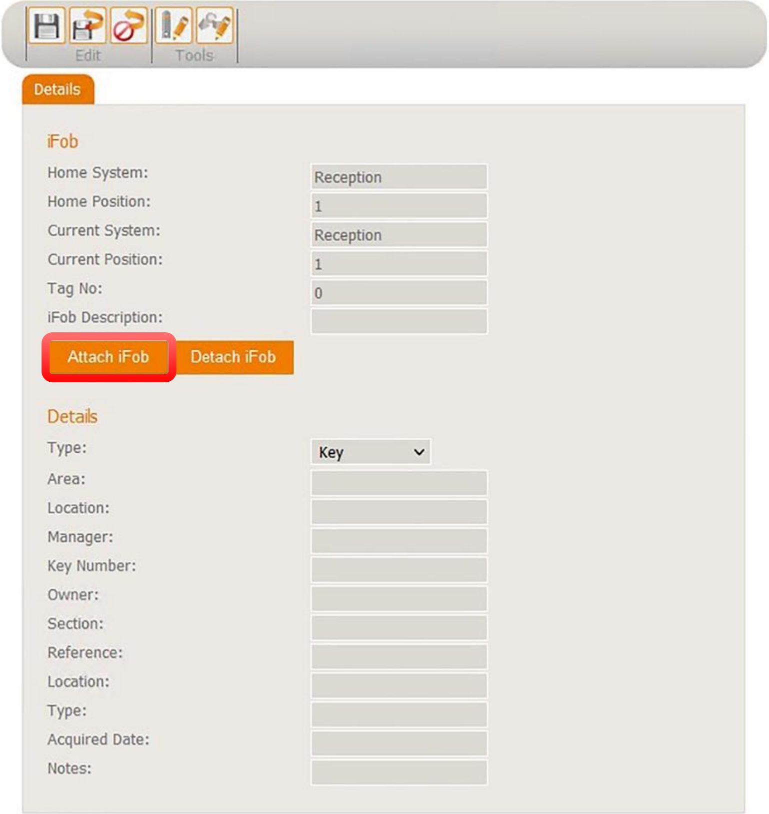
TrakaWEB by default has an item type already created named 'Key'. This item type can be used at any time. TrakaWEB also allows you to create your own item types and assign them to iFobs on the system viewer. Therefore, you could create an item type called Car Keys, and then create twenty car keys that you can then assign to the iFobs.

NOTE: It is possible to add up to 5 Items to a single iFob and they must all be of the same item type.

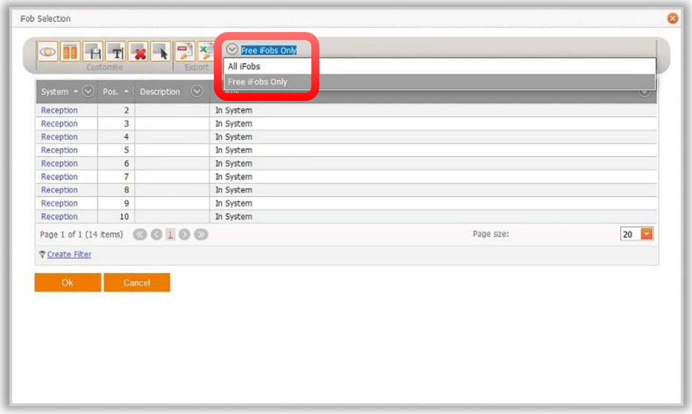
1. From the system viewer, highlight a position that currently does not have an item assigned. Then using the Ribbon Toolbar, select the Edit Item button.

2. You will be presented with the Details page. Here, you can edit the details as required and select the item type from the drop-down menu.

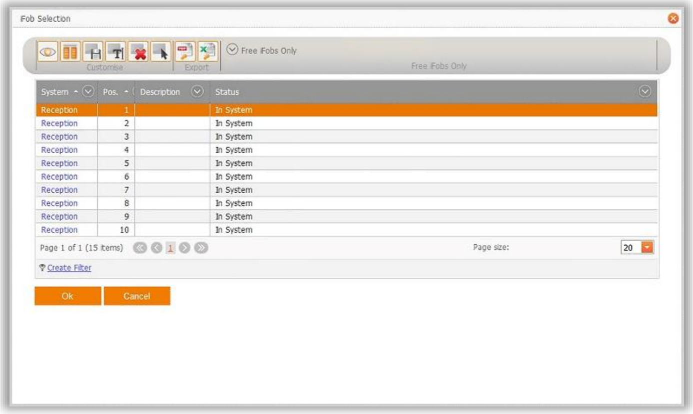
3. Select the Item Type and then select the **Attach iFob** button.



The **iFob Selection** screen will now appear, showing a list of all the iFobs in the system that currently have not been assigned items. From the drop-down menu on the ribbon toolbar, it is possible to view **All iFobs** or **Free iFobs Only.**



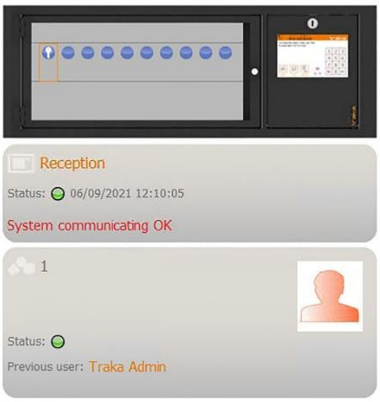
4. Select an iFob that you wish to add the item to.



5. Once you have made your selection, click on **OK** and you will return to the **New Item** page.

6. Click on the **Save** button to complete the process.

   On returning to the System Viewer, you will now see the item has been added to the selected iFob. Repeat the process to add items to the remaining iFobs as required.



NOTE: It is possible to change headings of the detail fields by Editing the Item Type.

After you have entered all the required details click the Save & Return button. This will take you to the items list for the system you are currently viewing. Clicking the Cancel button will return you to the Item Types page without saving the new item details.

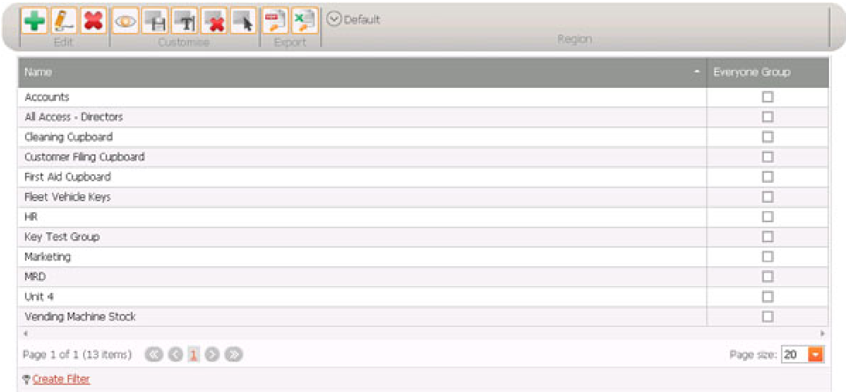
4.4.6 ITEM ACCESS GROUPS

Item Access Groups allow you to restrict users to only being able to access certain items. They are particularly beneficial, as you do not need to give each user individual access to each item/system, which could take some time depending on how large your work force is. Groups work by allowing items (across multiple systems) to be accessed by a group. You can then give users access to the groups they need, therefore allowing the users to remove/return the items they need.

NOTE: For more information on Software Item Access Restrictions, refer to the Software Permissions Groups section.

NOTE: For information on Common Item Access Groups, please refer to Random Return to Multiple Systems.

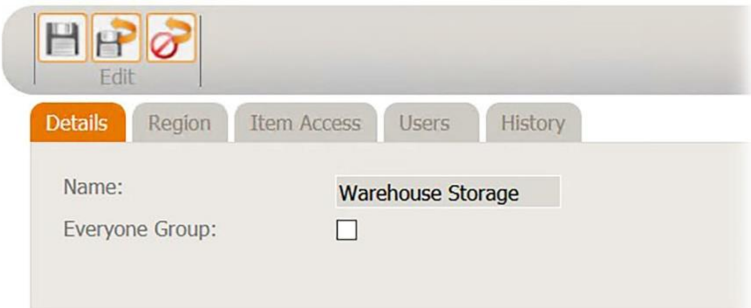
1. Select the Item Access page via the navigation toolbar. The Item Access Group list will then be displayed.



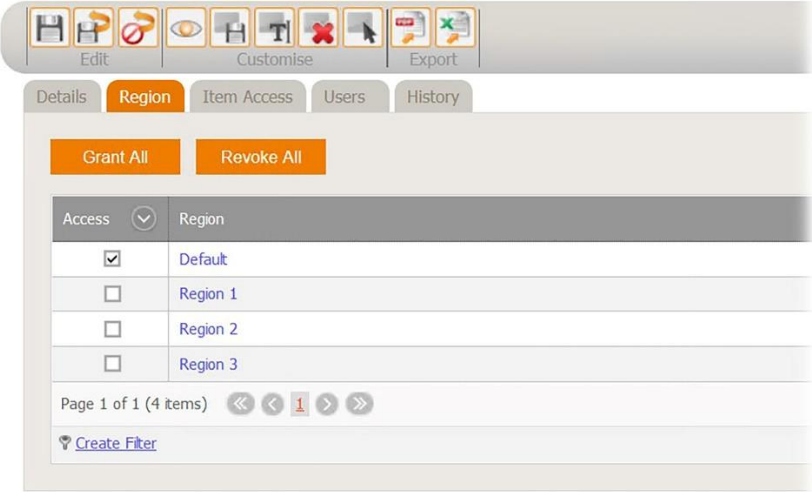
2. Click the Add button.

3. You will then be prompted to enter a group name.

4. Click the Save button to enable the Region, Item Access, Users & History tabs. At this point, you can select the option 'Everyone group'. An ‘Everyone Group’ automatically makes all users a member of the Item Access Group (removing the need to manually add them to the group individually), where the User’s region and Item Access Group’s regions match.

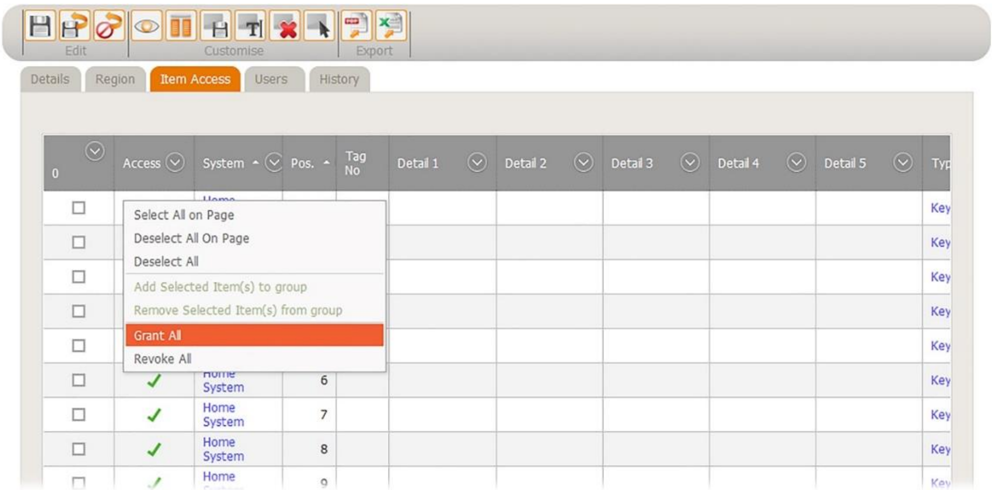


5. Next, select the region or regions you wish to apply to the group.

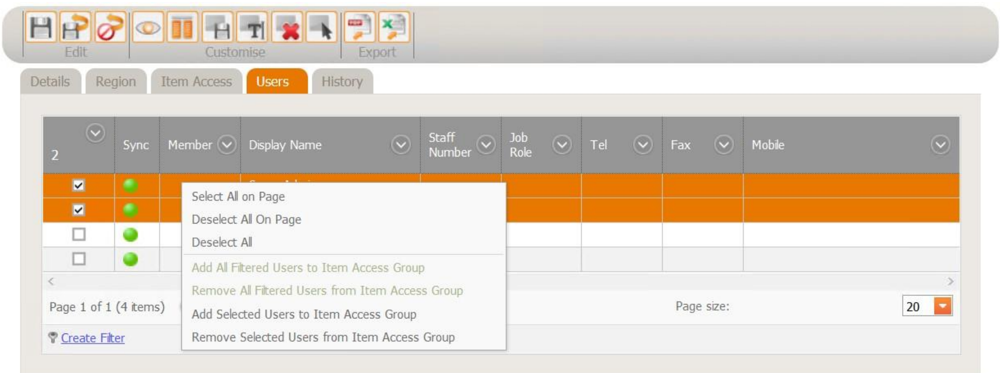


6. The Item Access list will display all the items in the database. The items listed here will depend on what systems are in the region/s you selected on the previous page. Here you can select which items the group will have access to. Simply check the box in the access column for the relevant items. Alternately, you can right click within the grid and select **Grant All** from the context menu.

NOTE: For more information on using the context menu, please refer to the Item Access section within Multi-Select/Multi-Edit.

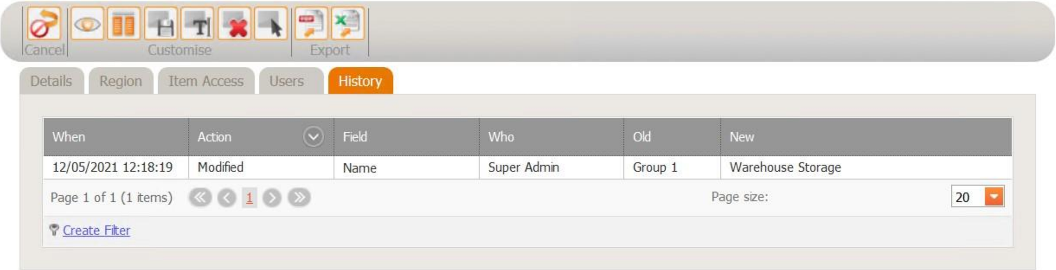


7. The Users tab will display a list of available users. To add users to the group, you can select them individually by left clicking on the checkbox to the left of the user. To add them to the current group, right click and select the option from the context menu.



NOTE: For more information on adding users to Item Access Groups using the context menu, please refer to the Item Access section within Multi Select/Multi Edit.

8. Once you have finished, click the **Save and Return** button or select the History tab. The history will show you a record of when the group was added, who by, what the name is and if it has been changed.



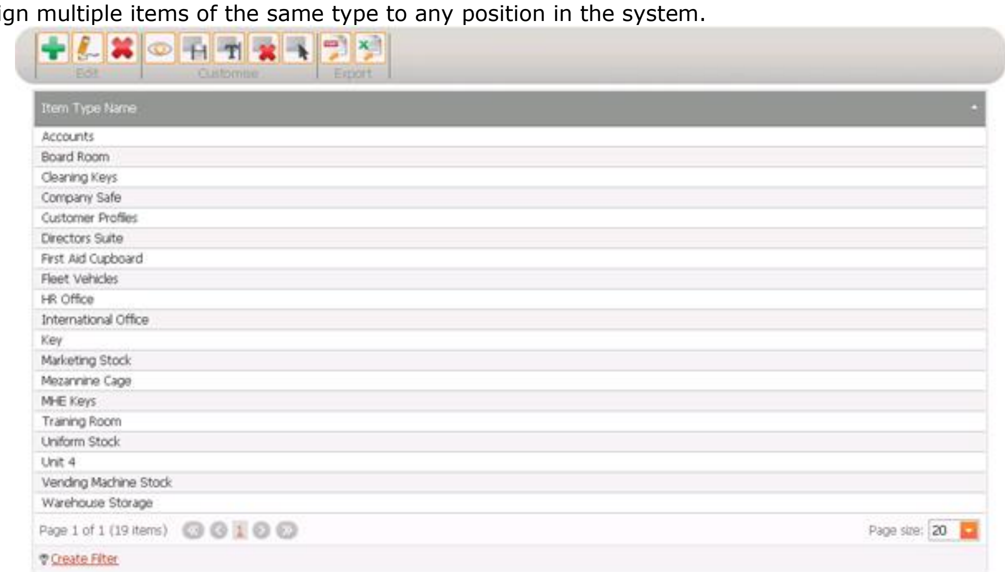
4.4.7 ITEM TYPES

In TrakaWEB, you can create your own item types that you can later assign to positions. This is useful as you may for example, have many different types of 'key' instead of one generic term to fit many types, e.g. Car Keys, Door Keys, and Building Keys etc. Alternatively, in a locker system for example you may have Radio, Laptop, and Mobile Phone etc.

1. Select Software Settings from the Navigation Toolbar and from there, click the Item Types button.

This will take you to the Item Types list where all the existing items are displayed. By default, TrakaWEB has a standard item type called 'Key' ready to be used. From here, you can add, edit and delete item types along with using the search tool to find specific items and finally exporting the item data to an Excel Spreadsheet or PDF document.

You can assign multiple items of the same type to any position in the system.

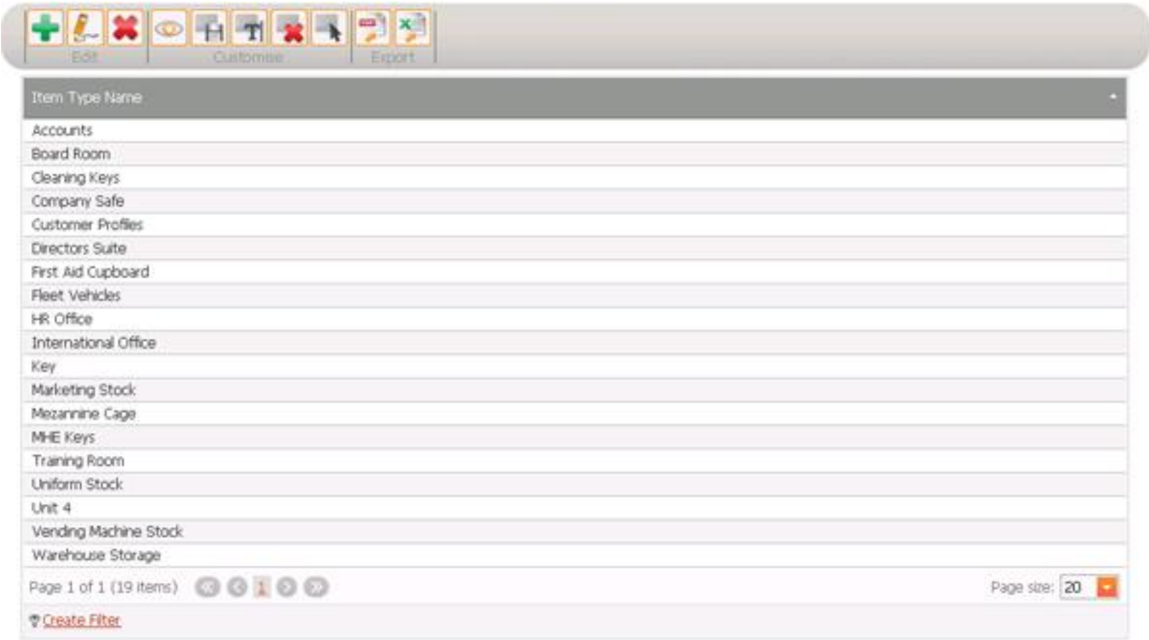


Please follow the links below for more information on adding, editing, deleting, searching & exporting.

4.4.7.1 ADDING NEW ITEM TYPES

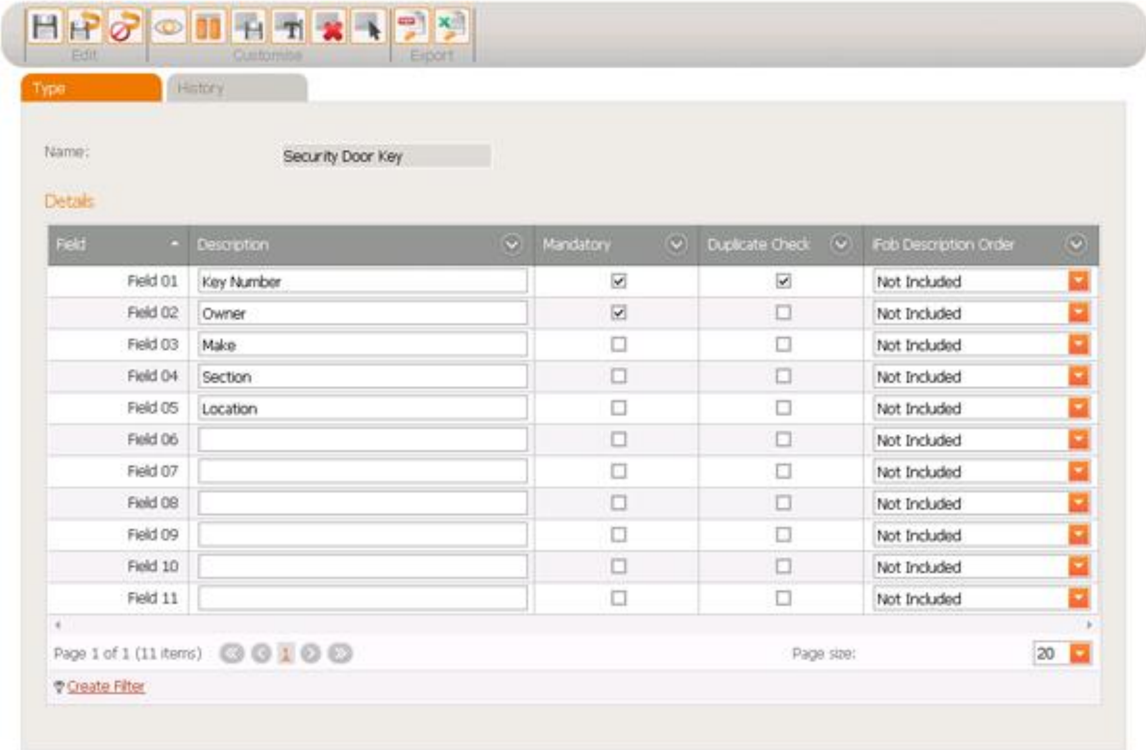
To create a new Item Type, you must click Software Settings and select the Item Type icon from the Navigation Toolbar.

1. The current item type list will then be displayed. If you have never added an Item Type before then you will see the TrakaWEB default item type 'Key'. To add another type, click the Add button.



2. The Item Type page will now appear. Here you can specify a name for the item type.

3. Click the save button. You will then be taken to the details page. Here you can enter the information that relates to the item type.



Description

There are eleven fields that you can enter details about the new item type e.g. if it is a key, you may want to add a description such as make, owner or model etc.

Mandatory Tick Box

Checking this box for will force the logged in TrakaWEB administrator to populate that particular field when adding this item to a position. E.g. if the mandatory check box was selected for the field 'Key Number', when the TrakaWEB administrator next creates a new item from this item type they will be forced to enter data into the 'Key Number' field before they are allowed to continue.

Duplicate Check Tick Box

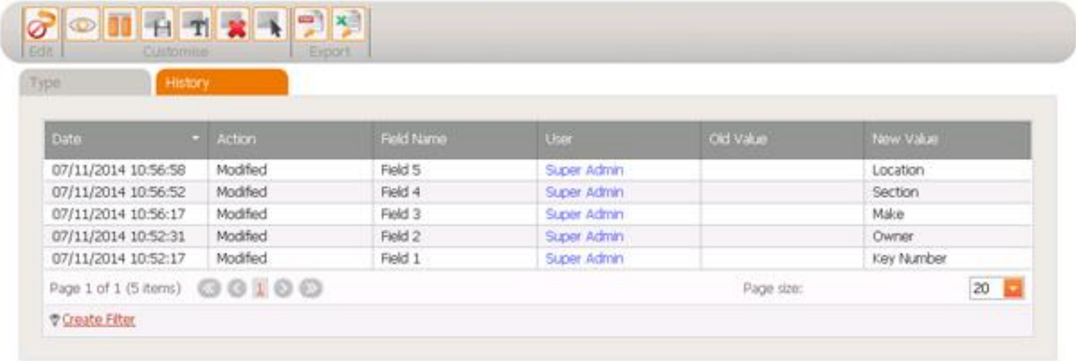
Checking this box will allow TrakaWEB to search if the identical credentials have been entered against the same field to another item before the details are saved. E.g. if the duplicate check box was ticked for the field 'Key Number' and a TrakaWEB administrator is creating a new item and attempts to enter a number that is already assigned to another item, TrakaWEB will inform you and will not allow you to continue.

iFob Description Order

You can select which fields you want as the iFob descriptions (if any). Simply use the drop down selection boxes and set them in numerical order.

4. Once you have selected the desired options, click the Save & Return button to go back to the previous page or click the history tab to view past records of changes you have made to each field.

History Tab
This tab keeps a record of all the changes made to each field name and the user who made them. This is useful if you ever want to know what the field titles used to be.



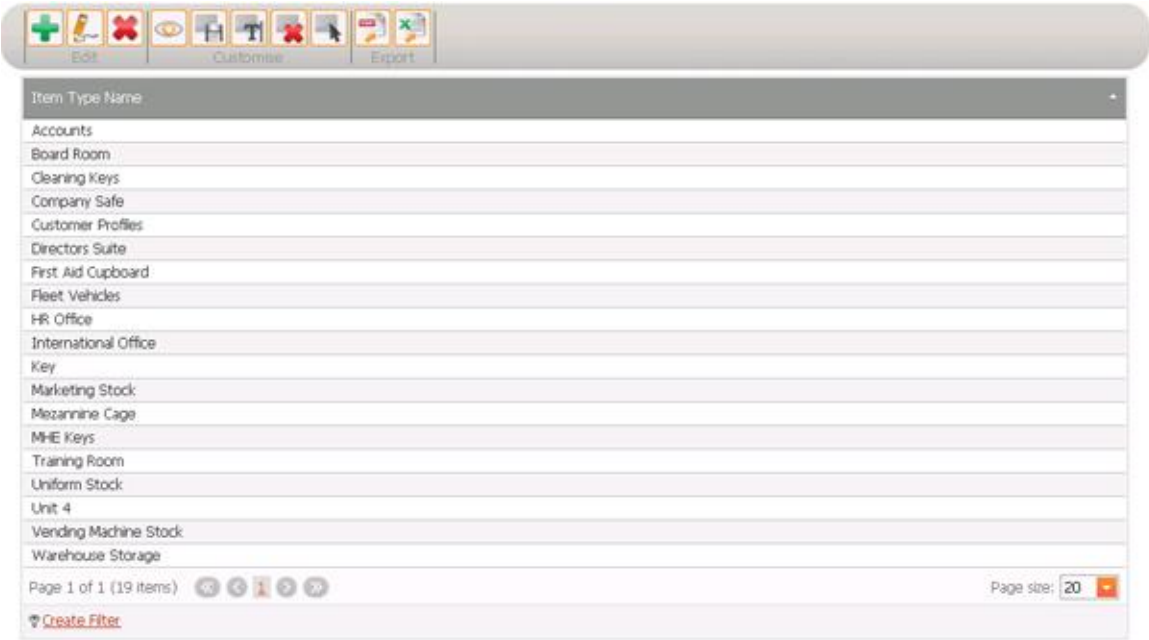
Date	Action	Field Name	User	Old Value	New Value
07/11/2014 10:56:58	Modified	Field 5	Super Admin		Location
07/11/2014 10:56:52	Modified	Field 4	Super Admin		Section
07/11/2014 10:56:17	Modified	Field 3	Super Admin		Make
07/11/2014 10:52:31	Modified	Field 2	Super Admin		Owner
07/11/2014 10:52:17	Modified	Field 1	Super Admin		Key Number

Now complete, you can now navigate to the Items section via the Navigation Toolbar and begin to create as many items of that item type that you require. Please see the Adding an Item to an iFob topic for more details.

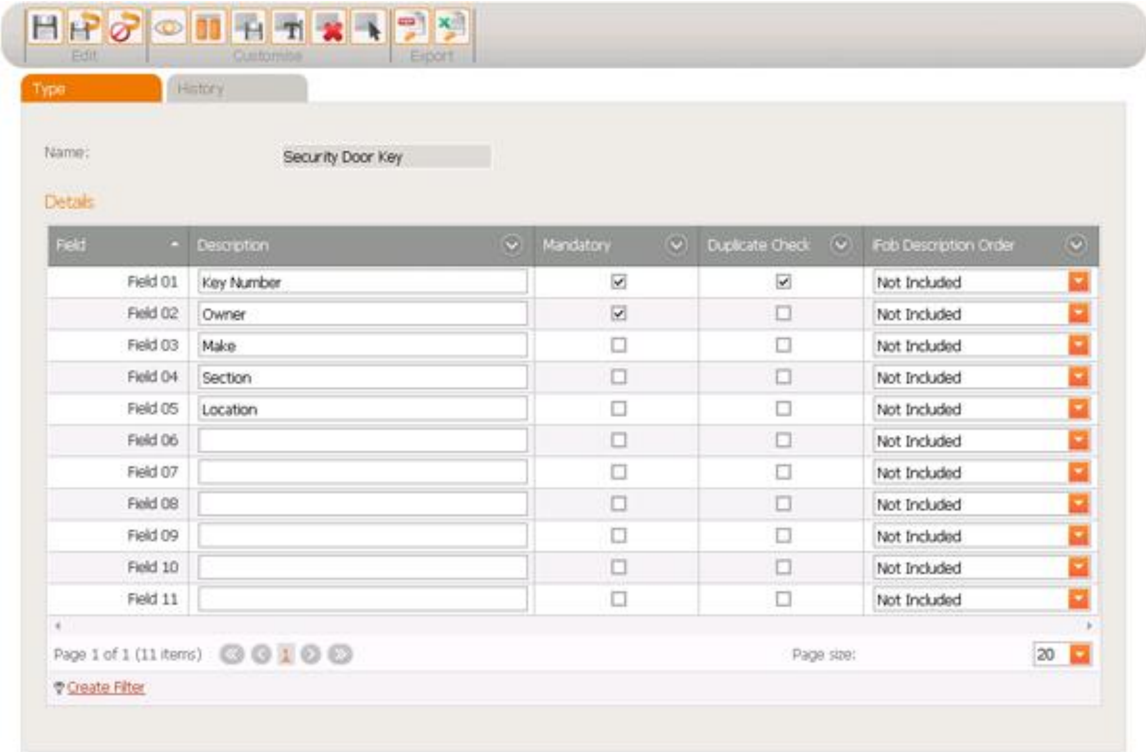
4.4.7.2 EDITING ITEM TYPES

1. Select Software Settings from the Navigation Toolbar and from there, click the Item Types button.

2. Once the Item list appears, highlight the desired item and select the edit button. In this example, Security Door Key has been selected.



3. The Item details page will now appear. Here you can change the name of the item itself and the eleven definable fields that relate to the Item Type.



4.5 REPORTS

4.5.1 REPORTS OVERVIEW

Reports are a compilation of information or activities that have occurred at the system. There are eight standard categories of reports within TrakaWEB; each category has one or more reports to generate. Please use the links below to view the appropriate report category.

General Reports

Status Reports

Exceptions Reports

Permissions Reports

Reason Reports

Regions Reports

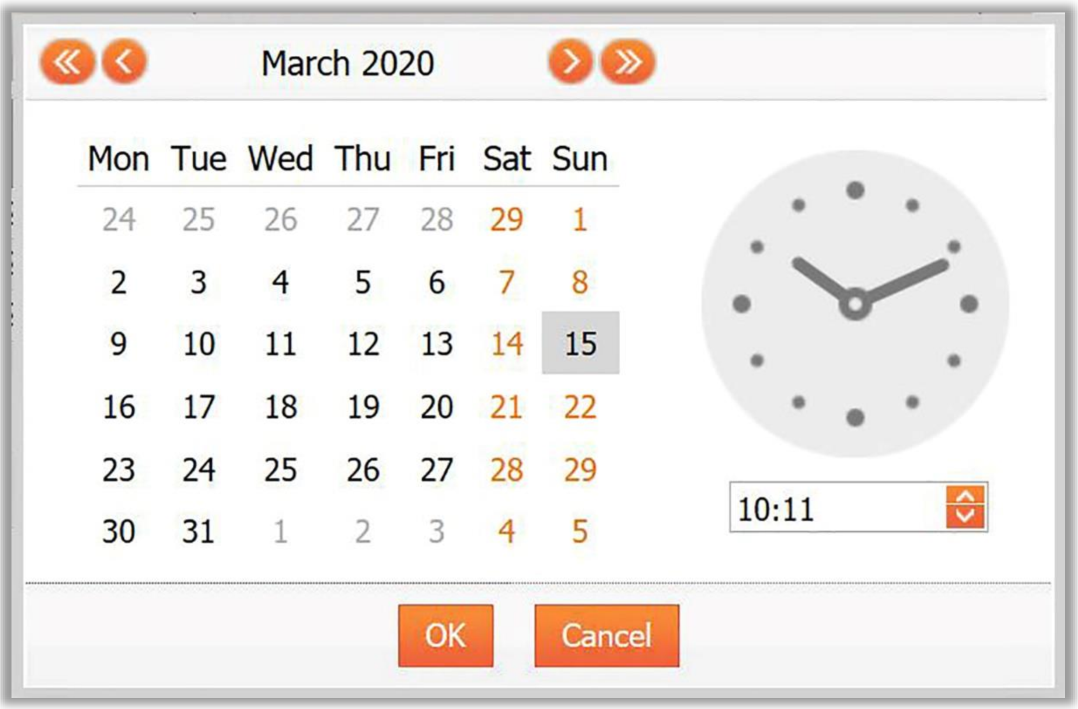
Utilisation Reports

Diagnostics Reports

NOTE: Only Optional Features that have been enabled will be displayed in the reports screen. For information regarding Cost Option reports, please refer to the Feature Options section.

NOTE: Before submitting a report, ensure that the required language has been specified otherwise the report may not display correctly due to different date formats i.e., DD/MM/YYYY or MM/DD/YYYY.

Most of the reports in TrakaWEB use a start and end date to filter search results. Clicking the arrow next to start time/end time will show a small calendar allowing you to select specific times from which you wish the report to retrieve data.



4.5.2 GENERAL REPORTS

The General Reports comprises of 2 report categories:

- Activity Report
- Central History Report

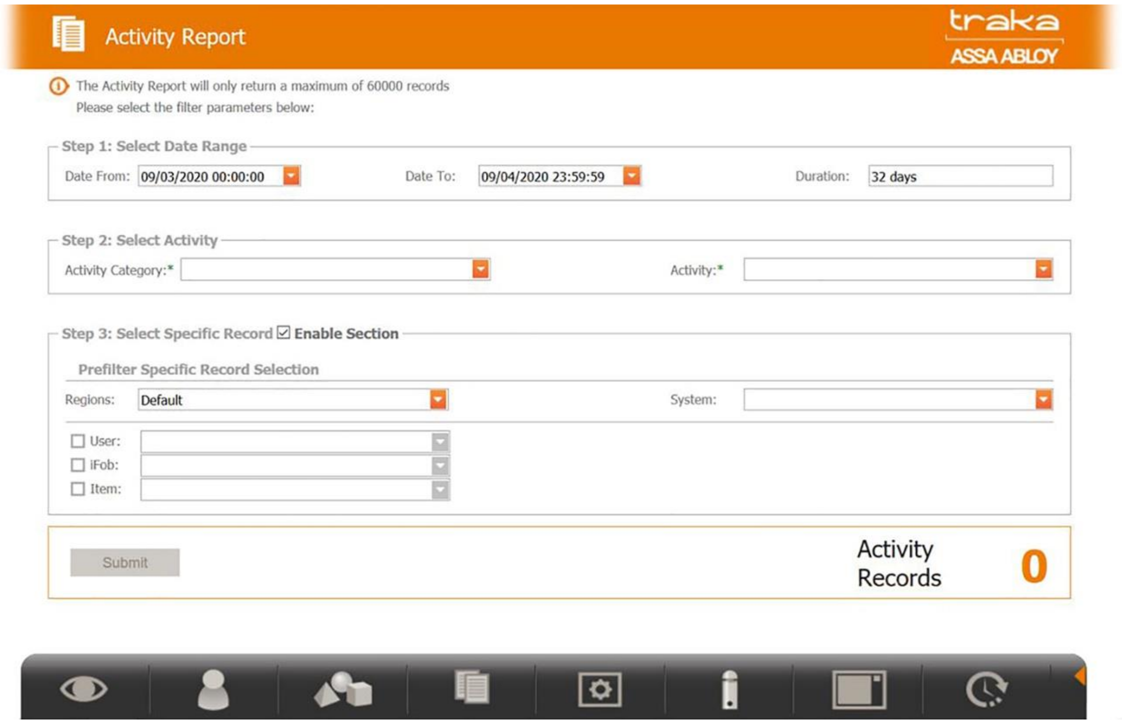
Activity Report

The Activity Report provides a pre-filter page specific to all system, iFob and Item Activity. It is divided into 3 sections to allow for a date range, activity type and a specific record selection. It will allow a maximum return of 60000 records.

1. Click the banner named **General** to expand the General category.

2. To view the Activity Report, click on the banner and select **View This Report.**

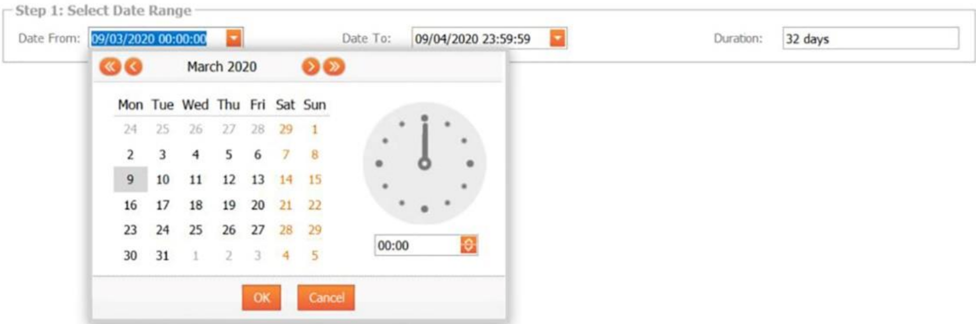
You will now be presented with the pre-filter page for the Activity Report.

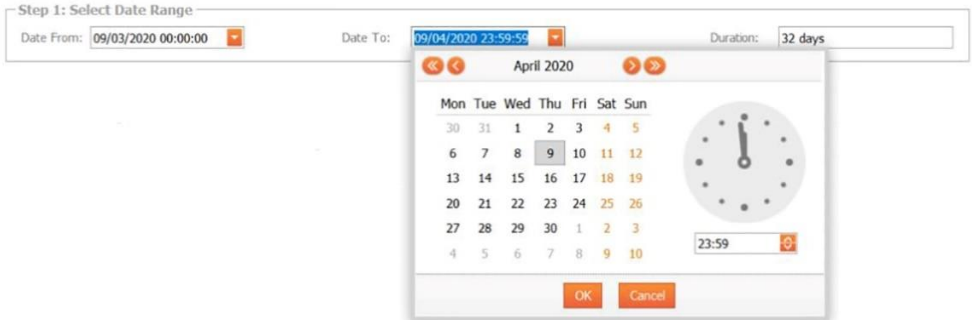


From the above example, the pre-filter page is divided up into 3 steps, concluding with a Submit option.

Step 1: Select Date Range

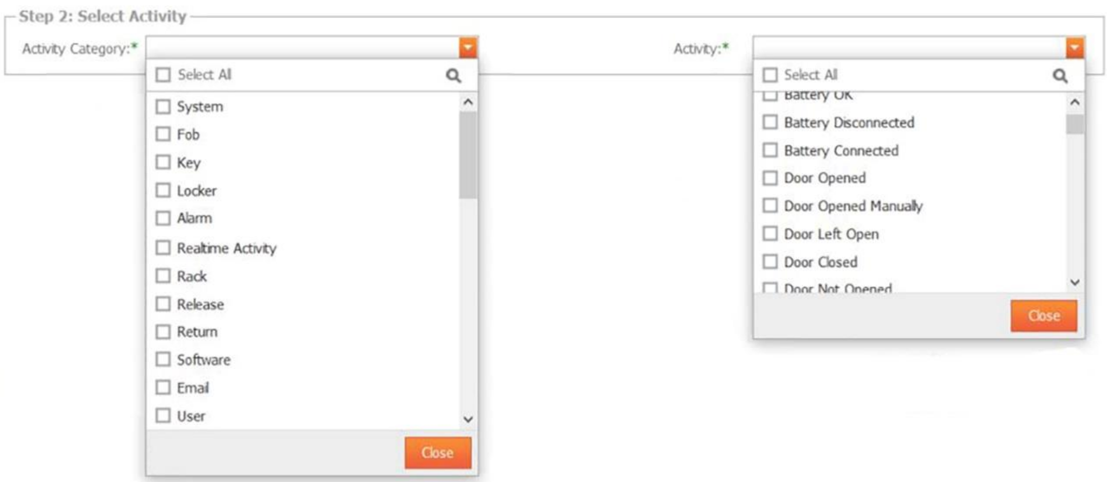
The **Select Date Range** comprises of 2 drop-down options to allow you to select both a start date and an end date. It will also display the overall duration.





Step 2: Select Activity

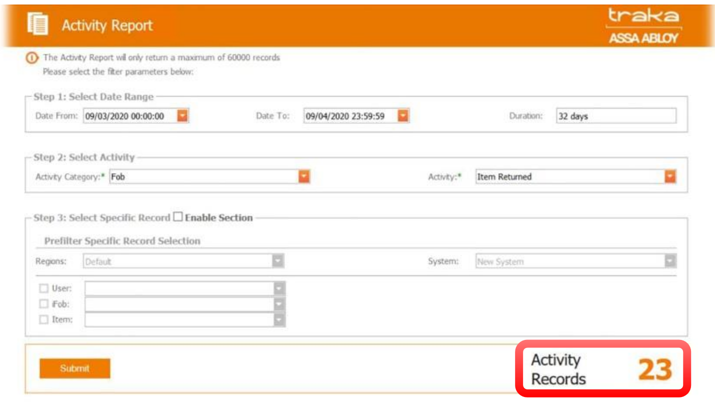
The **Select Activity** comprises of 2 drop-down menus. From the **Activity Category** menu, you can select from a list of different categories. These can be either selected individually or all at once. From the **Activity** menu, you can select from a list of different activities. These also can be selected individually or all at once.



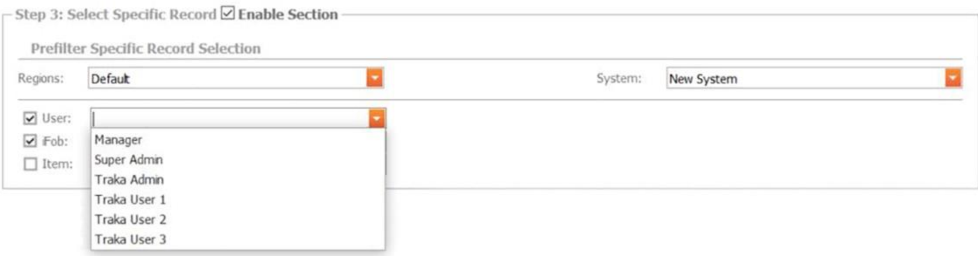
Step 3: Select Specific Record

The **Select Specific Record** is an optional step. It can be enabled by selecting the **Enable Selection** checkbox as shown below.

NOTE: If the checkbox is not selected, activity records will still be generated for the options selected in Step 2 as shown in the example below.



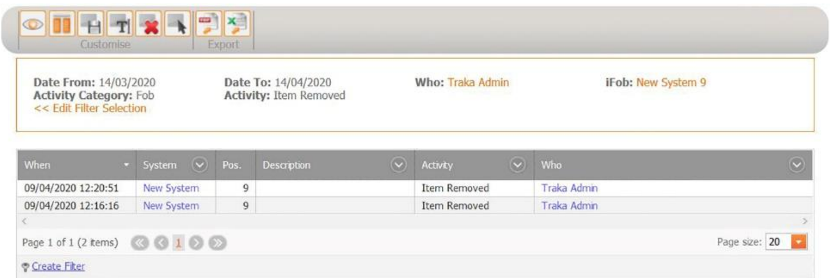
1. From the drop-down menus, select the required Region and System.
2. Select the User drop down and select from the list of users.



3. Depending on the system type, select from the drop-down menus for either iFob or Item.

Once you have finished making your selections, click on the **Submit** button.

The final report will provide a summary of the options that were selected and the overall report for those options.



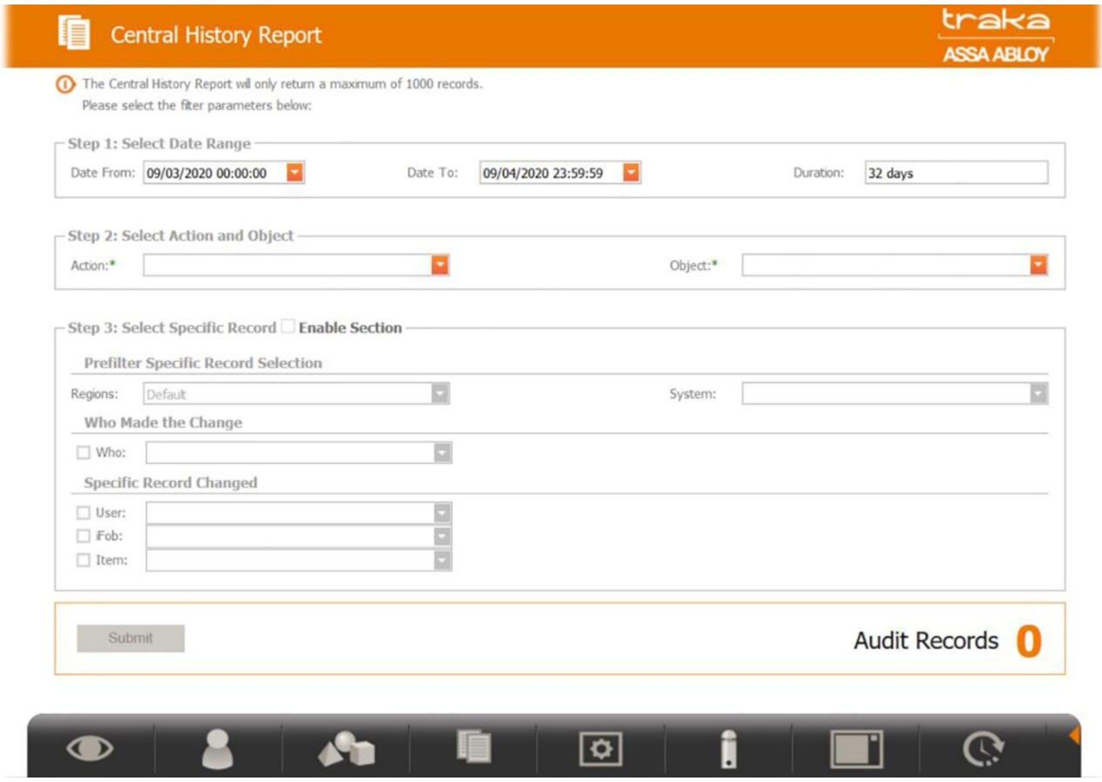
Central History Report

The Central History Report provides a pre-filter page that will show any changes that have been made to records and settings within TrakaWEB. It is divided into 3 sections to allow for date range, actions and a specific record selection. It will allow a maximum return of 1000 records.

1. Click the banner named **General** to expand the General category.

2. To view the Central History Report, click on the banner and select **View This Report.**

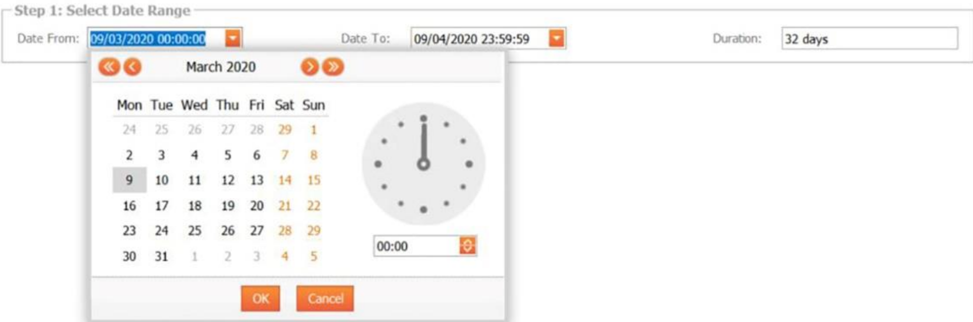
You will now be presented with the pre-filter page for the Central History Report.

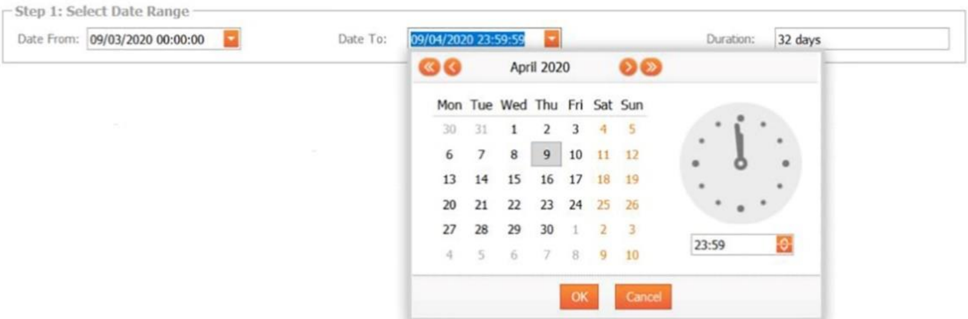


From the example above, the pre-filter page is divided up into 3 steps, concluding with a Submit option.

Step 1: Select Date Range

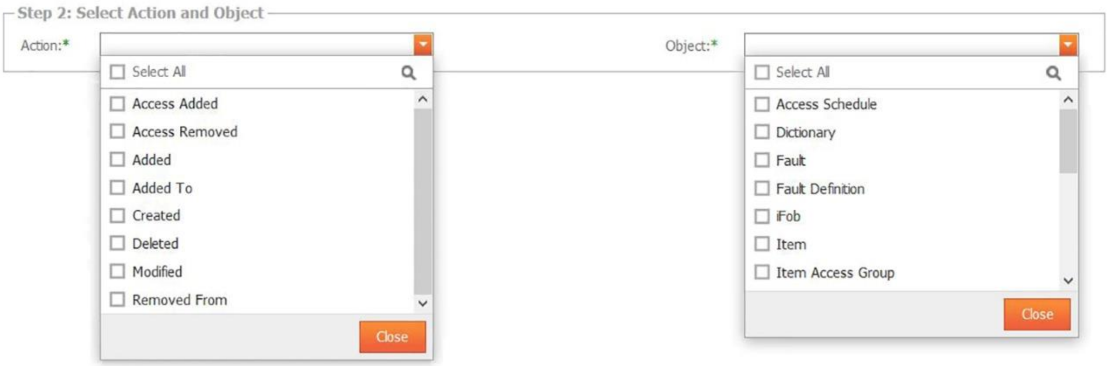
The **Select Date Range** comprises of 2 drop-down options to allow you to select both a start date and an end date. It will also display the overall duration.



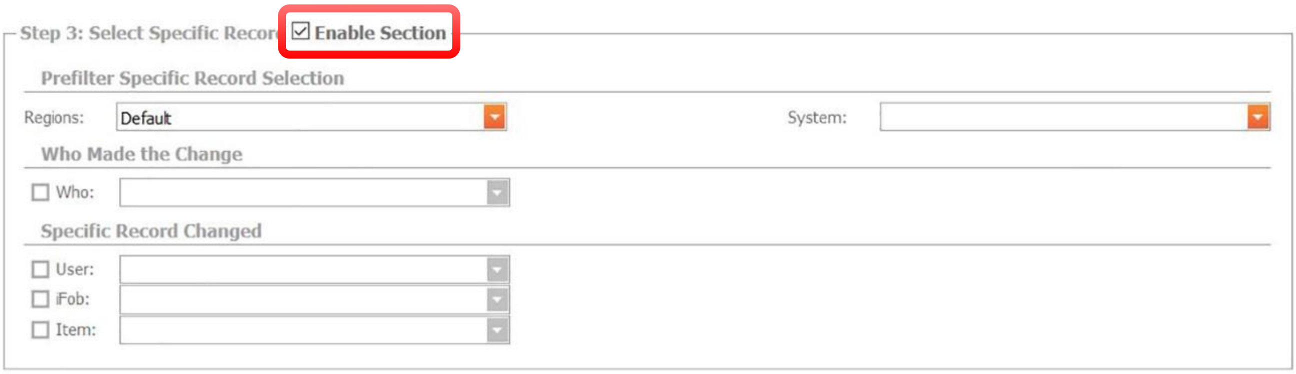


Step 2: Select Action and Object

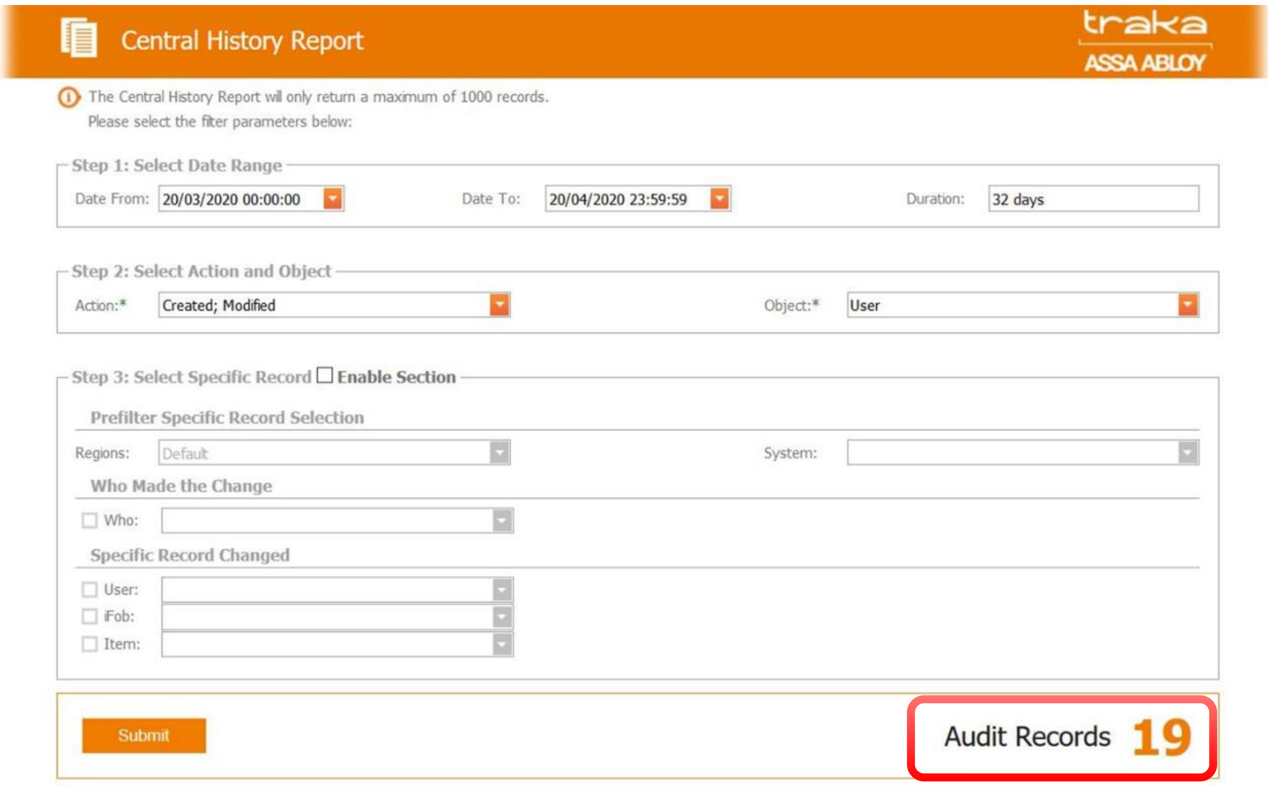
The **Select Action and Object** section comprises of 2 drop-down menus. From the **Action** menu, you can select from a list of different categories. These can be either selected individually or all at once. From the **Object** menu, you can select from a list of different categories in relation to the selected actions. These also can be selected individually or all at once.



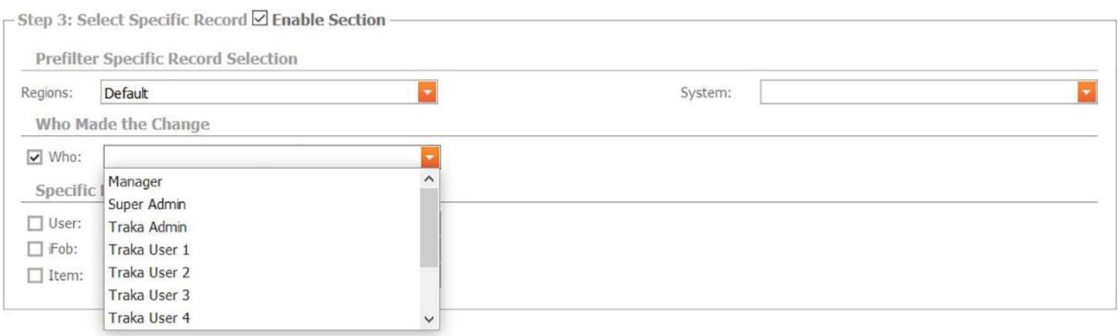
Step 3: Select Specific Record



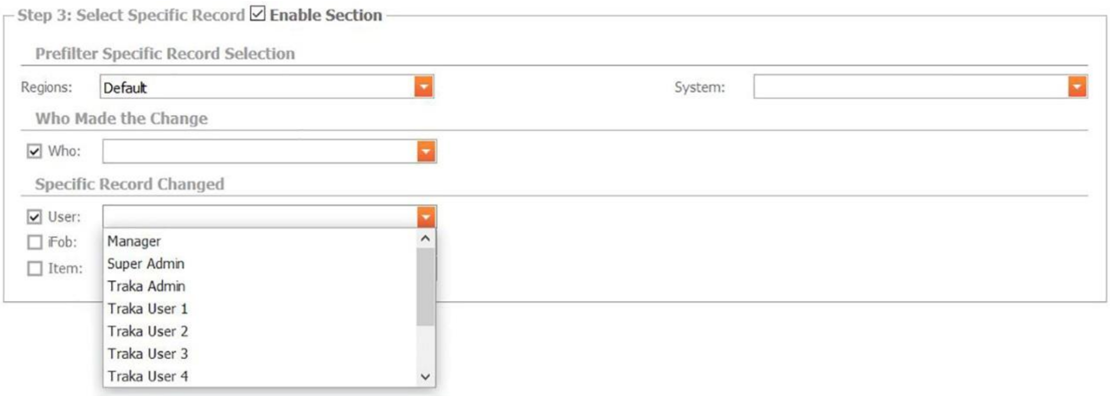
NOTE: If the checkbox is not selected, activity records will still be generated for the options selected in Step 2 as shown in the example below.



1. From the drop down menus, select the required Region and System.
2. To specify who made the change, select the checkbox and then click on the **Who** drop down and select from the list of users.



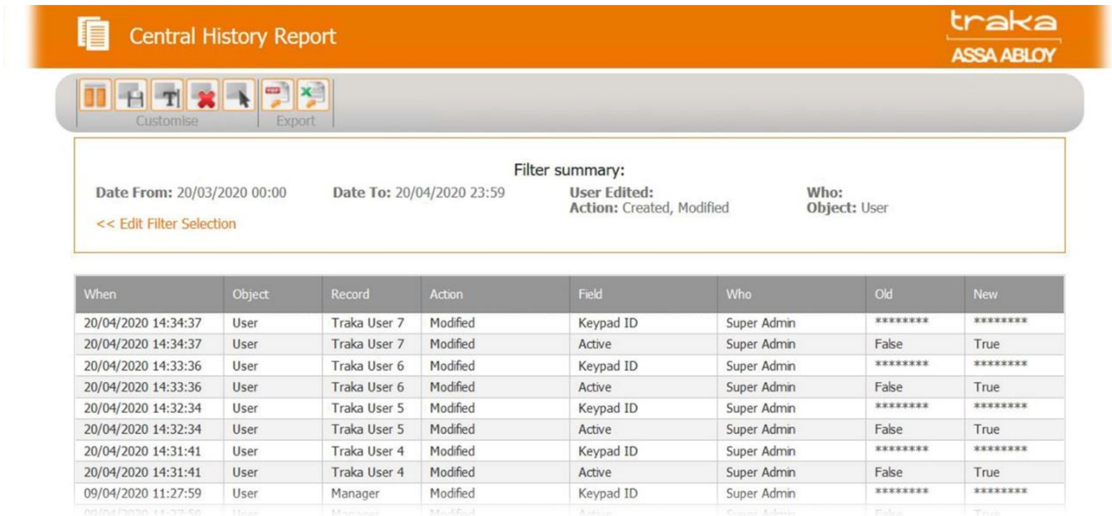
3. Select the User drop down and select from the list of users.



4. Depending on the system type, select from the drop down menus for either iFob or Item.

Once you have finished making your selections, click on the **Submit** button.

The final report will provide a summary of the options that were selected and the overall report for those options.



When	Object	Record	Action	Field	Who	Old	New
20/04/2020 14:34:37	User	Traka User 7	Modified	Keypad ID	Super Admin	********	********
20/04/2020 14:34:37	User	Traka User 7	Modified	Active	Super Admin	False	True
20/04/2020 14:33:36	User	Traka User 6	Modified	Keypad ID	Super Admin	********	********
20/04/2020 14:33:36	User	Traka User 6	Modified	Active	Super Admin	False	True
20/04/2020 14:32:34	User	Traka User 5	Modified	Keypad ID	Super Admin	********	********
20/04/2020 14:32:34	User	Traka User 5	Modified	Active	Super Admin	False	True
20/04/2020 14:31:41	User	Traka User 4	Modified	Keypad ID	Super Admin	********	********
20/04/2020 14:31:41	User	Traka User 4	Modified	Active	Super Admin	False	True
09/04/2020 11:27:59	User	Manager	Modified	Keypad ID	Super Admin	********	********

4.5.3 STATUS REPORTS

The Status Report comprises of 2 report categories:

- Current Item Status Report
- Curfew Status Report

Current Item Status Report

This report shows all items and their system status, e.g. whether or not it is in the system.

1. Click the banner named Status to expand the Status category.

2. Click **Current Item Status Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Curfew Status Report

This report shows all items that are out of the system and the curfews set against them.

1. Click the banner named Status to expand the Status category.

2. Click **Curfew Status Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

4.5.4 EXCEPTION REPORTS

The Exception Reports comprises of 5 different report categories:

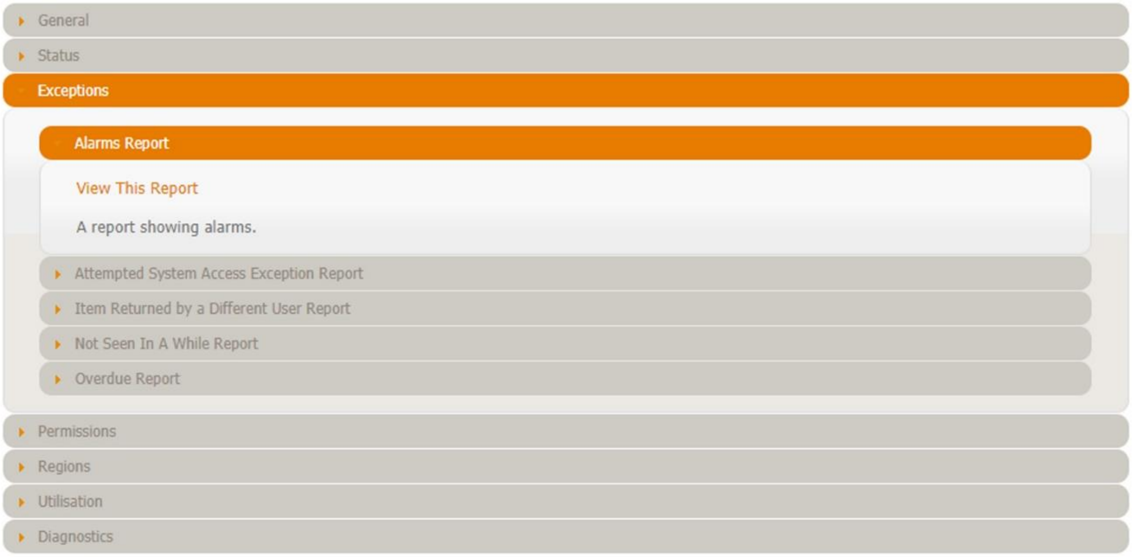
- Alarms Report
- Attempted System Access Exception Report
- Item Returned by a Different User Report
- Not seen in a While Report
- Overdue Report

Alarms Report

This report shows any alarms that have been triggered.

1. Click the banner named Exceptions to expand the Exceptions category.

2. Click **Alarms Report** to expand the information drop-down box, which will contain a brief description of the report.



3. Select 'View This Report'.

4. You will be presented with the event report page. From here, you can select the time frame you wish the report to gather information from. Selecting the start or end date will allow you to input the specific days and times for the report. See Reports Overview for further details.

5. After selecting the date and time the report will automatically generate.

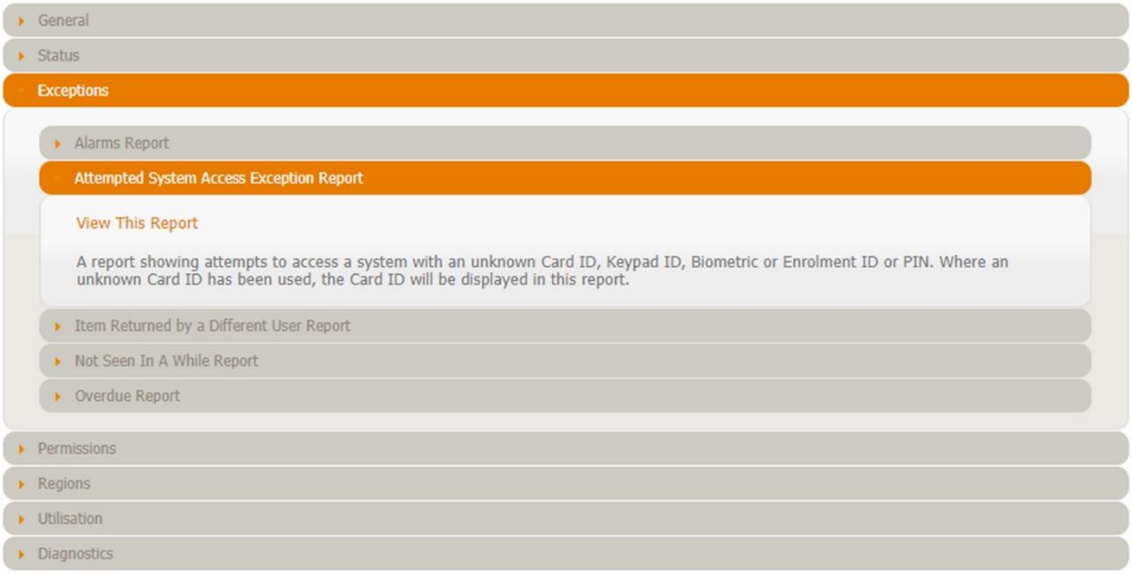
6. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Attempted System Access Exception Report

This report shows any attempts to access a system using an unknown Card ID, Biometric, Enrolment ID or PIN.

1. Click the banner named Exceptions to expand the Exceptions category.

2. Click **Attempted System Access Exception Report** to expand the information drop-down box, which will contain a brief description of the report.



3. Select 'View This Report'.

4. You will be presented with the event report page. From here, you can select the time frame you wish the report to gather information from. Selecting the start or end date will allow you to input the specific days and times for the report. See Reports Overview for further details.

5. After selecting the date and time the report will automatically generate.

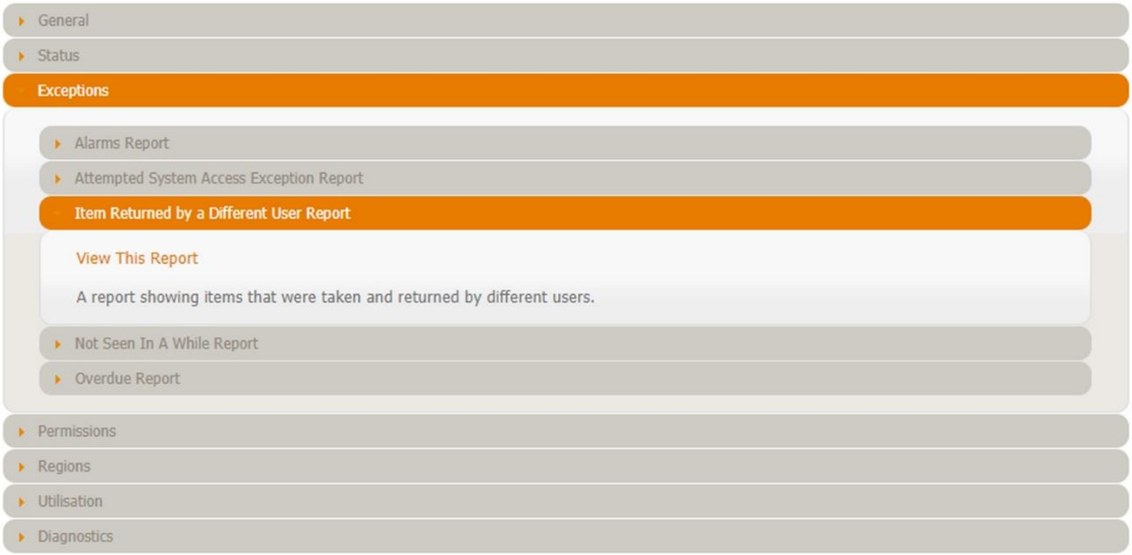
6. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Item Returned by a Different User Report

This report shows any items that were removed from the system and then later returned by a different user.

1. Click the banner named Exceptions to expand the Exceptions category.

2. Click **Item Returned by a Different User Report** to expand the information drop-down box, which will contain a brief description of the report.



3. Select 'View This Report'.

4. You will be presented with the event report page. From here, you can select the time frame you wish the report to gather information from. Selecting the start or end date will allow you to input the specific days and times for the report. See Reports Overview for further details.

5. After selecting the date and time the report will automatically generate.

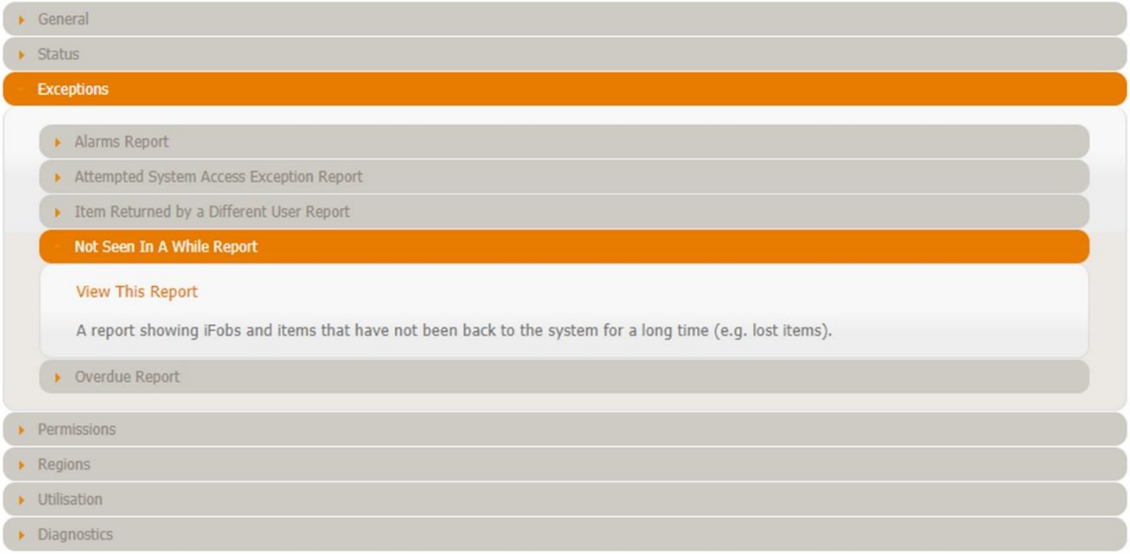
6. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Not Seen in a While Report

This report shows all items and iFobs that have been absent from the system for a long period of time.

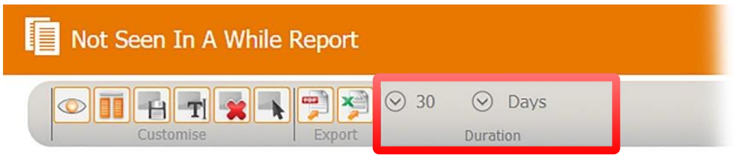
1. Click the banner named Exceptions to expand the Exceptions category.

2. Click **Not Seen in a While Report** to expand the information drop-down box, which will contain a User-determined time scaled description of the report.



3. Select 'View This Report'.

4. The report will automatically generate. The default duration is set to 30 days but can be adjusted by selecting the chevrons.



5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Overdue Report

This report shows all items in the system that have an overdue curfew.

1. Click the banner named Exceptions to expand the Exceptions category.

2. Click **Overdue Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

NOTE: If any optional features have been enabled, an extra report named 'Data Entry Exception Report' may also be available.

4.5.5 PERMISSIONS REPORTS

The Permissions Report comprises of 4 report categories:

- Item Access by Item Report
- Item Access by User Report
- Web Access by Group Report
- Web Access by User Report

Item Access by Item report

This report shows a list of items and under each item is the user who has access to it.

1. Click the banner named Permissions to expand the Permissions category.

2. Click **Item Access by Item Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a [PDF]() or into an [Excel]() Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Item Access by User report

This report shows a list of users and under each user is what items they have been granted access.

1. Click the banner named Permissions to expand the Permissions category.
2. Click **Item Access by user Report** to expand the information drop-down box, which will contain a brief description of the report.

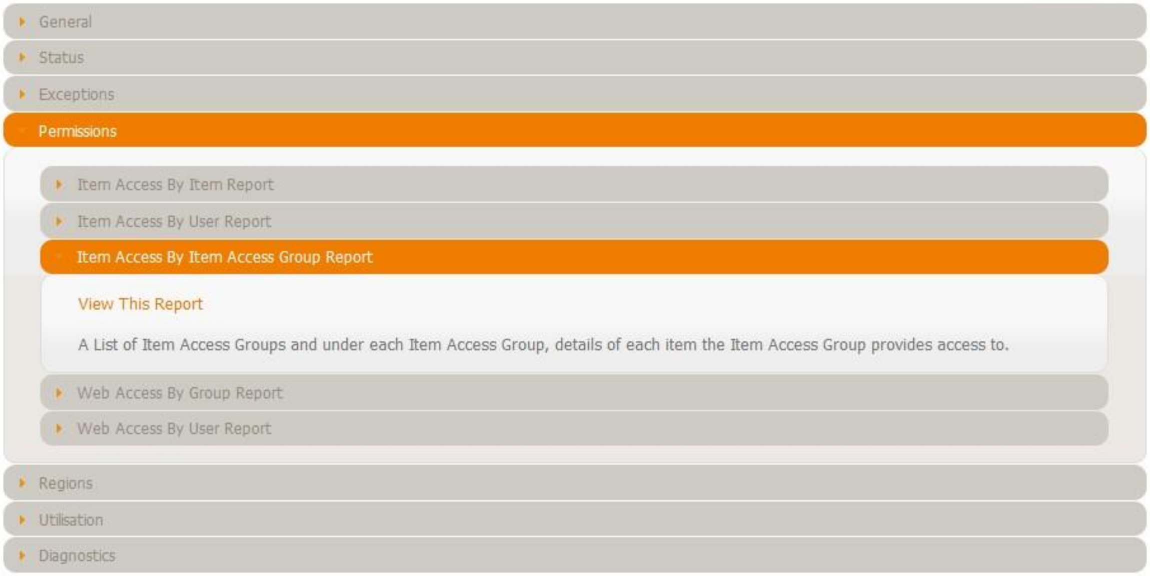
3. Select 'View This Report'.
4. The report will automatically generate.
5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Item Access by Item Access Group Report

This report shows a list of Item Access Groups and the item access associated with them.

1. Click the banner named Permissions to expand the Permissions category.

2. Click **Item Access by Item Access Group Report** to expand the information drop-down box, which will contain a brief description of the report.



3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Web Access by Group Report

This report shows a list of web access groups and the users who have access to them.

1. Click the banner named Permissions to expand the Permissions category.

2. Click **Web Access by Group Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Web Access by User Report

This report shows a list of web access groups and the users who are in those groups.

1. Click the banner named Permissions to expand the Permissions category.

2. Click **Web Access by User Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select ‘View This Report’.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

4.5.6 REASON REPORTS

Reason Logging is a cost option feature that allows a user to log the 'reason' they are removing/returning the item at the system. You can run specific reports of which reasons are most commonly used and which items they are used on.

Reasons Report

Running this report will show what 'reason' was logged against which item and the user who removed/returned the item, the date & time, system etc.

1. Click the banner named Reasons to expand the Reasons category.
2. Click **Reasons Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

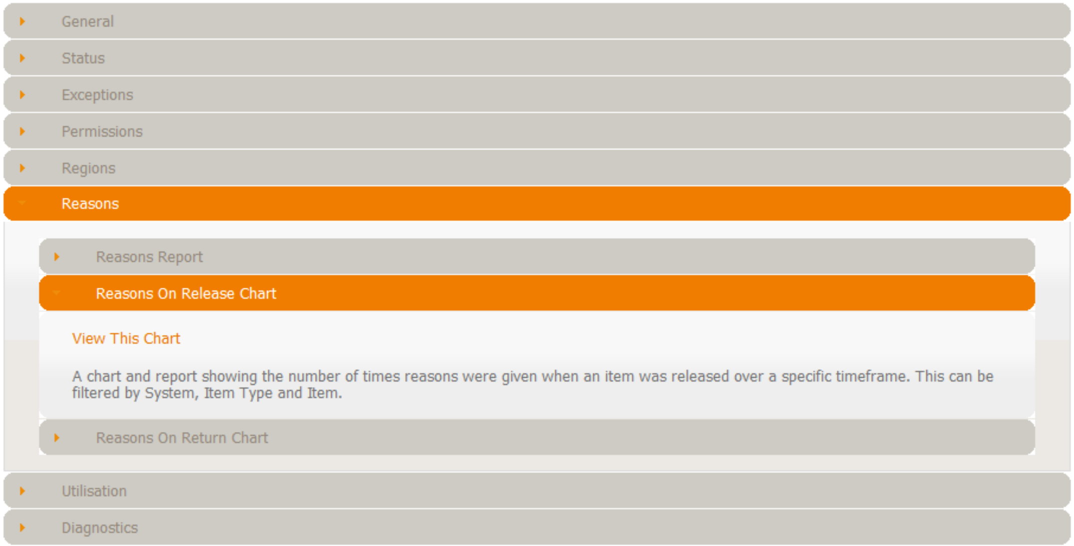
4. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Reasons on Release Chart

This report will graphically display the reason items are removed from the system. This is clearly represented by a pie chart diagram, which shows the most common uses of the items and the reasons that are logged against them when they are removed.

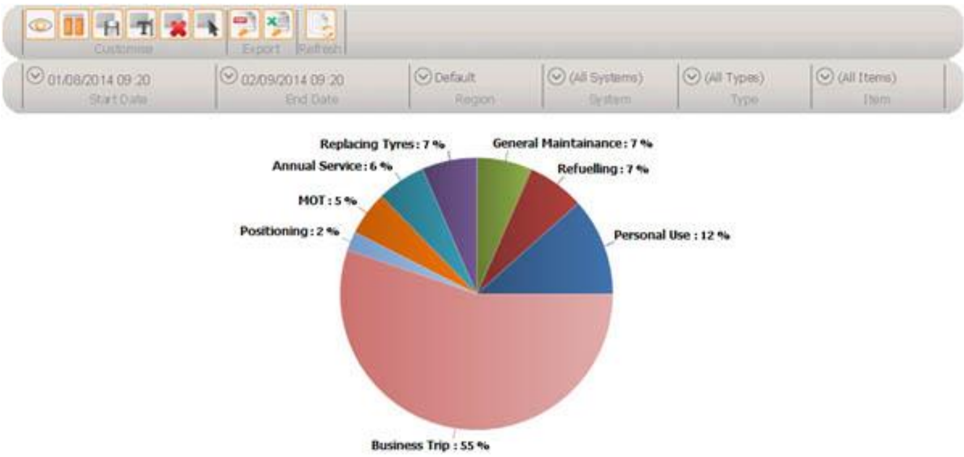
1. Click the banner named Reasons to expand the Reasons category.

2. Click **Reasons On Release Chart** to expand the information drop-down box which will contain a brief description of the report.



3. Select 'View This Report'.

You can filter this report by start date, end date, regions, type (item types) and items from the ribbon toolbar.



Reason	Number of times selected
Business Trip	55
Personal Use	12
Refuelling	7
General Maintainance	7
Replacing Tyres	7
Annual Service	6
MOT	5
Positioning	2

Page 1 of 1 (8 items) Page size: 20

You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Reasons on Return Chart

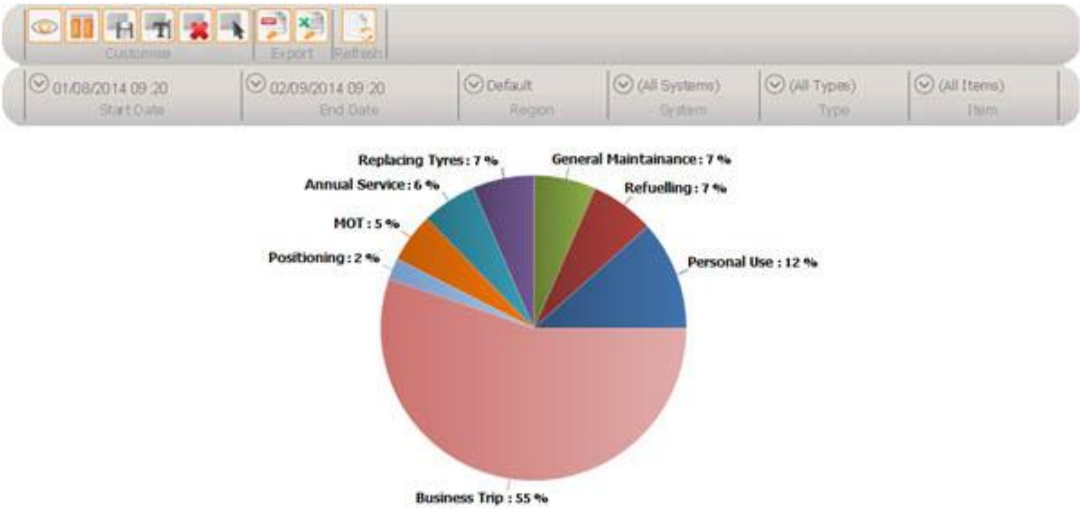
This report will graphically display the reason items are returned to the system. This is clearly represented by a pie chart diagram, which shows the most common uses of the items and the reasons that are logged against them when they are returned.

1. Click the banner named Reasons to expand the Reasons category.

2. Click **Reasons On Return Chart** to expand the information drop-down box which will contain a brief description of the report.

3. Select 'View This Report'.

You can filter this report by start date, end date, regions, type (item types) and items from the ribbon toolbar.



Reason	Number of times selected
Business Trip	55
Personal Use	12
Refuelling	7
General Maintainance	7
Replacing Tyres	7
Annual Service	6
MOT	5
Positioning	2

Page 1 of 1 (8 items) Page size: 20

4. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

4.5.7 REGION REPORTS

Users by Region Report

This report shows a list of regions and which users have access to each region.

1. Click the banner names Regions to expand the Regions category.

2. Click **Users by Region Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Activity Chart

This report/chart shows how many times an item has been removed from the system.

1. Click the banner named Utilisation to expand the category.
2. Click **Users by Activity Chart** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.
4. The report will automatically generate.
5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

4.5.9 DIAGNOSTICS REPORTS

The Diagnostics Report comprises of 2 report categories:

- iFob Undetectable Report
- Command List Report

iFob Undetectable Report

This report shows the number of times each iFob/item has gone undetectable in the last 30 days.

1. Click the banner names Diagnostics to expand the Diagnostics category.

2. Click **iFob Undetectable Report** to expand the information drop-down box, which will contain a brief description of the report.

3. Select 'View This Report'.

4. The report will automatically generate.

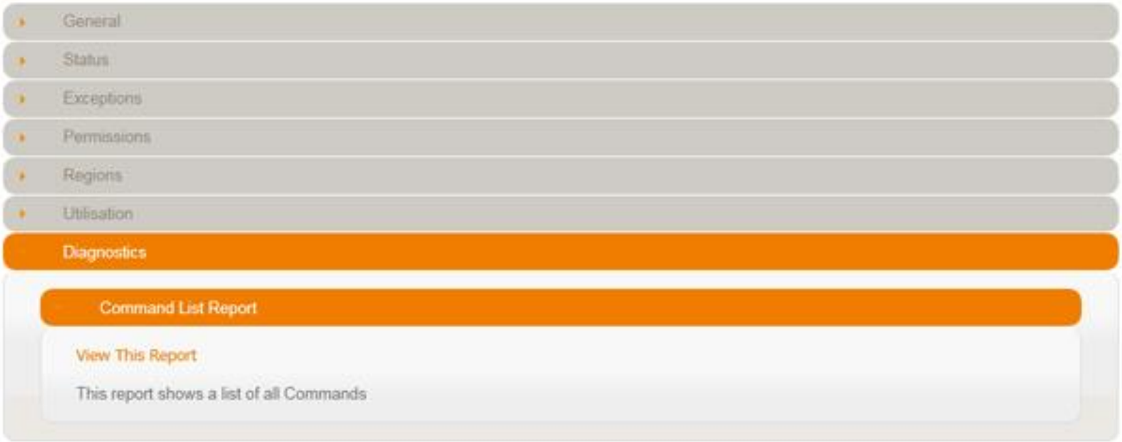
5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

Command List Report

This report shows how many times an item has been removed from the system.

1. Click the banner named Diagnostics to expand the Diagnostics category.

2. Click **Command List Report** to expand the information drop-down box, which will contain a brief description of the report.



3. Select 'View This Report'.

4. The report will automatically generate.

5. You can export the report as a PDF or into an Excel Spreadsheet by selecting the respective buttons from the ribbon toolbar.

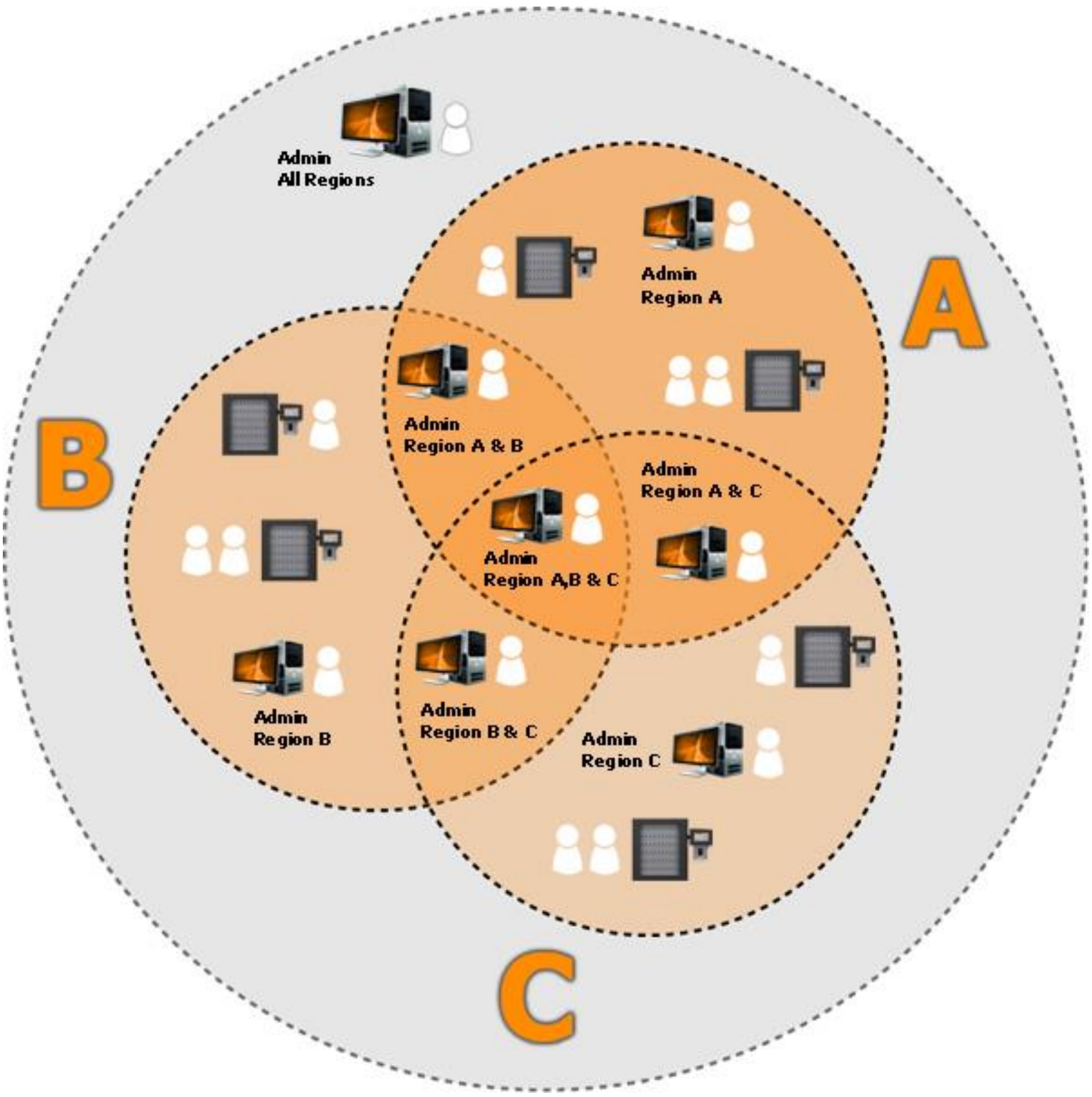
4.6 SOFTWARE SETTINGS

4.6.1 REGIONS

4.6.1.1 REGIONS OVERVIEW

Regions allow for TrakaWEB users to only access or edit the information on Systems, iFobs, Items and Users within their specified region(s). Multiple Regions provide much increased flexibility for customers with more complex web and system access requirements. An example of where Multiple Regions maybe necessary, is where an organisation has many Traka systems spread geographically and each region has one or more TrakaWEB Admin users that are only responsible for maintaining their own region(s). In addition some organisations may choose to regionalise by department e.g. Sales, Finance, Engineering, where each department has a TrakaWEB Administrator who can only see Traka Systems and Users within their department(s).

Below is a graphic representation of how Multiple Regions could be defined.



4.6.2 REGION VISIBILITY RULES

There are various 'Region Rules' that may be used to describe the behaviour of data visibility and data manipulation within TrakaWEB.

These rules are important due to the way in which Administrators and Data entities such as Item Access Groups may belong to more than one region. Therefore, the rules have been defined to help describe which users can see what.

So, for example, a user such as an Administrator logging into TrakaWEB must only be able to see Data that relates to the region(s) that they are a member of.

NOTE: It is worth taking into consideration that a System can only belong to a single Region but an Administrator, User or Item Access Group etc. can belong on one or multiple Regions.

The rule descriptions are as follows:

- Wholly Contained Regions
- Partially Contained Regions
- Multiple Levels of Filtering
- Visible Regardless of Filtering

Wholly Contained Regions:

The 'Wholly Contained Regions' rule describes Data that will only be visible to the Administrator that is logged in, when both the Administrator and the Data Entities meet the following parameters:

- They are members of the same Region but at the same time
- They are **NOT** members of other regions that are outside the scope of the logged in Administrators Regions

This will allow an Administrator who is logged in to have overall control of data and prevent anyone else that is not a member of the same region set from changing it.

The table below is an example of TrakaWEB already setup with 3 Regions. The Regions are named A, B and C. 'All Regions' refers to A, B and C collectively.

Administrator	Data Entity				
	All Regions (meaning A, B & C)	Region A	Region B	Region A & B	Region A, B & C
All Regions (meaning A, B & C)	Granted	Granted	Granted	Granted	Granted
Region A	Denied	Granted	Denied	Denied	Denied
Region B	Denied	Denied	Granted	Denied	Denied
Region A & B	Denied	Granted	Granted	Granted	Denied
Region A, B & C	Granted	Granted	Granted	Granted	Granted

Partially Contained Regions:

The 'Partially Contained Regions' rule describes Data that will only be visible to an Administrator that is logged in when both the Administrator and Data Entities meet the following parameters:

- They are members of the same Region but at the same time
- They are **ALSO** members of other Regions that are outside the scope of the logged in Administrators Regions

This will allow an Administrator who is logged in to have the ability to only allow them to edit their portion of particular regional Data. They will be unable to edit Data outside of their region set. Under the 'Partially Contained Regions' rule, common Data spanning multiple Regions will not be editable but may still be editable under the 'Wholly Contained Regions' rule.

The table below is an example of TrakaWEB already setup with 3 Regions. The Regions are named A, B and C. 'All Regions' refers to A, B and C collectively.

Administrator	Data Entity				
	All Regions (meaning A, B & C)	Region A	Region B	Region A & B	Region A, B & C
All Regions (meaning A, B & C)	Granted	Granted	Granted	Granted	Granted
Region A	Granted (Region A Portion)	Granted	Denied	Granted (Region A Portion)	Granted (Region A Portion)
Region B	Granted (Region B Portion)	Denied	Granted	Granted (Region B Portion)	Granted (Region B Portion)
Region A & B	Granted (Region A & B Portion)	Granted	Granted	Granted	Granted (Region A & B Portion)
Region A, B & C	Granted	Granted	Granted	Granted	Granted

Multiple Levels of Filtering:

Whilst considering regional visibility within TrakaWEB, there are 2 levels of filtering that can be applied to certain features or areas of the software that meet the following conditions:

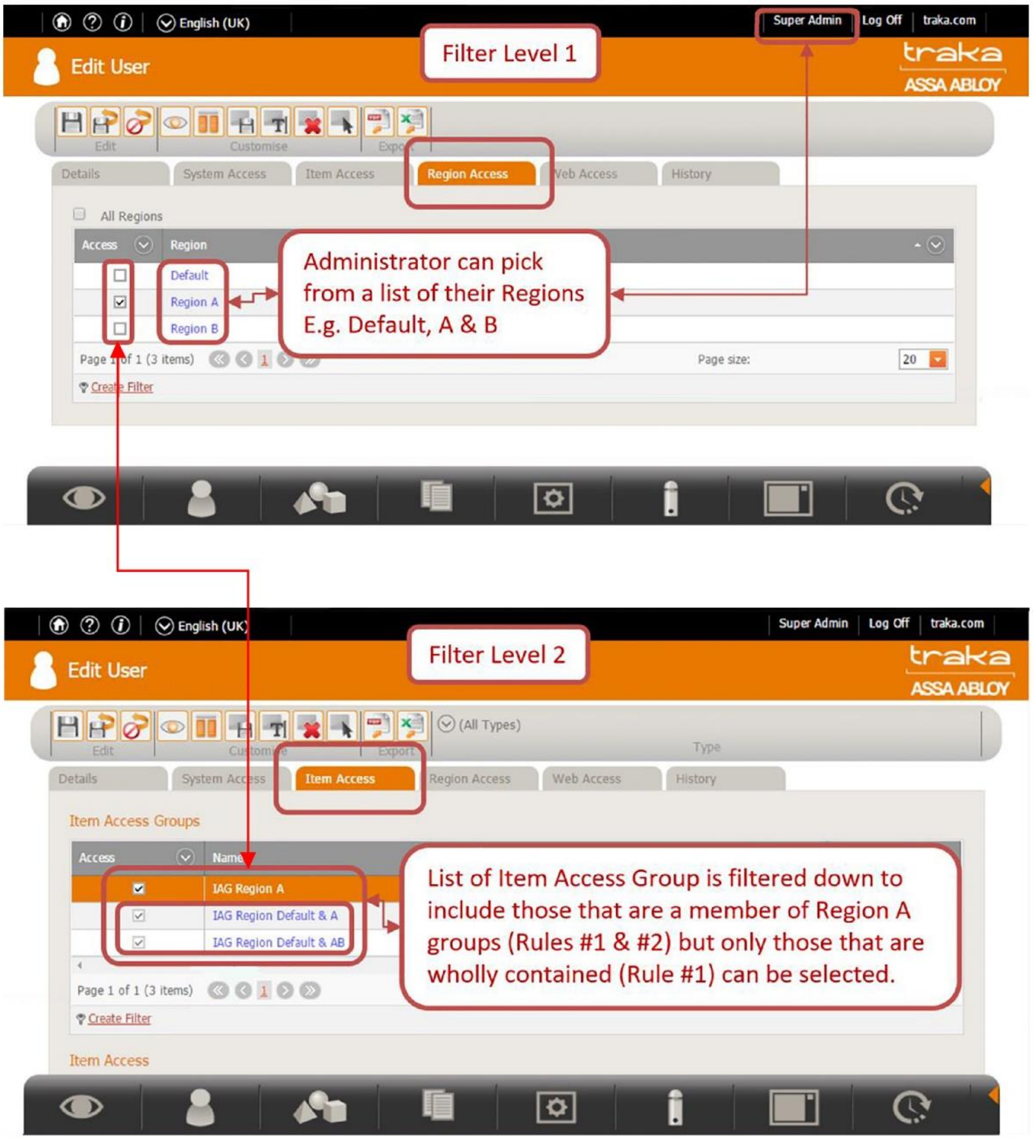
- The regional visibility of the logged in Administrator
- The selected regional visibility of the Data being edited

Consider the following example:

- An Administrator may be creating a User record
- The Administrator is a member of Regions Default, A & B
- The Administrator places a User into only Region A

This will now affect what access rights the Administrator can grant to the User (from the Item Access tab). This limits the list to any Item Access Groups that are a member of Region A – under the 'Partially Contained Regions' rule, but only allowing Item Access Groups that are a member of Region A only – the 'Wholly Contained Regions' rule.

This is shown below:



Visible Regardless of Regions:

For the 'Visible Regardless of Regions' rule, some features of TrakaWEB software will be accessible to all Administrators irrespective of Region visibility such as:

- Item Types
- Software Permissions Groups
- Activity Types

4.6.3 ADDING A NEW REGION

Regions allow TrakaWEB users to see and access only the information from Systems, Items and Users within their specified region(s). Regions are particularly useful when managing many systems spread across a large area.

1. To add a new region, you will need to navigate to the Regions page. Using the Navigation Toolbar at the bottom of the page, select Software Settings, then from the mini menu click Regions. This will display the list of all the current regions within your database.

2. Click the Add button.

3. You will then be prompted to enter a region name e.g. Research & Development.

4. Once you have entered a name, you can click the Save & Return button.

5. You will now be taken back to the region list, which will be populated with the newly added region. To add more regions simply click the Add button and restart the process from step 1.

4.6.4 MSME

4.6.5 EDITING A REGION

Editing a region allows you to rename an existing region. To edit a region, you will need to navigate to the Regions page.

NOTE: Please keep in mind that all the systems, users and groups will stay assigned to the region even after it has been renamed.

1. Using the Navigation Toolbar at the bottom of the page, select Software Settings, then from the mini menu click **Regions**. This will display the list of all the current regions within your database.

2. Highlight the region you wish to edit and click the **Edit** button.

3. You will then be able to rename the region. In the example below the **Research & Development** region has been renamed to **Production**.

4. Click the **Save** button.

5. Select the **History** tab. You will notice that a full history of changes made to that region is listed here. This clearly shows that the region has been renamed on the 21/03/13 by Aaron Kennedy and has been changed from **Research & Development** to **Production**.

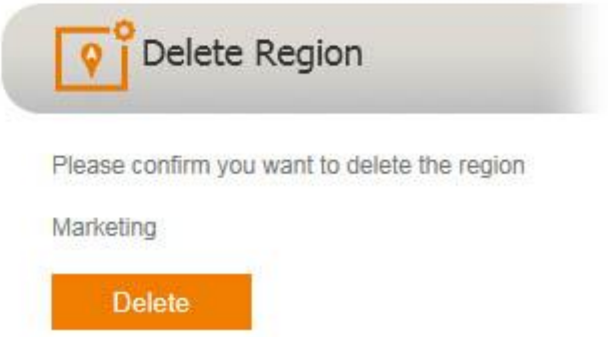
6. Click **Save & Return** and you will now be taken back to the region list. You will notice that the region you have just renamed has been updated in the list. To rename more regions, simply click the **Edit** button and restart the process from step 1.

4.6.6 DELETING A REGION

To delete a region, you will need to navigate to the Regions page.

1. Using the Navigation Toolbar at the bottom of the page, select Software Settings, then from the mini menu click Regions. This will display the list of all the current regions within your database.

2. Highlight the region you wish to delete and click the Delete button.
3. You will then be prompted by a message asking if you wish to permanently delete the region, select Delete.



4. You will now be taken back to the region list. You will notice that the region you have just deleted is no longer in the list. To delete more regions, simply restart the process from step 1.

4.7 SOFTWARE PERMISSION GROUPS

Software Permission Groups define what areas of the software users have access to within TrakaWEB. The default group is the 'Super Admin' group, which has full access to TrakaWEB. However, you may want a user to be able to create and edit another user's details but not be able to delete them. Alternatively, you may want to grant a manager access to the Items and iFobs within their group, but not to the rest of the business. Using the expandable list, you can quickly select what permissions the group does or does not have.

The two subsections below will demonstrate how to create the two examples given.

To assign a software permission group to a user, refer to Permission Groups.

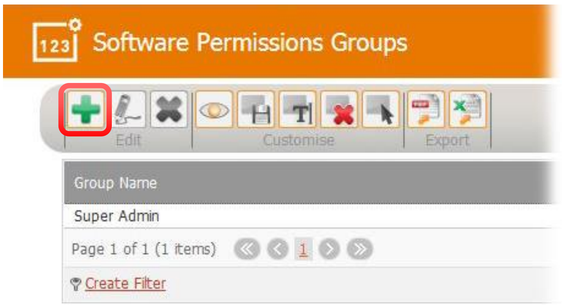
4.7.1 CREATING A NEW SOFTWARE PERMISSIONS GROUP

1. Using the navigation toolbar at the bottom of the page, click Software Settings, then select Software Permissions Groups.

2. You will now be taken to the Software Permissions Groups landing page. The only Group initially present will be 'Super Admin'.

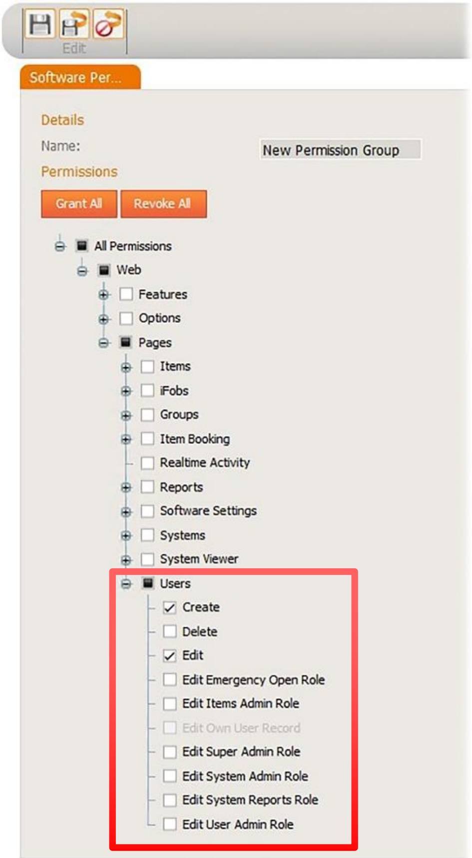
NOTE: By default, the 'Super Admin' group will have access to all permissions, which cannot be edited by another Group.

3. To create a new group, click on the Add button.

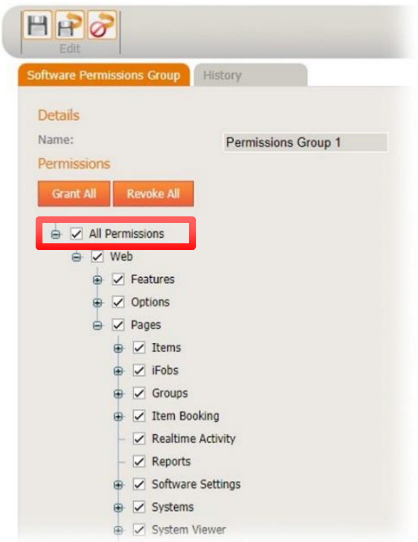


4. You will then be prompted to enter a group name.

5. Under the name field are two expandable tick boxes, one named 'All Permissions', and the other named 'Web'. You can now expand the 'Web' list and select which permissions you wish the group to have access to. For example, you may want any users within this group to be able to create and edit users but never able to delete them or allow them to edit System admin or System Reports Roles. To do that, simply expand the 'pages' tab, and then expand the 'users' tab and select Create & Edit. Ensure that the remaining roles remain unticked as shown in the example below.



Selecting the 'All Permissions' box will allow all permissions to that group.

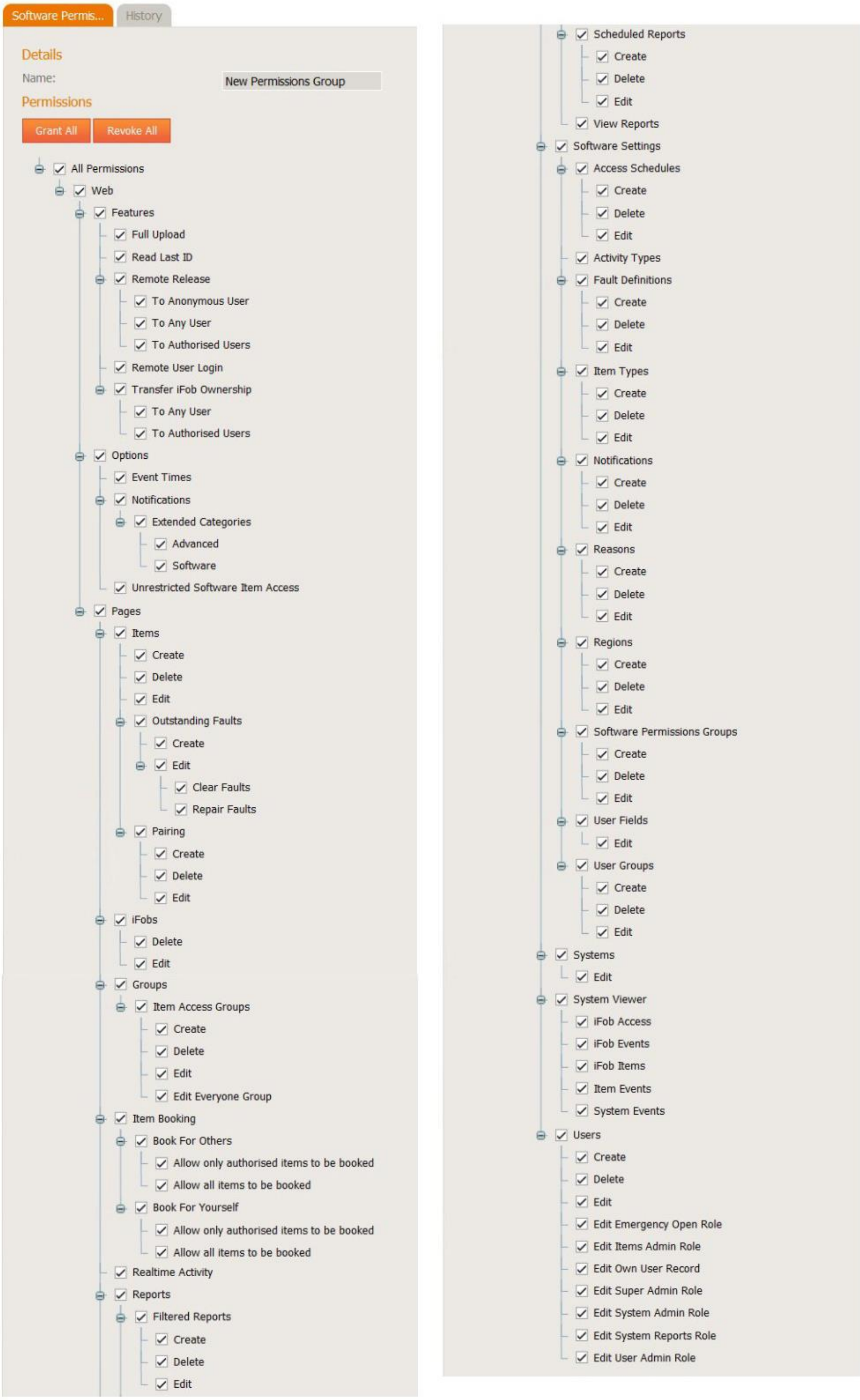


NOTE: If you select the title of a group of options then all the sub options within that list are also selected. E.g., iFobs list consists of Edit & Delete. By selecting the header 'iFobs', you will activate all the sub options.

Once the group has been created, you can assign it to a user in Permission Groups.

4.7.2 PERMISSIONS

The following is a list of all the Software Permissions in TrakaWEB.



4.7.2.1 PERMISSIONS DETAILS

All Permissions:

WEB
By default, the 'Web' list will be expanded and will allow you to select which permissions you wish the group to have access to.

4.7.2.2 FEATURES

Features:

Full Upload
Selecting this checkbox will enable a user to perform a full upload of users, iFobs and events to TrakaWEB.

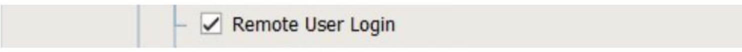
Read Last ID
Selecting this checkbox will read the last card ID presented to a 16bit system within a user record on the Edit User page.

Remote Release:

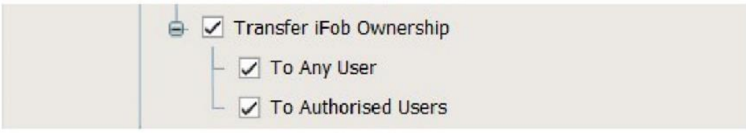
To Anonymous User
Selecting this checkbox will enable a user to release an iFob/item to a user who is not in the database.

To Any User
Selecting this checkbox will enable a user to release an iFob/item to any user in the database

To Authorised User
Selecting this checkbox will enable a user to only release an iFob/item to a user who has been granted access to that item.



Remote User Login
Selecting this checkbox will enable a user to remotely log another user into the system.

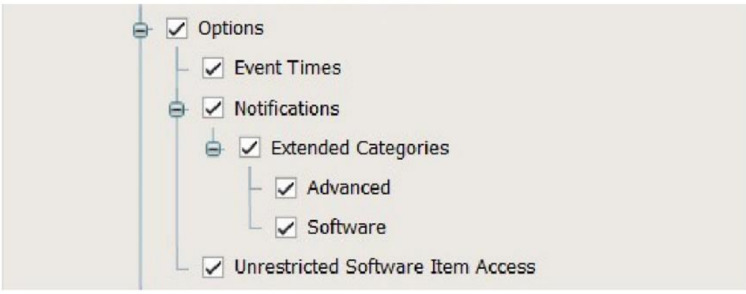


Transfer iFob Ownership:

To Any User
Selecting this checkbox will enable a user to transfer ownership of the item(s) in the selected position to any user in the database whilst the item(s) is/are already out of the system.

To Authorised Users
Selecting this checkbox will enable a user to transfer ownership of the item(s) in the selected position whilst the item(s) is/are already out of the system, providing the user has been granted access to the item(s).

4.7.2.3 OPTIONS



Options:

Event Times
Selecting this checkbox will enable a user to view the times at which events occurred.

Notifications

Extended Categories:

Advanced
Selecting this checkbox will enable a user to edit any advanced category related email notifications.

Software
Selecting this checkbox will enable a user to edit any software category related email notifications.

Unrestricted Software Item Access
Selecting this checkbox will enable a user to 'Edit Own User Record' when ticked and will enable users to edit their own software group details. It will also restrict and unrestrict item access in the Item Booking feature.

4.7.2.4 PAGES

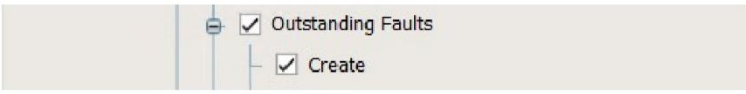
Pages

Items:

Create
Selecting this checkbox will enable a user to add new items to the system.

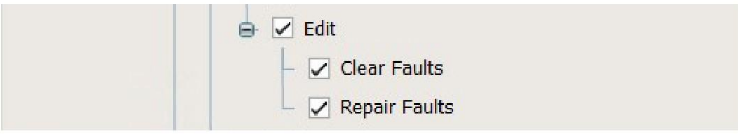
Delete
Selecting this checkbox will enable a user to delete existing items from the system.

Edit
Selecting this checkbox will enable a user to edit existing items in the system.



Outstanding Faults:

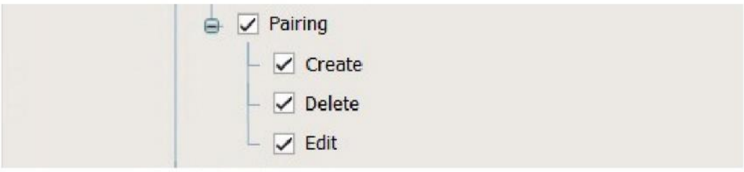
Create
Selecting this checkbox will enable a user to create outstanding faults in TrakaWEB.



Edit:

Clear Faults
Selecting this checkbox will enable a user to clear existing faults in TrakaWEB.

Repair Faults
Selecting this checkbox will enable a user to repair existing faults in TrakaWEB.



Pairing:

Create
Selecting this checkbox will enable a user to create Item or Locker Pairing rule in TrakaWEB.

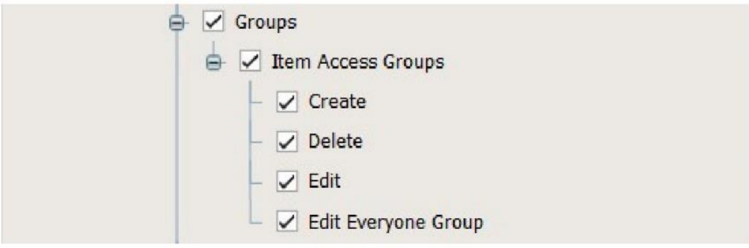
Delete
Selecting this checkbox will enable a user to delete an existing Item or Locker Pairing rule in TrakaWEB

Edit
Selecting this checkbox will allow a user to edit existing Item or Locker Pairing rules in TrakaWEB.

iFobs:

Delete
Selecting this checkbox will enable a user to delete an existing iFob in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit an existing iFob in TrakaWEB.



Groups

Item Access Groups:

Create
Selecting this checkbox will enable a user to create Item Access Groups in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Item Access Groups in TrakaWEB

Edit
Selecting this checkbox will enable a user to edit existing Item Access Groups in TrakaWEB

Edit Everyone Group
Selecting this checkbox will enable a user to edit an Item Access Group if it is set as an Everyone Group in TrakaWEB.

Item Booking

Book For Others:
Allow only authorised items to be booked

Selecting this checkbox will enable a user to only book authorised items for others in TrakaWEB.

Allow all items to be booked
Selecting this checkbox will enable a user to book all items in the system for others in TrakWEB even if they have not been granted access to them.

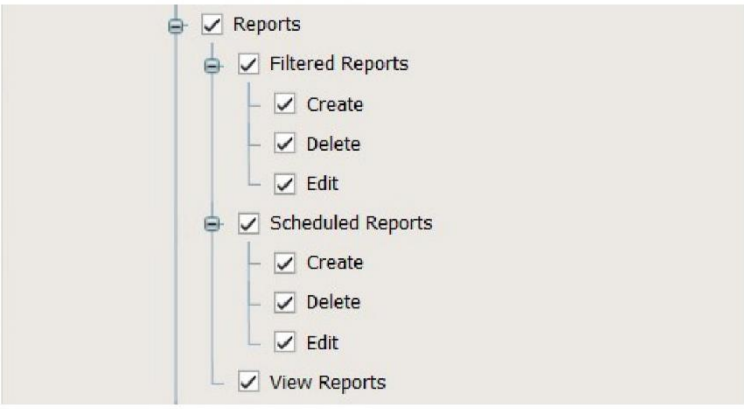
Book For Yourself:

Allow only authorised items to be booked
Selecting this checkbox will allow users who have been granted access to particular items to be able to take them during a booking.

Allow all items to be booked
Selecting this checkbox will allow users to take all booked items even if they have not been granted access to them.

NOTE: If Unrestricted Item Access is unticked, the user will only be able to grant items to others that the booking user has access to.

Realtime Activity:
Selecting this checkbox will allow a user to access the Realtime Activity page in TrakaWEB.



Reports

Filtered Reports:

Create
Selecting this checkbox will enable a user to create Filtered Reports in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Filtered Reports in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Filtered Reports in TrakaWEB.

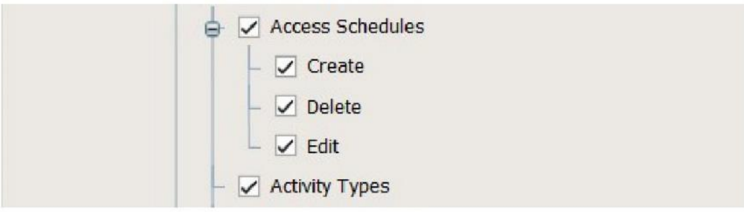
Scheduled Reports:

Create
Selecting this checkbox will enable a user to create Scheduled Reports in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Scheduled Reports in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Scheduled Reports in TrakaWEB.

View Reports
This will allow a user to view all available reports in TrakaWEB.



Software Settings

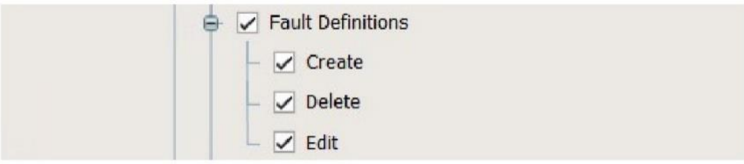
Access Schedules:

Create
Selecting this checkbox will enable a user to create Access Schedules in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Access Schedules in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Access Schedules in TrakaWEB.

Activity Types
Selecting this checkbox will enable a user to access the Activity Types page within Software Settings in TrakaWEB.



Software Settings

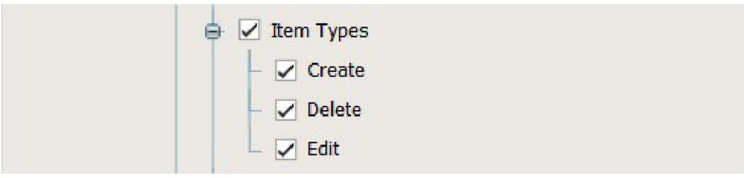
Fault Definitions:

Create
Selecting this checkbox will enable a user to create Fault Definitions in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Fault Definitions in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Fault Definitions in TrakaWEB.

Activity Types
Selecting this checkbox will enable a user to access the Activity Types page within Software Settings in TrakaWEB.



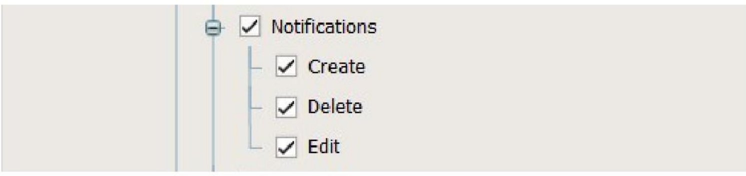
Software Settings

Item Types:

Create
Selecting this checkbox will enable a user to create Item Types in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Item Types in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Item Types in TrakaWEB.



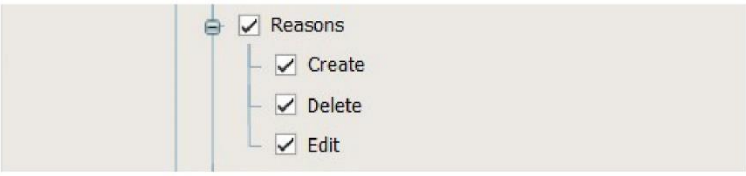
Software Settings

Notifications:

Create
Selecting this checkbox will enable a user to create Email Notifications in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Email Notifications in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Email Notifications in TrakaWEB.



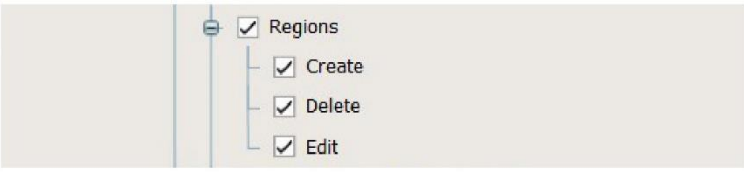
Software Settings

Reasons:

Create
Selecting this checkbox will enable a user to create Reasons in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Reasons in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Reasons in TrakaWEB.



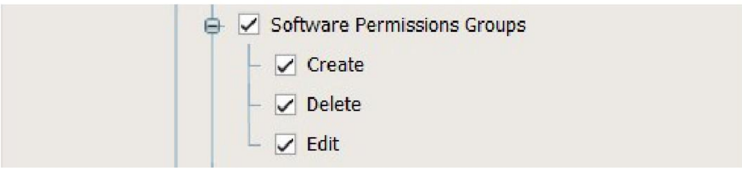
Software Settings

Regions:

Create
Selecting this checkbox will enable a user to create Regions in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Regions in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing Regions in TrakaWEB.



Software Settings

Software Permissions Groups:

Create
Selecting this checkbox will enable a user to create Software Permissions Groups in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing Software Permissions Groups in TrakaWEB.

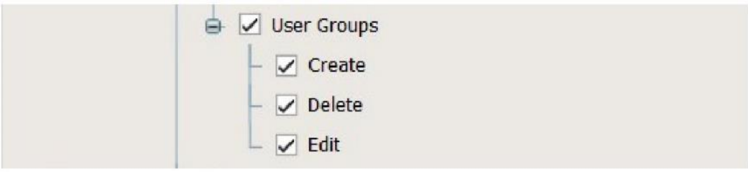
Edit
Selecting this checkbox will enable a user to edit existing Software Permissions Groups in TrakaWEB.

NOTE: The 'Edit Own User Record' option is greyed out when Unrestricted Software Item Access is unticked. This means that members of that Group will not be able to edit their own Software Group details. Therefore, they will not be able to upgrade the group to Full Admin access. For more information, please refer to UD0260 - TrakaWEB Version 4 User Guide.

Software Settings

User Fields:

Edit
Selecting this checkbox will enable a user to edit the user details on the User Fields Page in TrakaWEB.



Software Settings

User Groups:

Create
Selecting this checkbox will enable a user to create User Groups in TrakaWEB.

Delete
Selecting this checkbox will enable a user to delete existing User Groups in TrakaWEB.

Edit
Selecting this checkbox will enable a user to edit existing User Groups in TrakaWEB.

Systems:

Edit
Selecting this checkbox will enable a user to edit existing Systems in TrakaWEB.

System Viewer:

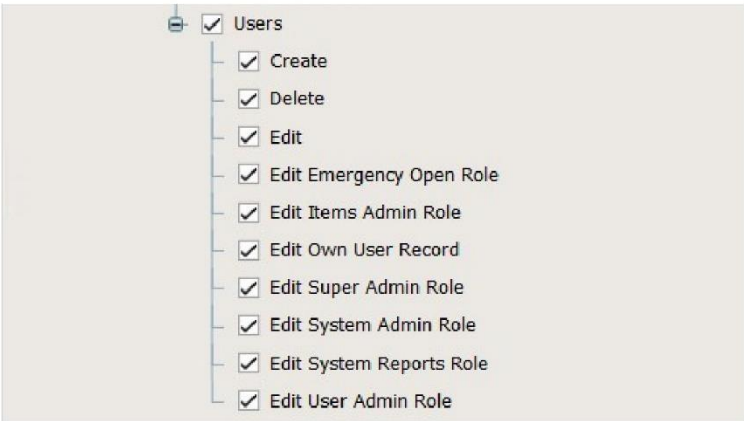
iFob Access
Selecting this checkbox will enable a user to view the iFob Access panel on the System Viewer page in TrakaWEB.

iFob Events
Selecting this checkbox will enable a user to view the iFob Activity panel on the System Viewer page in TrakaWEB.

iFob Items
Selecting this checkbox will enable a user to view the Item Activity panel on the System Viewer page in TrakaWEB.

Item Events
Selecting this checkbox will enable a user to view the Items panel on the System Viewer page in TrakaWEB.

System Events
Selecting this checkbox will enable a user to view the System Activity panel on the System Viewer page in TrakaWEB.



NOTE:

The 'Edit' option must be checked for a user to be able edit other user credentials and roles in TrakaWEB.

A user cannot edit users in Software Permissions Groups that have higher permissions than themselves.

The 'Edit Own User Record' option is greyed out when Unrestricted Software Item Access is unticked. This means that members of that Group will not be able to edit their own Software Group details.

Users:

Create
Selecting this checkbox will enable a user to create/add users to the system.

Delete
Selecting this checkbox will enable a user to delete existing users from the database.

Edit
Selecting this checkbox will enable a user to edit existing users on the database.

Edit Emergency Open Role
Selecting this checkbox will enable the user to grant other users with the Emergency Open role in TrakaWEB.

Edit Items Admin Role
Selecting this checkbox will enable the user to grant other users with the Items Admin role.

Edit Own User Record
Selecting this checkbox will enable a user to edit their own user record.

Edit Super Admin Role
Selecting this checkbox will enable a user grant other users with the Super Admin role.

Edit System Admin Role
Selecting this checkbox will enable a user to grant other users with the System Admin role.

Edit System Reports Role
Selecting this checkbox will enable a user to grant other users with the System Reports role.

Edit User Admin Role
Selecting this checkbox will enable a user to grant others with the User Admin role.

4.7.3 CREATING A RESTRICTED ADMIN ACCESS GROUP

Occasionally, you may want to grant a group with limited Admin rights. For example, you may want a Manager to be able to administrate the Items, iFobs and Groups within their department, but not have access to the assets outside of their department.

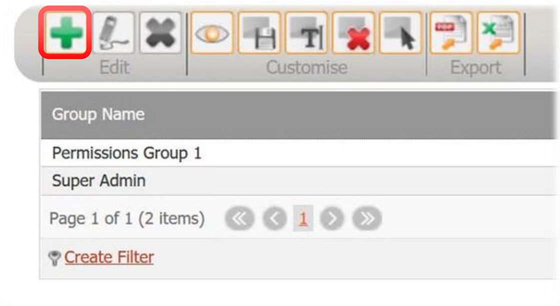
This however is not related to the functionality of Regions whereby an Administrator may only edit users that have the same or lower region set as the user they are editing. For more information on the rules applicable to Regions, please refer to the **Regions** section.

NOTE: This feature is only available in TrakaWEB 3.7.0 and above.

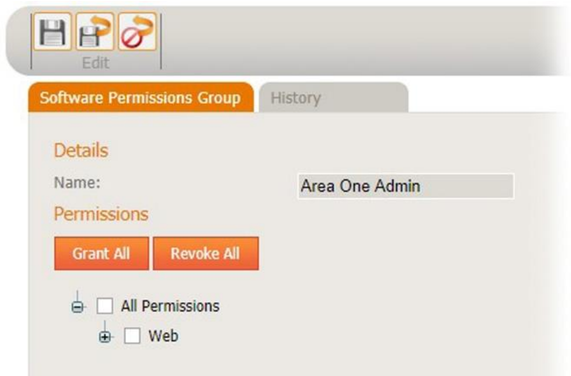
NOTE: A member of a restricted admin group cannot edit their own group, or the Super Admin group.

1. Using the Navigation Toolbar at the bottom of the page, click Software Settings, then select Software Permissions Groups.

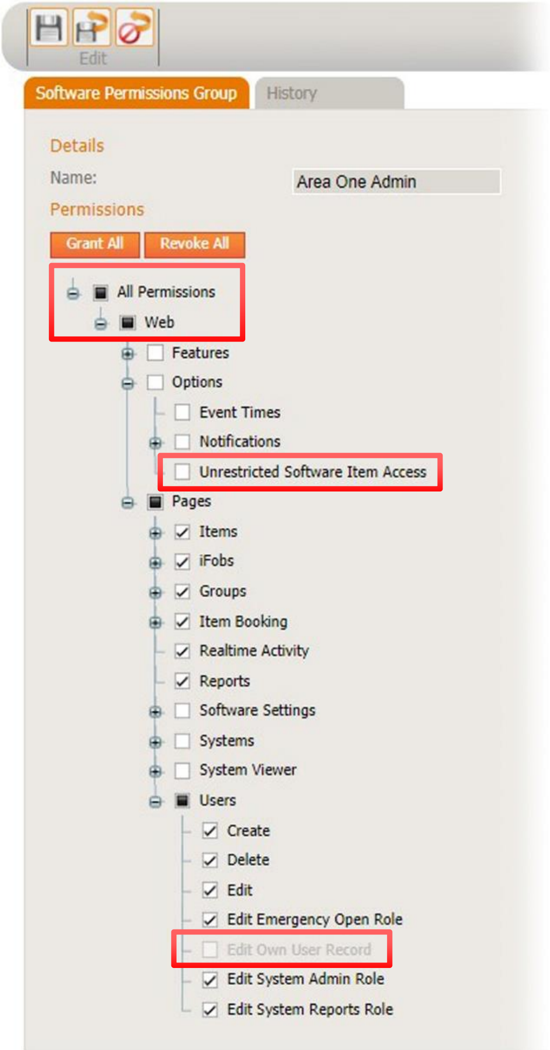
2. To create a new group, click on the Add button.



3. You will then be prompted to enter a group name.



4. Under the name field are two expandable tick boxes, one named 'All Permissions', and the other named 'Web'. You can now expand the 'Web' list and select which permissions you wish the Group to have access.



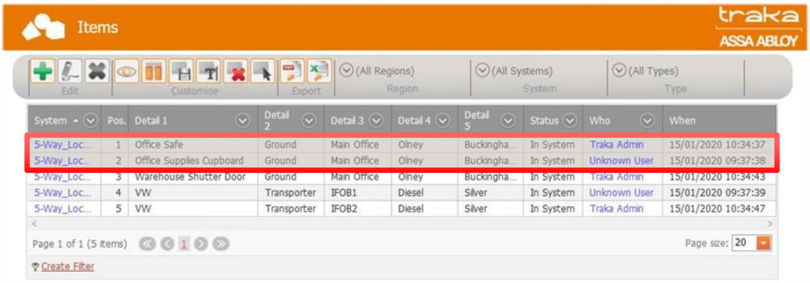
NOTE: The 'Edit Own User Record' option is greyed out when Unrestricted Software Item Access is unticked. This means that members of that Group will not be able to edit their own Software Group details. Therefore, they will not be able to upgrade the group to Full Admin access.

NOTE: If a restricted admin creates a new Item Access Group, the admin user will be automatically added to that Group, so that they are able to perform administration to it.

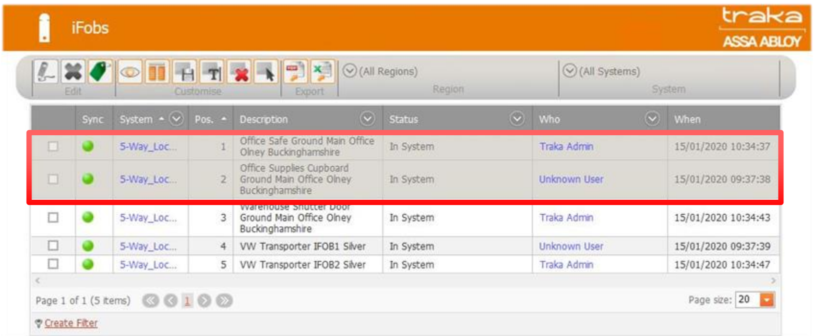
Once the group has been created, you can assign it to a user in Permission Groups.

4.7.4 RESTRICTIONS APPLIED TO UNRESTRICTED SOFTWARE ITEM ACCESS

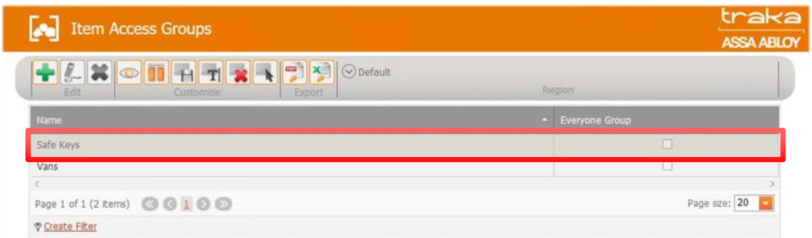
Once the restricted admin user logs into Traka Web, they will notice that when they attempt to edit an Item, iFob or Item Access Group, anything that they do not have admin rights to, will be greyed out and not available to edit.



Items

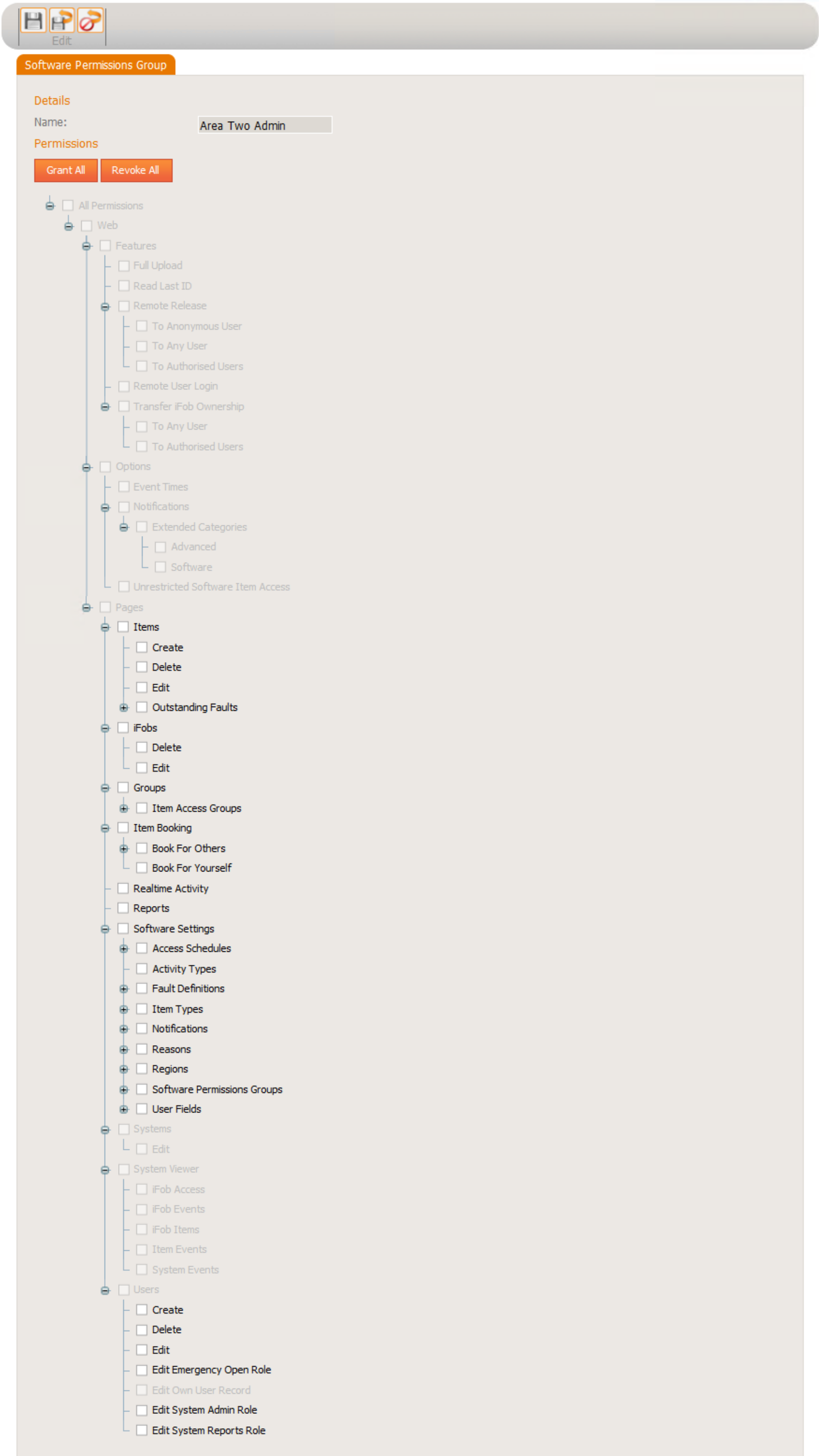


iFobs



Item Access Groups

A further security protocol set in place is that if a user is assigned to the Restricted Admin Access Group, and has been granted 'Software Permissions Groups' access, they will only be able to create a group with the same access level, or lower than their own. Any options that they do not have access to themselves, will be greyed out and will not be selectable.

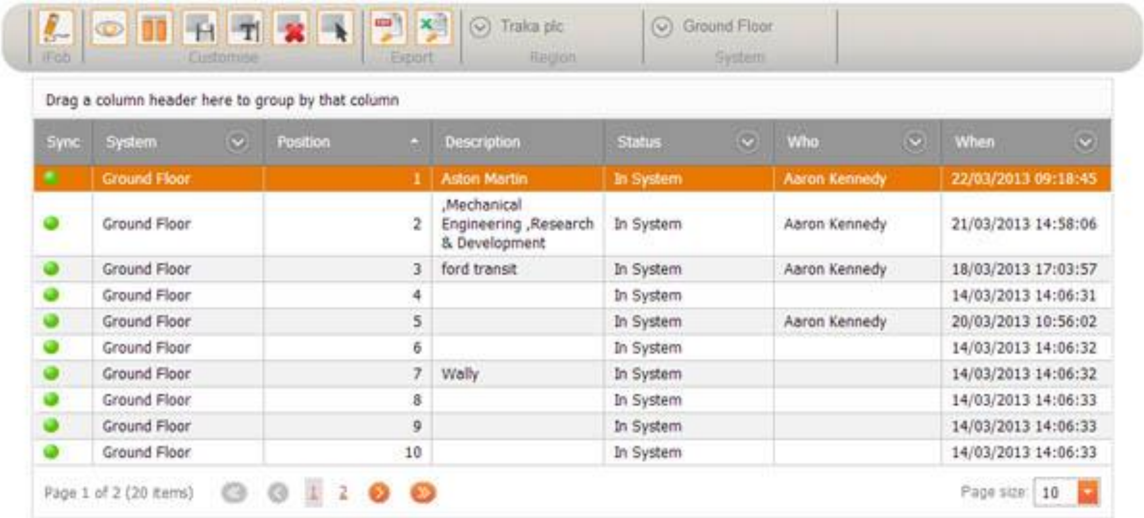


4.8 IFOBS

4.8.1 IFOB LIST

NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' in a Locker System.

From the Navigation Toolbar at the bottom of the screen click the iFob icon. You will then be taken to the iFob list. All the iFobs in your Traka Touch system will automatically synchronise when you log into TrakaWEB (providing you enabled communications from your Traka Touch system). The list shows all the iFobs that are currently in your Traka Touch system, their current status & various definable detail columns. To only view the iFob from a specific region or system you must select the appropriate filter from the Ribbon Toolbar.



Region & System Filter

When looking at the iFob list you can filter which iFobs you wish to view by defining the Region the system belongs to, and the system the iFob belongs to. Clicking the small arrow button next to each field will show you a list of selectable systems & regions (providing that your database has more than one region and system). For more information, see the Regions and Systems topics.

Sync Column

The status of the iFob is defined by a graphic next to the iFob description. If the status image is green then all events from the iFob are up-to-date and have been read back to TrakaWEB. If the events from the iFob have not been read back from the Traka Touch system then the image will turn red.

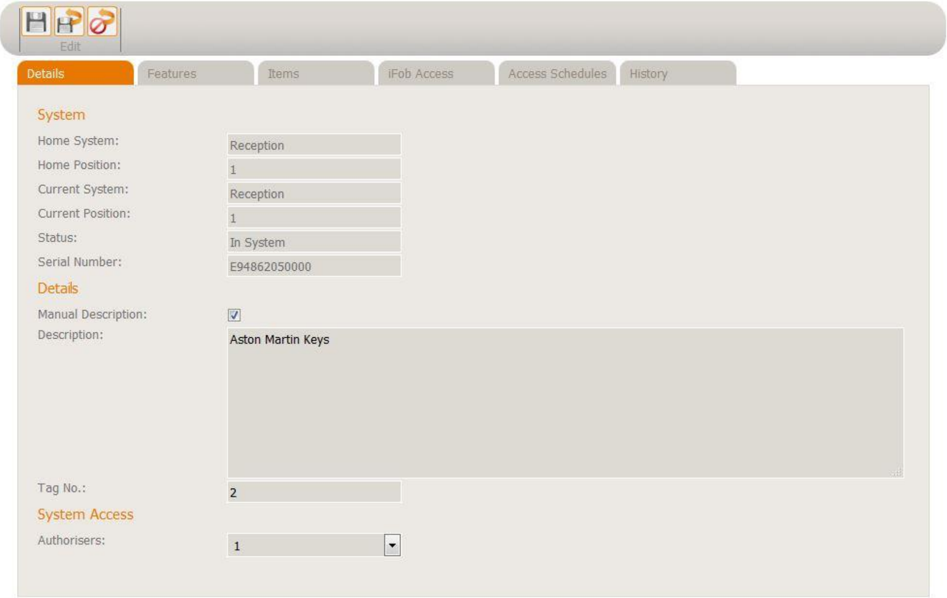
Show/Hide Grid Columns

Throughout TrakaWEB, there are many grids that display important information for the page you are currently viewing. For example, the Users page has the Users List Grid, which displays all of the users within the database. The Show/Hide Grid Columns button allows you to add or remove fields/columns of your choice to the grid. Every grid is different and will provide additional fields. The User list will allow you to add any or all of the eleven user detail fields.

4.8.2 IFOB DETAILS

NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' in a Locker System.

The details tab displays a range of information for the selected iFob, including the iFob description and the system the iFob belongs to. These are listed in more detail below.



System

System
Displays the name of the system the iFob belongs to.

Position
Displays the position in which the iFob is located in the system.

Status
This field will show the status of the iFob e.g. Out of the System.

Details

Manual Description
Check this box to enable the description field below. If this box is unchecked then the description from an assigned item to that iFob can be used. Refer to 'iFob Description Order' in the Adding New Item Types section for more information.

Description
Here you can view the iFob description. This can be automatically generated by the item details, or you can change the description by checking the Manual Description tick box above and entering manually.

System Access

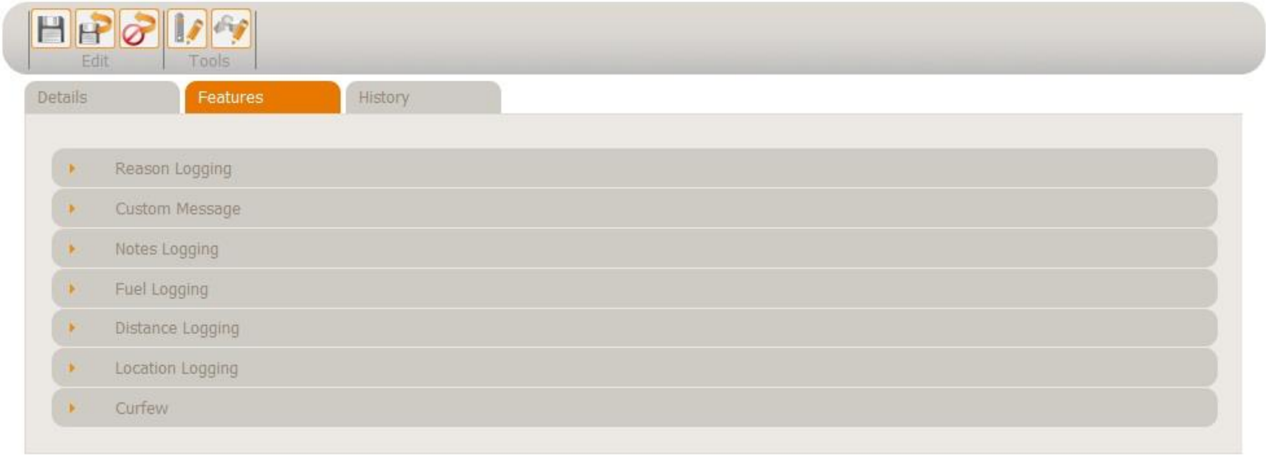
Tag No
This section allows you to enter a tag number for the iFob position.

Authorisers
From this drop down selection box, you can choose how many users are required to authorise the release of this iFob/item.

Features

The features tab allows you to switch any pre-enabled options on or off. From here, you can also set item curfews.

For more information on Features, please refer to the Feature Options sections of this document.

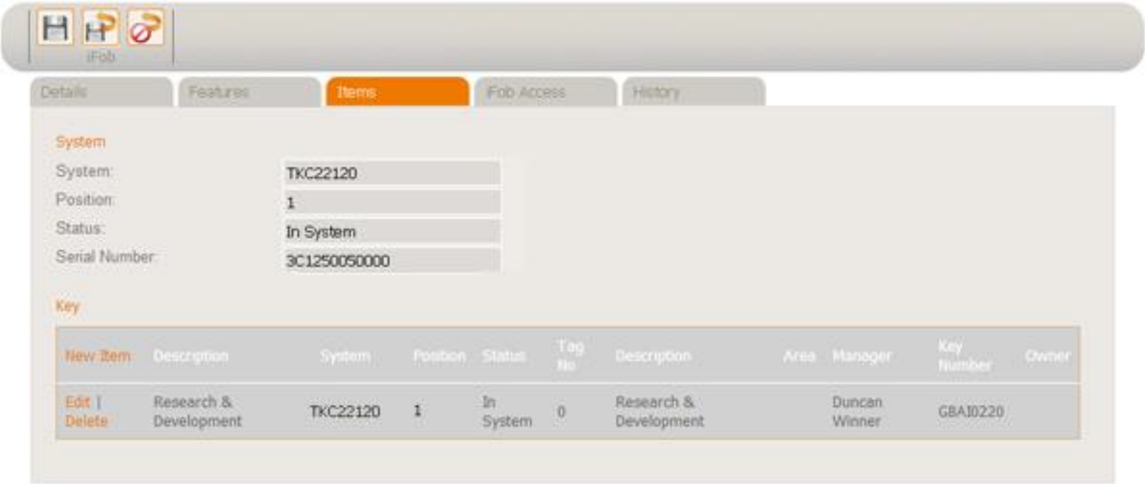


Curfew Value

Curfew Type
Curfews are a non-cost option built into TrakaWEB and are used to reduce the amount of time an item is out of the system, or how long a user can have an item in their possession. Please view the Curfew Topic for more details.

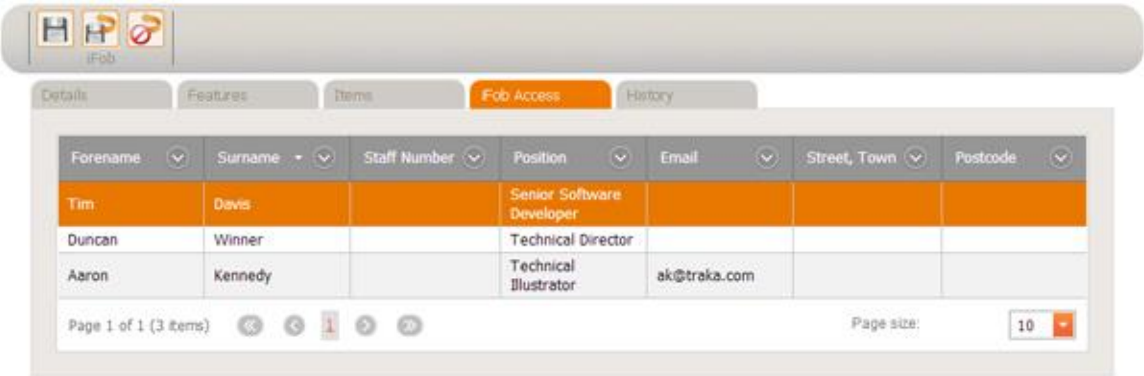
Items

The items tab has information on the items attached to the iFob, the system the item belongs to, and the serial number of the iFob the item is assigned to etc. You can delete the item from the iFob by clicking Delete or edit the item by clicking Edit. To create a new item you can simply click New Item.



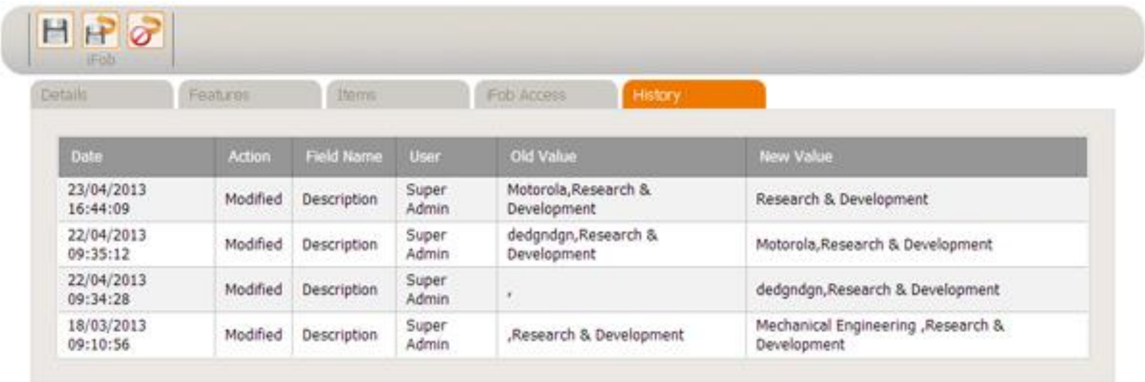
iFob Access

This tab shows a list of users who currently have access to the selected iFob.



History

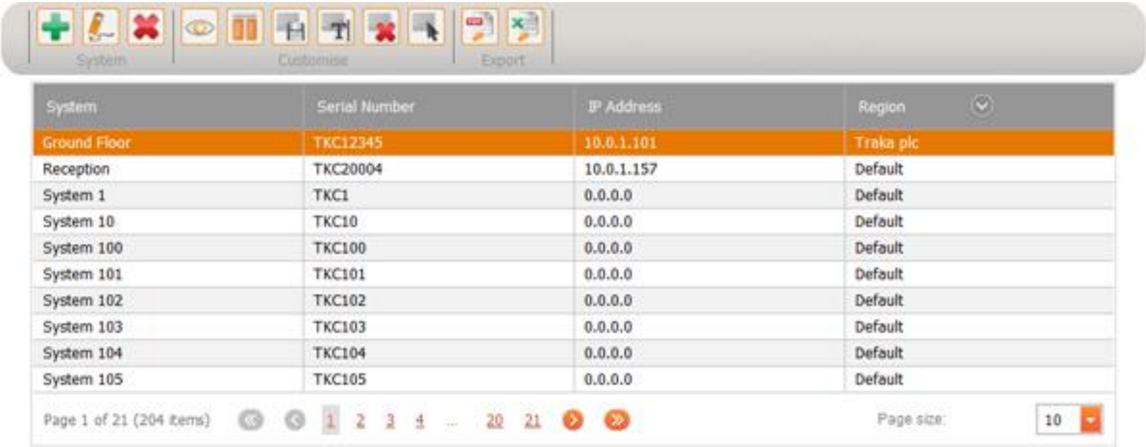
The History tab will show you a record of when the item was added, who by, what the name of the item is and if it has been changed.



4.9 SYSTEMS

4.9.1 SYSTEMS

From here, you can view or edit the systems you currently have in the database.



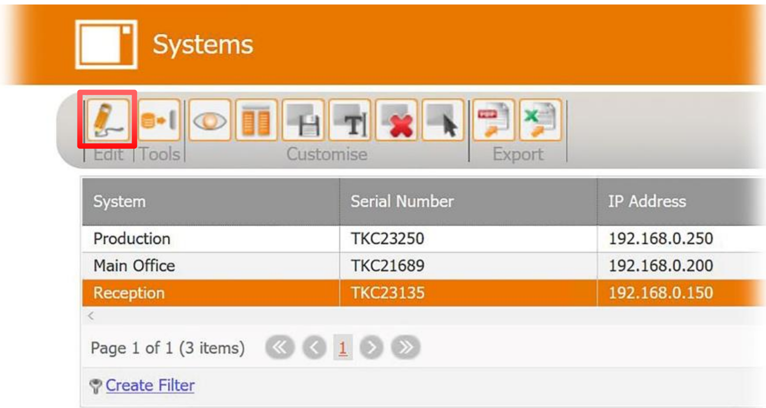
Show/Hide Grid Columns

Throughout TrakaWEB, there are many grids that display important information for the page you are currently viewing. For example, the Users' page has the Users' List Grid, which displays all of the users within the database. The Show/Hide Grid Columns button allows you to add or remove fields/columns of your choice to the grid. Every grid is different and will give different fields to add to the grid. The User list will allow you to add any or all of the eleven user detail fields.

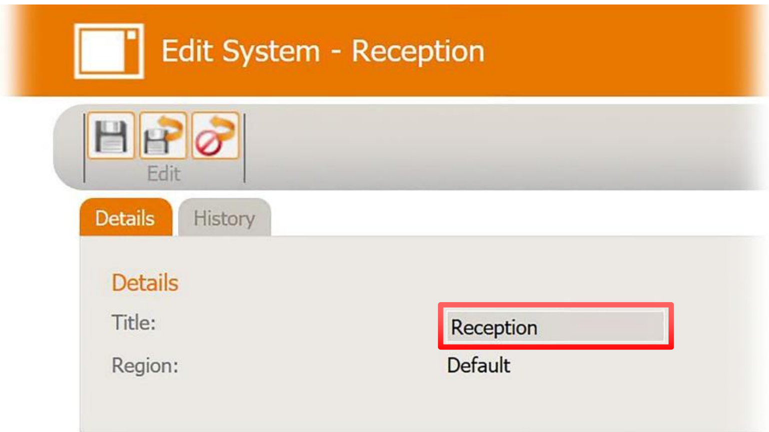
4.9.2 EDITING A SYSTEM

1. From the Navigation Toolbar, select the **Systems** icon.

2. You will then be taken to the **Systems** page. Select the system you wish to change and click the **Edit** button.



3. The **Edit System** page allows you to change the name of the system it belongs to.



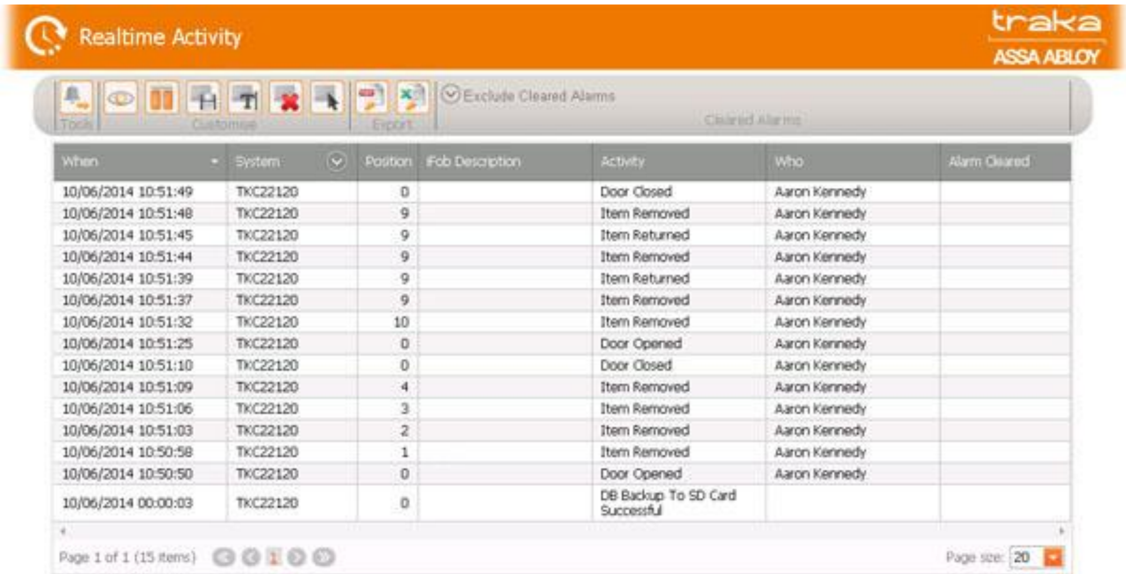
4. Once the change has been made, click the **Save and Return** button to be taken back to the systems list.

4.10 REALTIME ACTIVITY

The Realtime Activity Grid allows you to view up to 24 hours' worth of activities and alarms that transpire at the Traka Touch system. From here, you can view who triggered the activity, the date and time it occurred, the system the activity took place, the position in the system the activity affected (if any) etc.

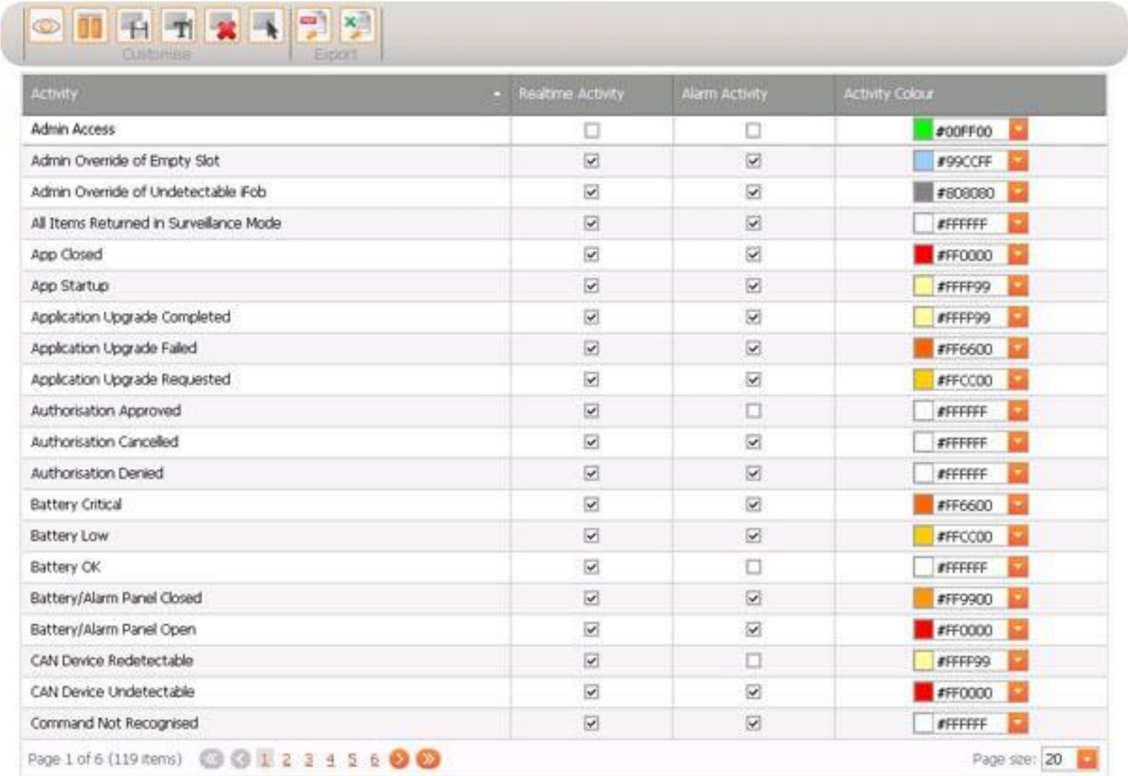
You cannot remove any activities from this grid manually and after 24 hours the list will update and show the most recent activities. You can view the history of activities that took place by running a General > Activity Report.

The customise tools in the ribbon toolbar will allow you to search the grid for information, add columns to the grid and create, edit and delete layouts. Please review the ribbon toolbar topic for more details.



To view the full list of activities, select the Software Settings button from the Navigation Toolbar and click the Activity Types button as shown below.

This will display all the activity types that exist within the Traka Touch system.



Activity	Realtime Activity	Alarm Activity	Activity Colour
Admin Access	☐	☐	#00FF00
Admin Override of Empty Slot	☑	☑	#99CCFF
Admin Override of Undetectable Fob	☑	☑	#808080
All Items Returned in Surveillance Mode	☑	☑	#FFFFFF
App Closed	☑	☑	#FF0000
App Startup	☑	☑	#FFFF99
Application Upgrade Completed	☑	☑	#FFFF99
Application Upgrade Failed	☑	☑	#FF6600
Application Upgrade Requested	☑	☑	#FFCC00
Authorisation Approved	☑	☐	#FFFFFF
Authorisation Cancelled	☑	☑	#FFFFFF
Authorisation Denied	☑	☑	#FFFFFF
Battery Critical	☑	☑	#FF6600
Battery Low	☑	☑	#FFCC00
Battery OK	☑	☐	#FFFFFF
Battery/Alarm Panel Closed	☑	☑	#FF9900
Battery/Alarm Panel Open	☑	☑	#FF0000
CAN Device Redetectable	☑	☐	#FFFF99
CAN Device Undetectable	☑	☑	#FF0000
Command Not Recognised	☑	☑	#FFFFFF

The column to the right of the activity name is the Realtime Activity check box. When ticked, the corresponding activity will appear in the activity grid when triggered at the Traka Touch system.

Creating Alarms

Activities can be turned into alarms by checking the Alarm Activity box. This will allow you to assign a colour to the activity via the colour column. Simply select a colour from the drop down selection box, or enter a hexadecimal value of your choice to achieve the exact colour required.

When the activity is triggered at the system, it will appear in the activity grid as an alarm. The alarm will be highlighted with the colour you assigned to it.

When	System	Position	Fob Description	Activity	Who	Alarm Cleared
10/06/2014 10:55:36	TKC22120	0		Admin Access	Aaron Kennedy	☐
10/06/2014 10:51:49	TKC22120	0		Door Closed	Aaron Kennedy	
10/06/2014 10:51:48	TKC22120	9		Item Removed	Aaron Kennedy	
10/06/2014 10:51:45	TKC22120	9		Item Returned	Aaron Kennedy	

Clearing Alarms

To clear an alarm from the grid, simply click the alarm cleared check box. If you have multiple alarms listed in the grid, you can select the clear all alarms button (shown below) from the ribbon toolbar.

You can view all the alarms you have cleared by selecting 'Include Cleared Alarms' from the drop down selection box on the ribbon toolbar. The alarms will still be marked as cleared but they will now be visible again on the activity grid.

Alarms that have been cleared can be viewed in the Exception > Alarms Report.

4.11 AUTHORISER

Authoriser is a standard option within TrakaWEB and Traka Touch. It can be assigned to a User in a situation where an elevated level of security is required. When a User requests a specific Item/iFob from the system, another User with the Authoriser role will also be required to access the system with their ID prior to the Item/iFob being released. Authorisation is applied to items or iFobs and up to three Authorisers may be assigned per Item/iFob.

There is also an option whereby a user with the Authoriser role must be in a different User Group to the person requesting the Item/iFob but will not be permitted to remove an item themselves. Whilst setting up a User with the Authoriser role, they can be assigned with an override option. This will enable them to remove specific Items/iFobs without requiring Authorisation for themselves.

NOTE: A system with non-locking receptor strips will release an item without prompting authorisation.

The Authoriser role can also be setup within Traka Touch. For more information on the Traka Touch process for Authorisation, please refer to **UD0011 – Traka Touch User Guide.**

4.11.1 ASSIGNING A USER WITH THE AUTHORISER ROLE

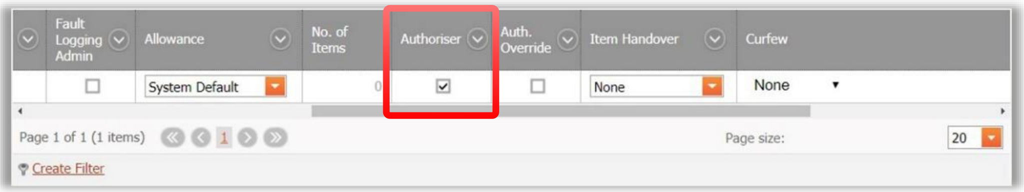
1. Access the User list by selecting the User icon from the Navigation toolbar.

If you already have users set up in your Traka Touch system, then this list will be populated with all of those users along with all the other users in the database. If you have not added any users to your system, you will need to Add Users.

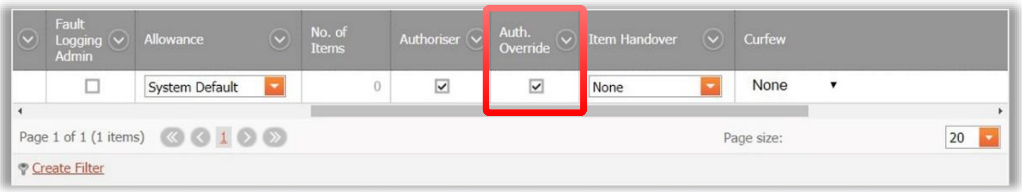
2. Select a User to edit and then navigate to the System Access tab.

The option for assigning a user with the Authoriser role is located on the System Access Grid.

3. Click in the **Authoriser** check box to assign the selected user as an Authoriser.



4. If the selected User is also to have the Authoriser Override role, click in the **Auth. Override** check box.

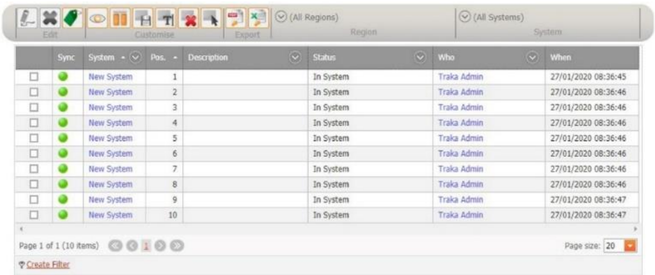


5. Once completed, click **Save & Return**.

4.11.2 SELECTING ITEMS THAT REQUIRE AUTHORISERS

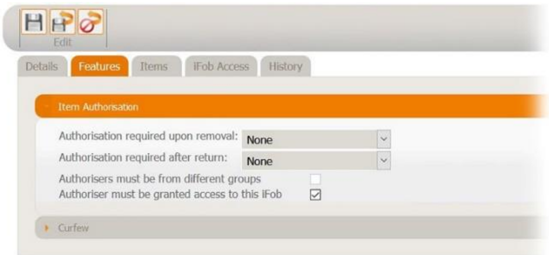
1. Select the iFob icon from the Navigation Toolbar.

2. Double click to select an iFob from the list.



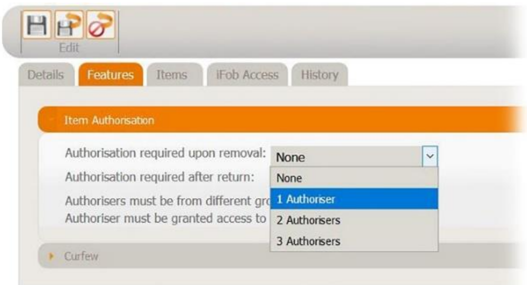
You will now be taken to the Edit iFobs page.

3. From the Edit iFob Details page, select the **Features** tab and then expand the **Item Authorisation** panel.



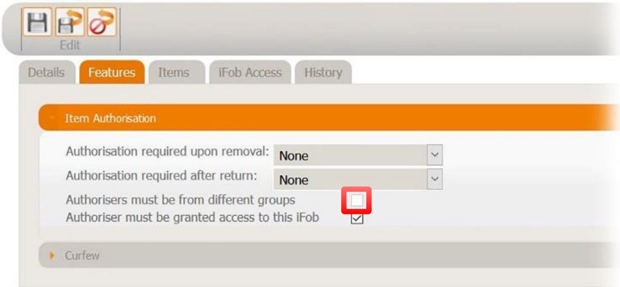
You will notice two drop-down boxes. One for **Authorisation required upon removal** and one for **Authorisation required after return.**

4. Select the **Authorisation required upon removal** drop-down and assign the required number of Authorisers.

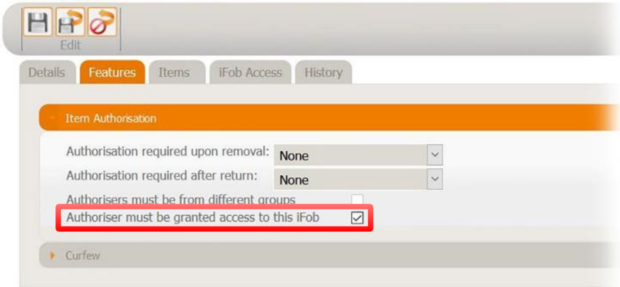


5. Select the **Authorisation required after return** drop-down and assign the required number of Authorisers.

The **Authorisers must be from different groups** checkbox will remain unticked as it only applies to Authorisers from different groups and so is not required for standard Authorisation.



Another check box is also available; **Authoriser must be granted access to this iFob.**

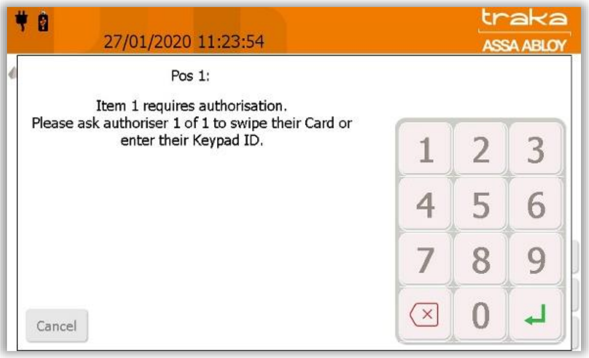


With this check box ticked, Authorisers can only grant authorisation on iFobs that they have access to.

6. Once complete, click on **Save & Return**.

4.11.3 TAKING ITEMS/IFOBS

A user may access the system using their Keypad ID, Swipe Card or Fingerprint to remove an Item. However, if the Item they wish to take requires Authorisation, a message will request that they ask an Authoriser to access the system first.



NOTE: If the user has the Auth. Override enabled, they will be able to remove any Items/iFobs that have been assigned the Authoriser requirement.

For more information on the Traka Touch procedures for removing Items/iFobs, please refer to **UD0011 – Traka Touch User Guide.**

4.12 AUTHORISER FROM A DIFFERENT GROUP ON REMOVAL & RETURN

In certain work environments, particularly Casinos, a rule maybe enforced that requires the Authoriser be from another department or 'User Group'.

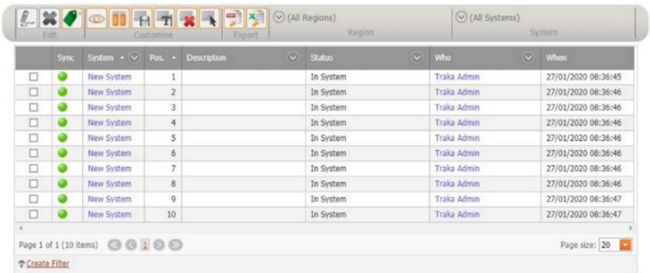
As TrakaWEB will be required for associating a User to a User Group, this option will not be available for standalone systems.

Clicking a check box will enable Authorisers from different groups. This will not be available if the Traka Touch App version does not support this functionality.

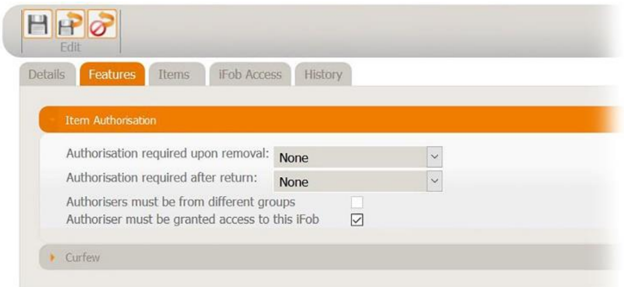
This option is compatible with FRSS & RRSS Key Cabinets and RFID Locker Systems.

4.12.1 ENABLING THE OPTION

1. From the iFob screen, select the Item/iFob to which you wish to apply the authorisation.

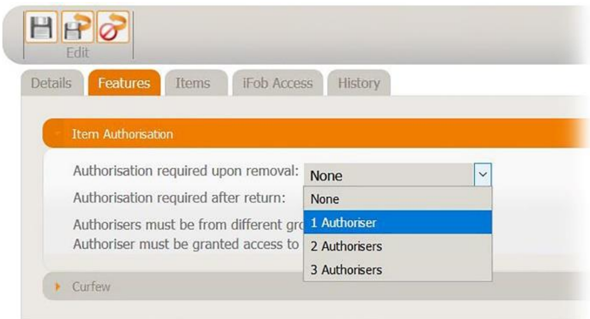


2. From the Edit iFob Details page, select the **Features** tab and then expand the **Item Authorisation** panel.



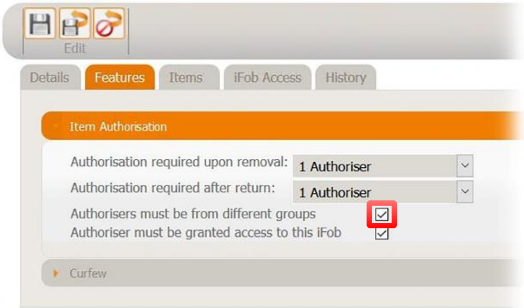
You will notice two drop-down boxes. One for **Authorisation required upon removal** and one for **Authorisation required after return.**

3. Select the **Authorisation required upon removal** drop-down and assign the required number of Authorisers.



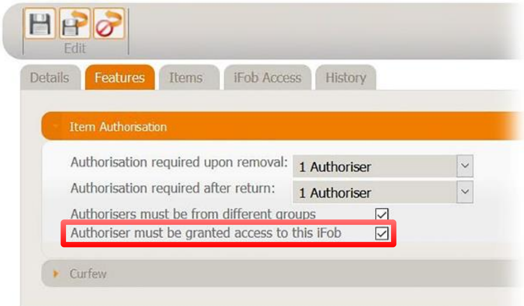
6. Select the **Authorisation required after return** drop-down and assign the required number of Authorisers.

After selection, the checkbox for **Authorisers must be from different groups** will now be available. Place a tick in the box.



NOTE: It is important that this check box is ticked; otherwise, the functionality will not be available for authorisers from different groups.

Another check box is also available; **Authoriser must be granted access to this iFob.**



With this check box ticked, Authorisers can only grant authorisation on iFobs that they have access to.

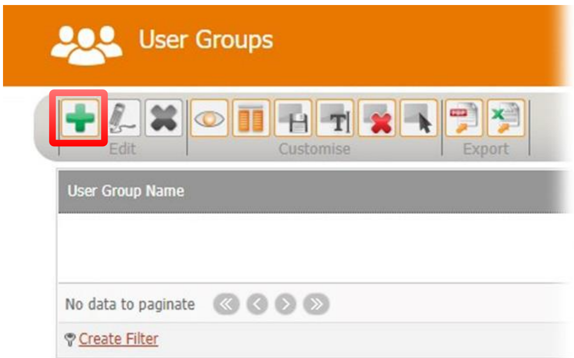
7. Once complete, click on **Save & Return**.

4.12.2 CREATING USER GROUPS

The next stage in the process of enabling an authoriser from a different group is to create a new User Group for users and Authorisers.

1. From Software Settings on the Navigation Toolbar, select the User Groups icon.

2. At the User Groups page, click on the Create button to create a new group.



3. At the next page, you will be required to enter a name for the new group.

4. Once completed, click on **Save & Return** and you will see the new group on the User Groups page.

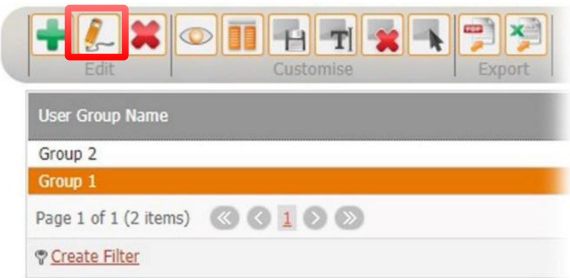
NOTE: You must create at least two groups as depending on how many Authorisers are required, they must each be in a different group to the user requiring the Item/iFob.

4.12.3 EDITING USER GROUPS

Should you need to change the name of an existing User Group, it can be edited.

1. Select User Groups from Software Settings on the Navigation Toolbar.

2. Select the group to edit and then click on the Edit button.



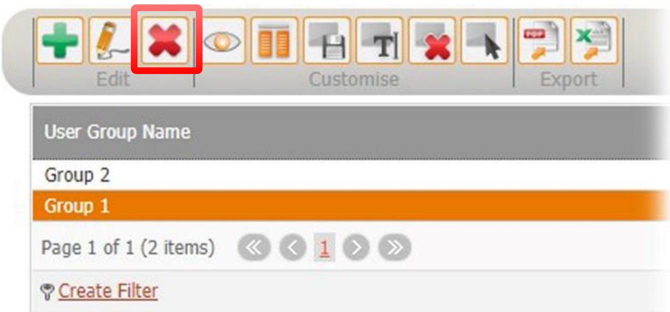
3. Edit the name of the User Group and then click on **Save & Return**.

4.12.4 DELETING A USER GROUP

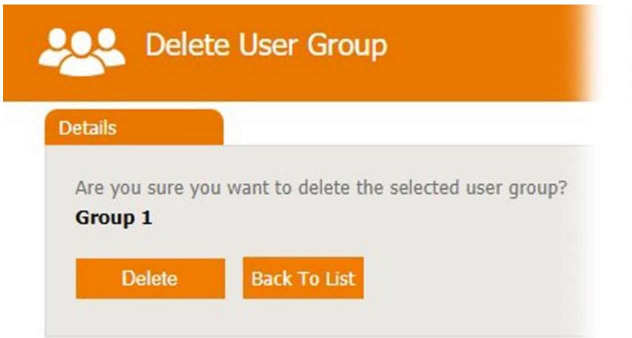
Providing there are no Users assigned to it, the group may be deleted if it is no longer required.

1. Select User Groups from Software Settings on the Navigation Toolbar.

2. Select the User Group to delete and then click on the Delete button.



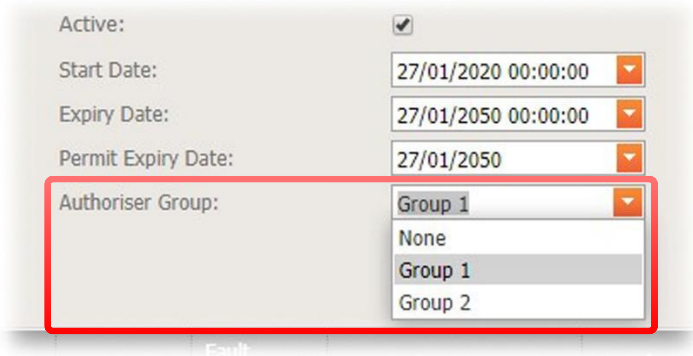
You will then be required to confirm that you wish to delete the selected group. Selecting the **Delete** button will remove it and selecting **Back to List** will return to the list of User Groups.



4.12.5 ASSIGNING USERS TO USER GROUPS

After the required User Groups have been created, you can then assign Users to them. In the following example, two Groups have been created. One group for the User taking the taking the Item/iFob and a second group for the Authoriser. Selecting **None** will prevent the user from accessing any items that require authorisation.

1. From the Users list, double click on a User to edit them.
2. From the System Access tab, locate the **Authoriser Group** dropdown menu.
3. From the dropdown menu, select a User Group to assign the selected User.



4. Repeat the above process to assign the authoriser to a different User Group.
5. Once completed, click on Save & Return.

4.12.6 REMOVING & RETURNING ITEMS

NOTE: The user must be assigned to a User Group or they will not be able to remove or return items that require authorisation.

NOTE: The Authoriser must be assigned to a User Group or they will not be able to provide the required assistance to release or return an Item/iFob.

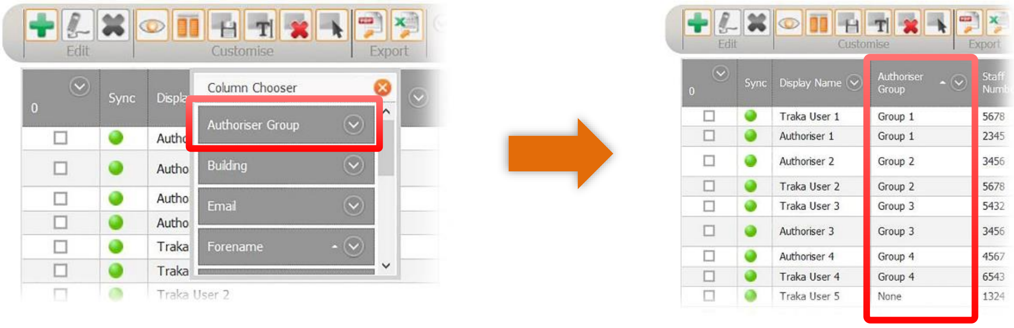
For more information on Using Traka Touch with **Authoriser from a Different Group,** please refer to **UD0011 – Traka Touch User Guide.**

4.12.7 AUTHORISER GROUP COLUMN

An additional column may be added to the User page. This will enable you to view which users are in which group. For clarity, this column may also be filtered if there are many users on the system.

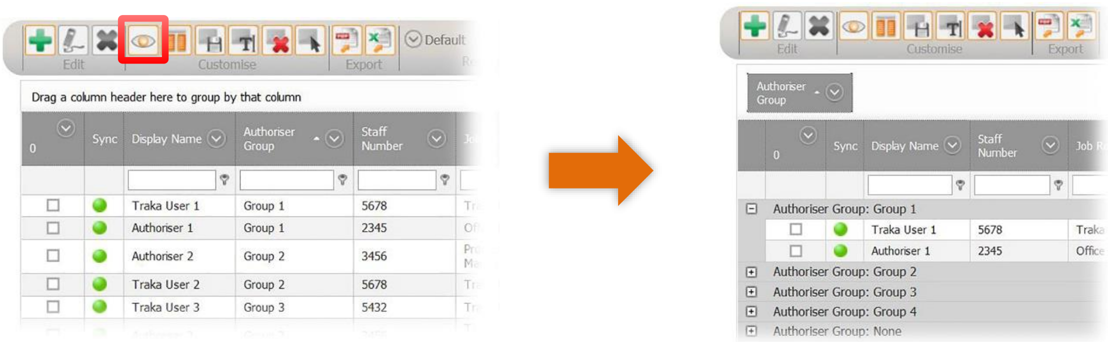
1. Navigate to the Users page and select **Show/Hide Grid Columns** from the ribbon toolbar.

2. From the Column Chooser, click and drag the **Authoriser Group** option to a position on the grid.



The **Authoriser Group Column** will display all the available User Groups and the users that are associated with them. Using the down arrow at the top of the column it is possible to filter which users are associated with individual User Groups.

By selecting the 'eye' icon on the ribbon toolbar, the user groups may also be grouped. This way, you can expand the group list and view the user details for the Authoriser Group.

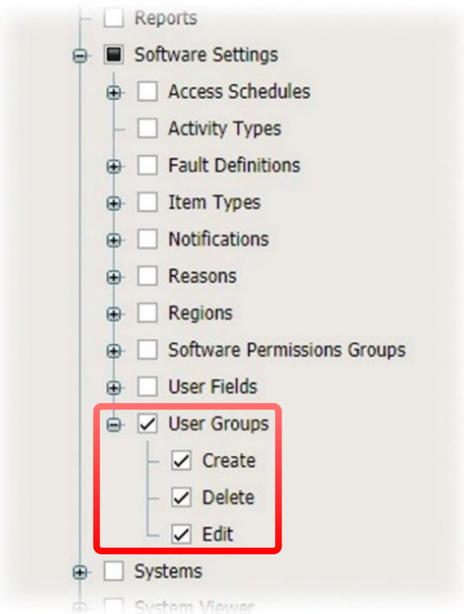


4.12.8 SOFTWARE PERMISSIONS

A Software Permissions category is provided within Software Permission Groups with Create, Edit and Delete permissions.

1. From Software Settings on the Navigation Toolbar, Select the Software Permissions Groups icon.

2. From within the Software Settings tree, locate User Groups. From here, you can allocate the Create, Delete and Edit permissions.



3. Once completed, click on **Save & Return**.

4.12.9 AUDITING

A user with the User Groups Edit permission enabled will be able to access the History tab. Here, an audit trail for the User Group's history and Item Access Group history is visible and any changes made, such as additions, updates or deletions may be viewed.

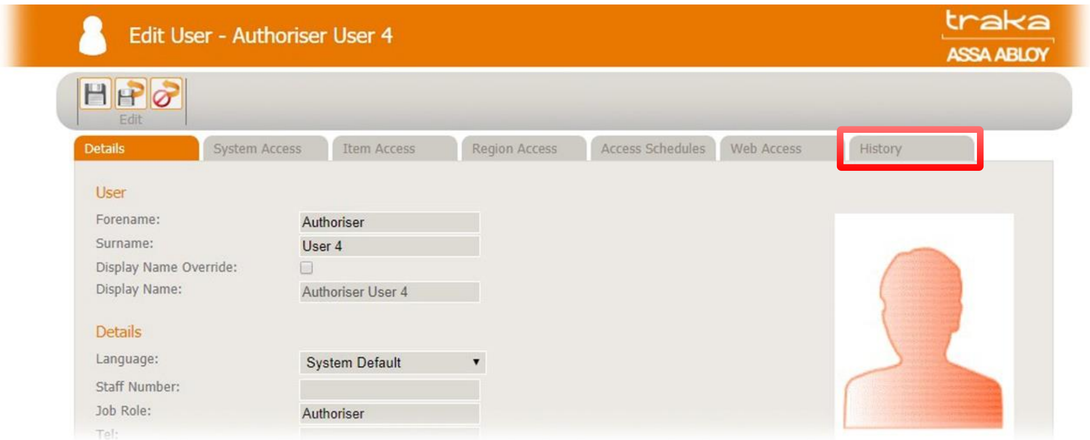
User

To access the audit data for users:

1. Navigate to the Users Page.
2. Double click on the required user.

You will now be taken to the Edit User page for that user.

3. Click on the History tab.

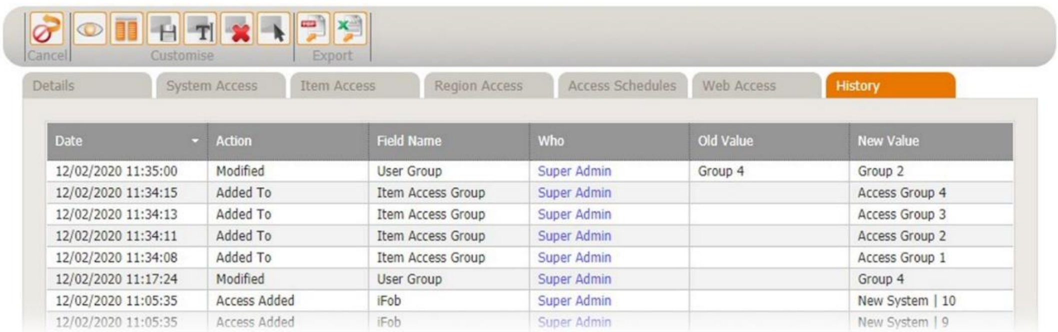


The history page will display the audit information for that user as shown in the example below.

The **Old Value** and **New Value** columns show any changes that have occurred such as a user being moved out of an existing group (Old Value) and into another (New Value).

iFob information is divided into three segments and divided by a pipe character:

Home System | Home Position | iFob Description (if present)



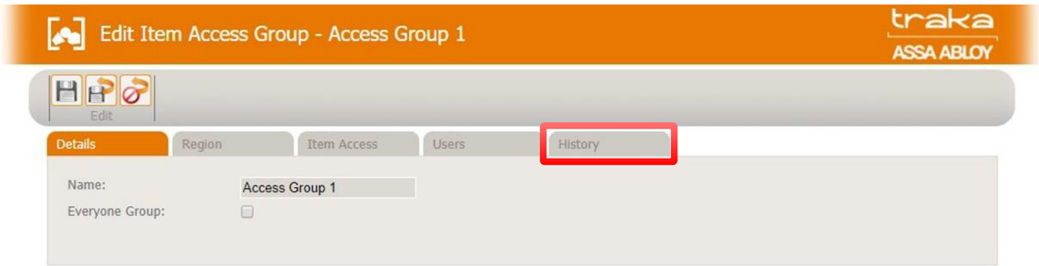
Item Access Groups

To access the audit data for Item Access Groups:

1. Navigate to the Item Access Groups page.
2. Double click on the required Item Access group.

You will now be taken to the Edit Item Access Group page for the selected Item Access Group.

3. Click on the History tab.

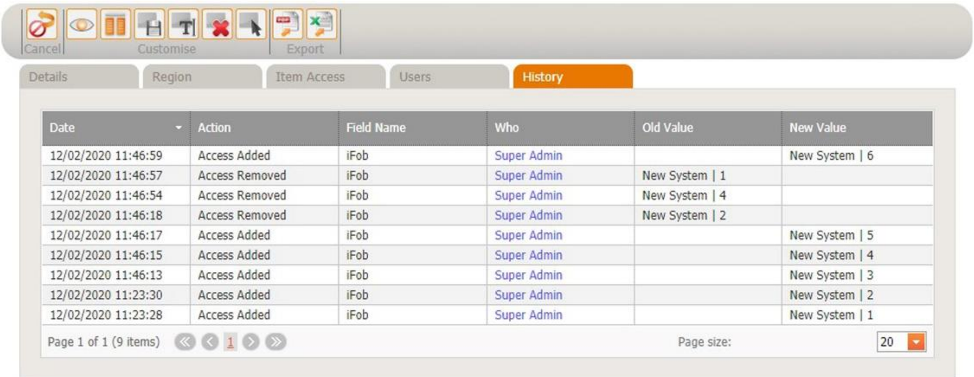


The history page will display the audit information for that Item Access Group as shown in the example below.

The **Old Value** and **New Value** columns show any changes that have occurred such as access being revoked to a group (Old Value) and granted to another (New Value). This creates a record for each iFob.

iFob information is divided into three segments and divided by a pipe character:

Home System | Home Position | iFob Description (if present)



Date	Action	Field Name	Who	Old Value	New Value
12/02/2020 11:46:59	Access Added	iFob	Super Admin		New System | 6
12/02/2020 11:46:57	Access Removed	iFob	Super Admin	New System | 1	
12/02/2020 11:46:54	Access Removed	iFob	Super Admin	New System | 4	
12/02/2020 11:46:18	Access Removed	iFob	Super Admin	New System | 2	
12/02/2020 11:46:17	Access Added	iFob	Super Admin		New System | 5
12/02/2020 11:46:15	Access Added	iFob	Super Admin		New System | 4
12/02/2020 11:46:13	Access Added	iFob	Super Admin		New System | 3
12/02/2020 11:23:30	Access Added	iFob	Super Admin		New System | 2
12/02/2020 11:23:28	Access Added	iFob	Super Admin		New System | 1

Page 1 of 1 (9 items) 1 Page size: 20

Curfews are a non-cost option built into TrakaWEB and Traka Touch and are used to reduce the amount of time an item is out of the system, or how long a user can have an item in their possession. There are two different types of curfew, Relative & Absolute. You can set these curfews against both users and items. This is a very useful feature within businesses that have shift patterns and users taking many items from various systems, as it will highlight if items are not returned to the system by the end of a user's shift.

NOTE: For more information regarding Curfews and Traka Touch, refer to UD0011 – Traka Touch User Guide.

Status Icons & Activity

Any items out under curfew or overdue will be shown on the system viewer and will be kept up to date as often as TrakaWEB communicates with the Traka Touch system(s).

- When this icon is displayed, the item is currently out under a curfew.

- When this icon is displayed, the item is out under a curfew and is overdue.

You will also see an activity generated on overdue items in the Activity Grid.

4.13.1.1 USER CURFEWS

Curfew Types

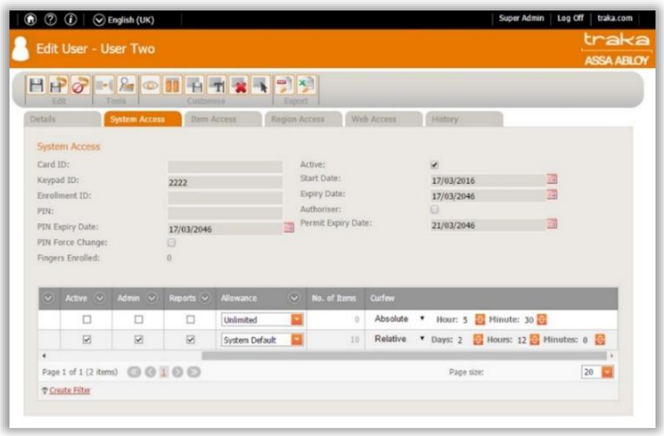
Absolute
This curfew allows you to set a time by which all the users' items should be returned. For example, if you set the curfew to 17:30, all items taken by the user before this time will become overdue if not returned by 17:30.

Relative
This curfew allows you to set a length of time for which the all the users' items may be out of the system. This time limit is set in multiples of Days, Hours and Minutes to a maximum of 365 days, 23 hours and 59 minutes. Thus, if you expect the item to be returned within 1 hour, you should complete the curfew accordingly. If the item is not returned within 1 hour, an activity will be generated and displayed in the Activity Grid.

Setting up a User Curfew

1. To set a user curfew highlight the desired user from the user list and select the Edit button.

2. Select the System Access tab. The grid at the bottom contains a column named Curfew Value. Using the drop-down box, select the type of curfew required against the system you wish the curfew to apply and the time or number of days, hours and minutes (depending on the curfew type).



3. Once you have completed the curfew select one of the Save options at the top of the window.

Curfew Types

Absolute
This curfew allows you to set a time by which an item should be returned. For example, if you set the curfew to 17:30, the item will become overdue if not returned by 17:30. If the item is removed after 17:30 it must be returned by 17:30 the following day.

Relative
This curfew allows you to set a length of time for which an item may be out of the system. This time limit is set in multiples of Days, Hours and Minutes to a maximum of 365 days, 23 hours and 59 minutes.

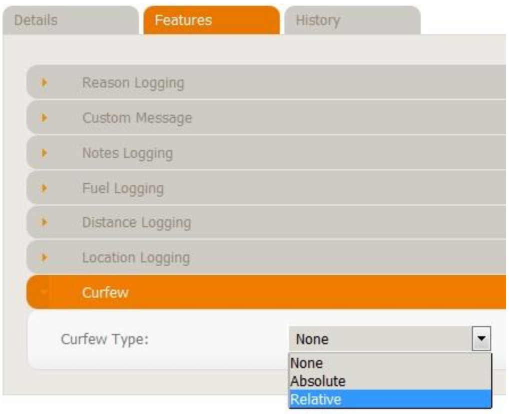
Setting up an iFob Curfew

NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' attached to the asset inside a Locker Compartment.

1. To set an iFob curfew, highlight the desired position from the system viewer and select the edit iFob button. Alternatively, you can select the iFob icon from the navigation toolbar, then from the iFob list highlight the desired iFob and select the edit iFob button.

2. The iFob details will then appear. Navigate to the Features tab.

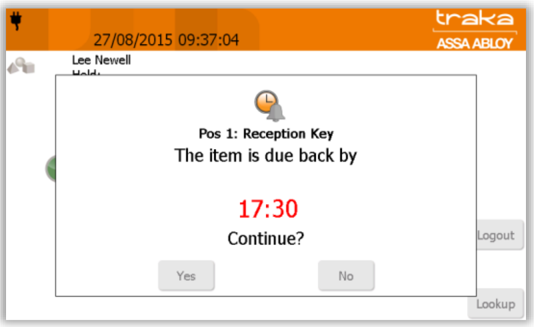
3. At the bottom of the window, you will notice the curfew fields. From the drop down box, select which type of curfew you wish to set e.g. Absolute or Relative, then set the desired time or number of days, hours and minutes (depending on the curfew type).



4. Once you have completed the curfew, select one of the Save options at the top of the window.

Traka Touch

1. When a user accesses the Traka Touch System and attempts to remove an item, they will be presented with a message similar the following.



2. Clicking 'Yes' will release the item.

NOTE: By selecting 'Yes', the user accepts that the item must be back in the system by the time stated in the message.

3. Remove the item from the system.

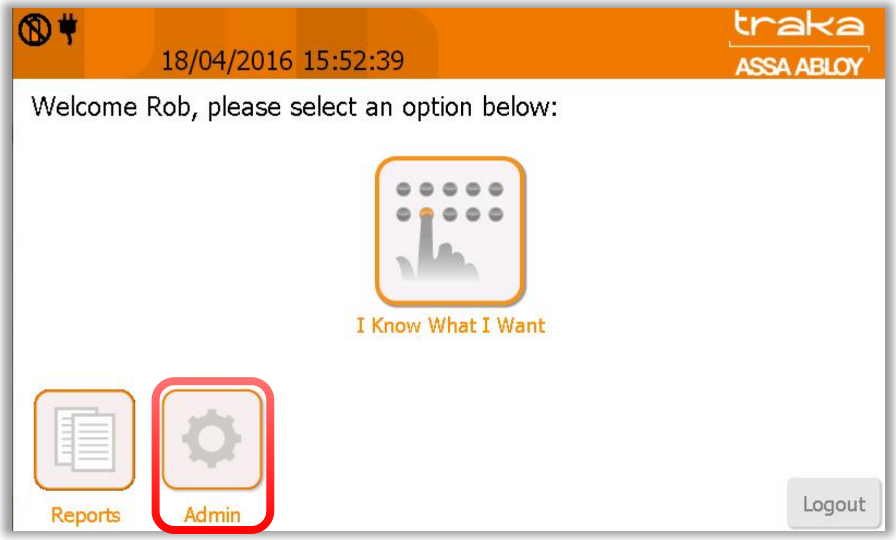
The item is now under curfew and will become overdue if it is not returned to the system by the stated time.

4.13.2 SETTING UP CURFEWS IN TRAKA TOUCH

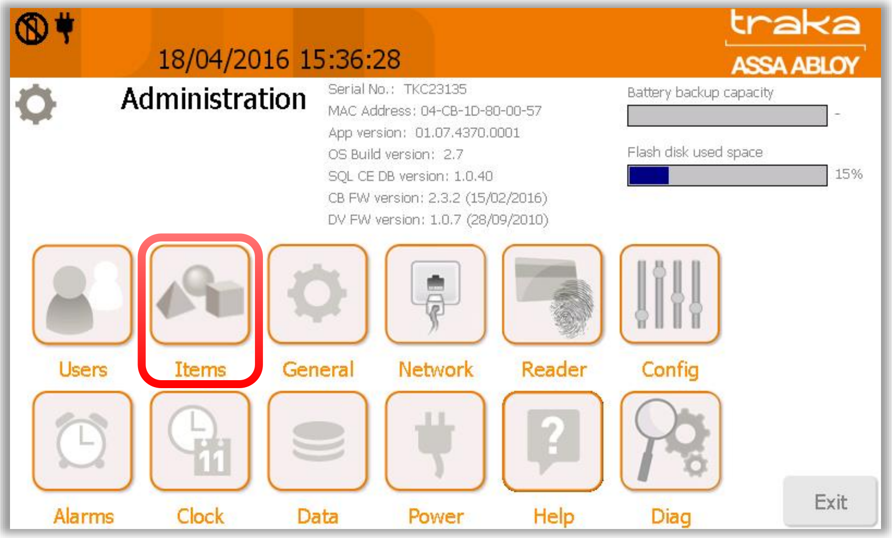
The functionality of TrakaWEB Curfews can also be applied to the Traka Touch System. As with 'Absolute' and 'Relative' Curfews, a specific time or a set number of days, hours and minutes can be applied. These can also be applied to both 'Items' and 'Users'.

Setting up an Item Curfew

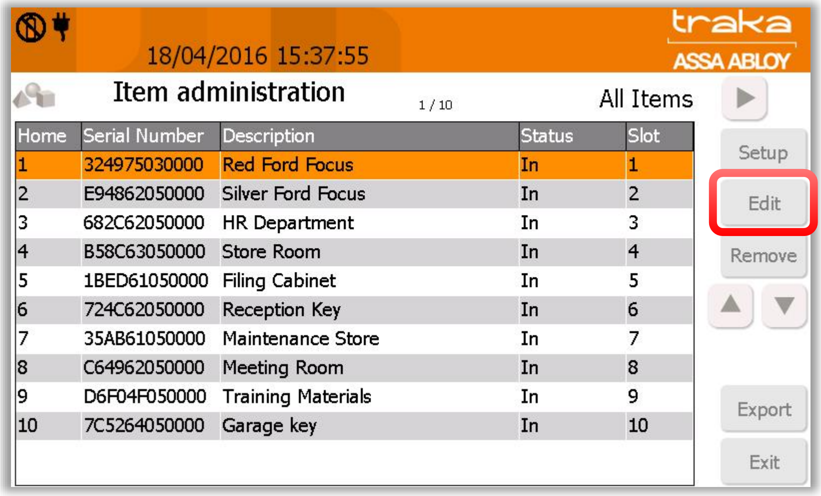
1. Access the Traka Touch System and click on 'Admin'.



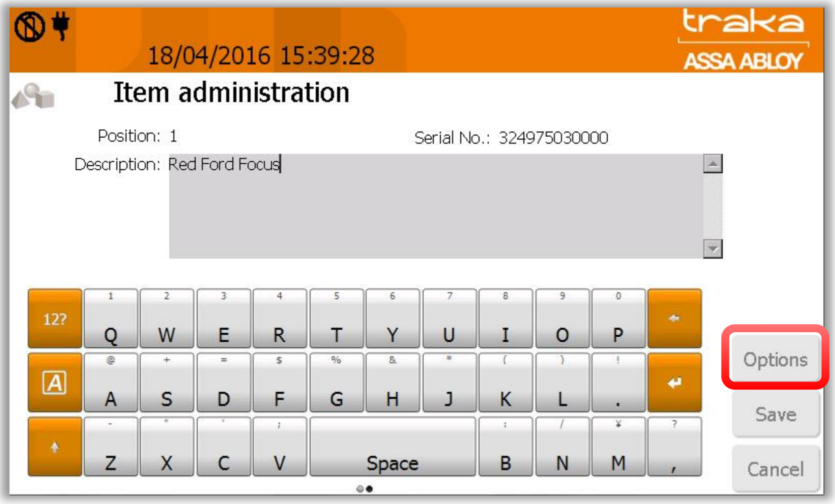
2. You will now be taken to the 'Administration' screen. Click on 'Items'.



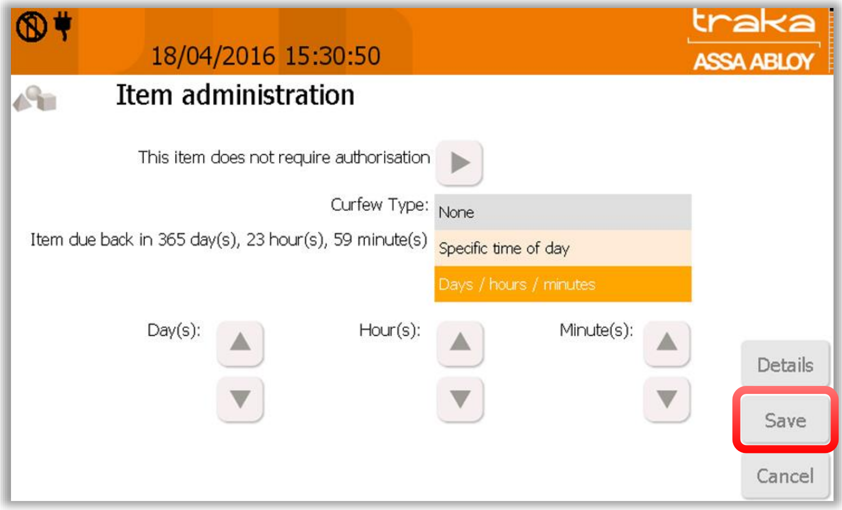
3. Select the item you wish to apply the Curfew against and then click on 'Edit'.



4. The next screen allows you to change the description of the Item if required. Click on 'Options' to continue.

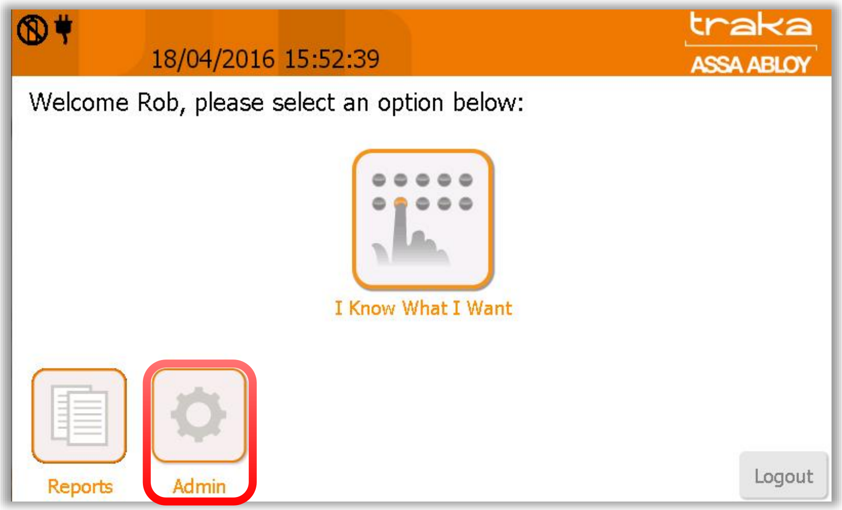


At the next screen, you will be presented with the option for 'Specific time of day' and 'Number of days, hours and minutes'. The buttons immediately below will enable you cycle up and down through the units corresponding to Days, Hours and Minutes. Once you have set the Curfew, click 'Save'.

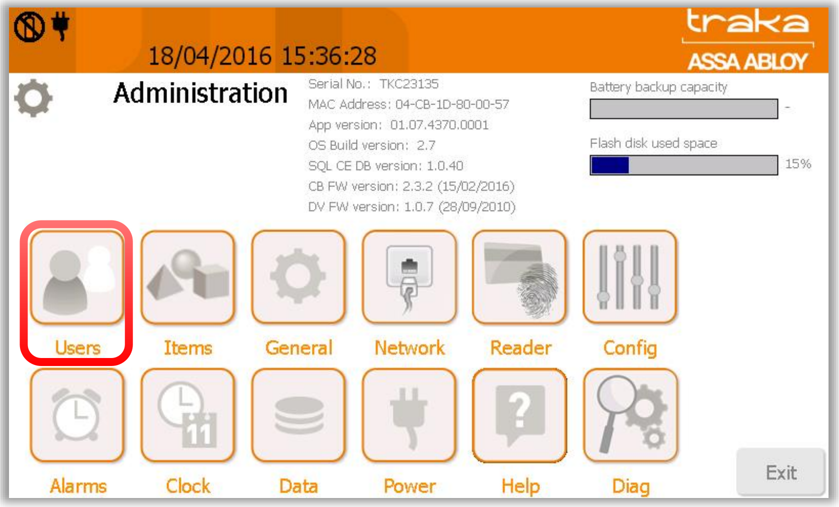


Setting up a User Curfew

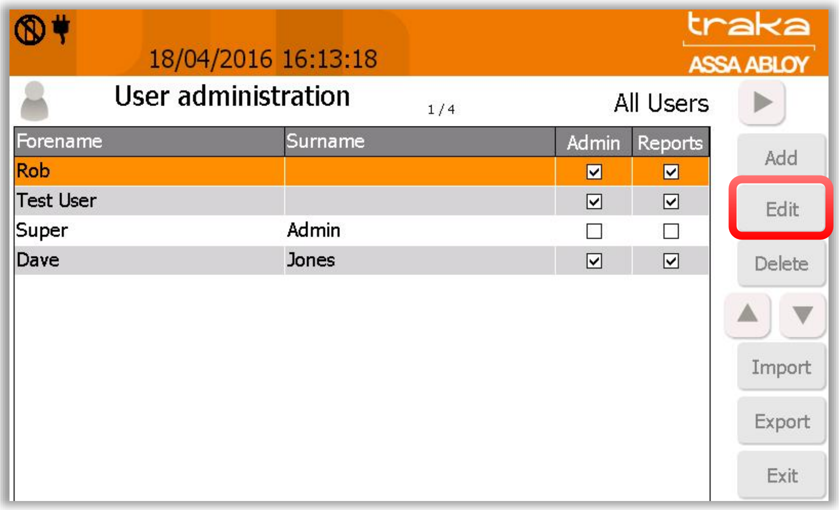
1. Access the Traka Touch System and click on 'Admin'.



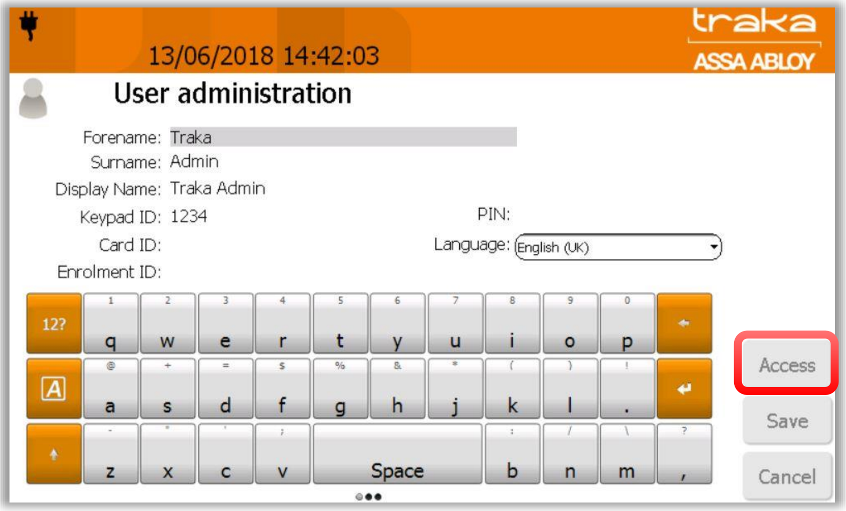
2. You will now be taken to the 'Administration' screen. Click on 'Users'.



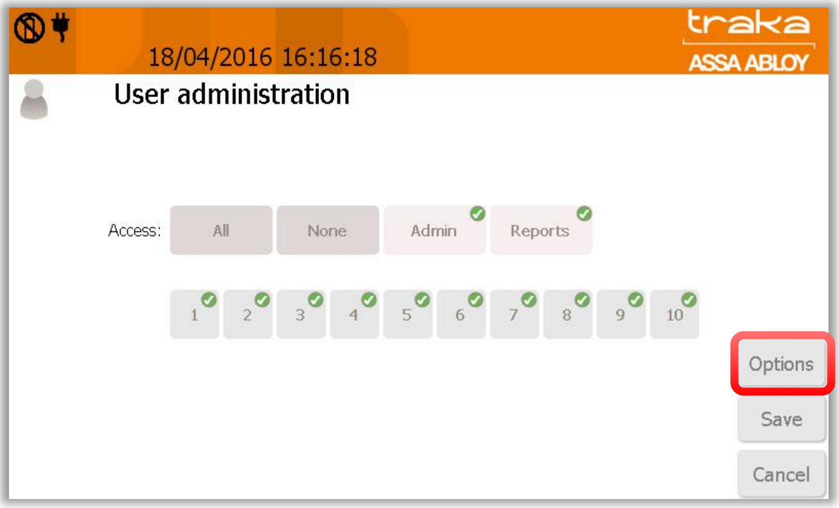
3. Select the User you wish to apply the Curfew against and click 'Edit'.



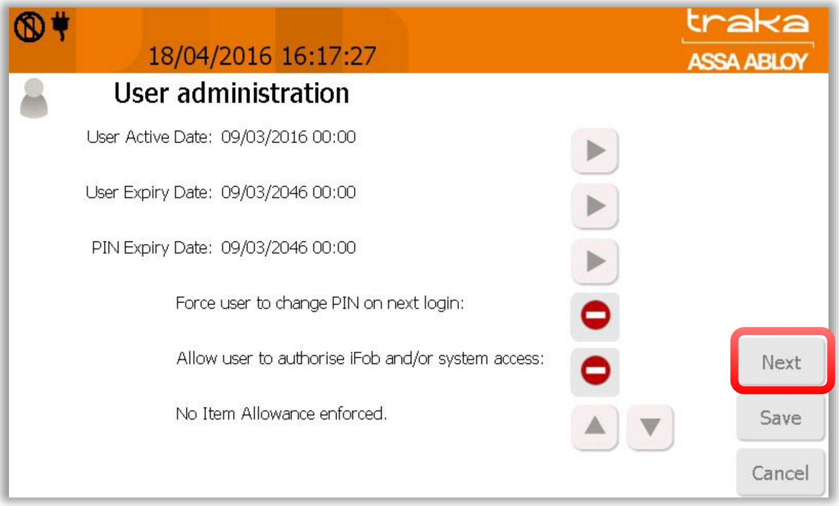
4. The next screen will allow you to edit details about the User if required. Click on the 'Access' button.



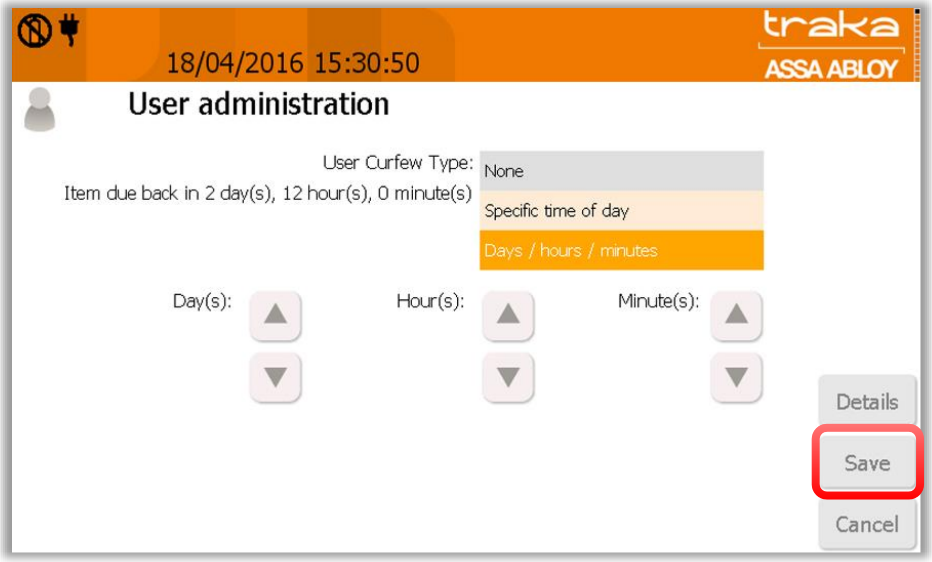
5. You will now be taken to the 'User Administration' screen. Click the 'Options' button to continue.



6. You will now be taken to the next 'User Administration' screen. Click on the 'Next' button.



7. At the next screen, you will be presented with the option for 'Specific time of day' and 'Number of days, hours and minutes'. The buttons immediately below will enable you cycle up and down through the units corresponding to Days, Hours and Minutes. Once you have set the Curfew. Click on 'Save'.



4.14 EMERGENCY OPEN

The Emergency Open option will be a standard feature on all Traka Touch Locker systems using Traka Touch v2.3 and above with TrakaWEB v3.3 and above. It will allow a user with the option enabled on their profile to open all the doors on a Locker system. This will be achieved in sequential order and as quickly as possible by simply pressing the **Emergency** icon- on the Traka Touch screen.

The option can be enabled on a user-by-user basis. The Emergency Open option will open all doors regardless of the users' assigned access rights or any access schedules that may have been allocated to the user and/or item.

Any other cost options such as Notes Logging or Reason Logging will be overridden and will not be displayed. Curfew functionality will remain, but no prompts will be made available.

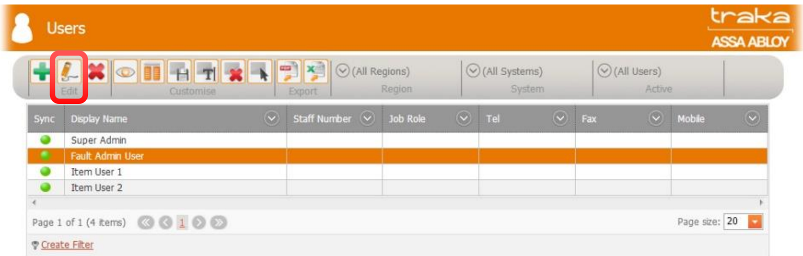
If your system is a stand-alone configuration i.e., it is not connected to TrakaWEB, the option to grant or revoke the Emergency Open permission to a User maybe carried out in Traka Touch. For more information, please refer to **UD0090 – Traka Touch Lockers User Guide.**

Should the Emergency Open option be activated or deactivated at any time, an event will be recorded to show any activity. These events may also have alarm relays programmed against them or the event may be used to trigger an email notification.

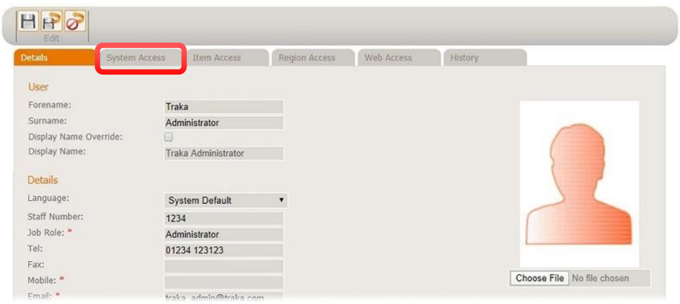
Whilst the Emergency Open option is activated and 1 or more doors remain open, the configured auto-logout timeout will not apply. All the doors must be closed before the user is logged out.

4.14.1 ENABLING THE OPTION

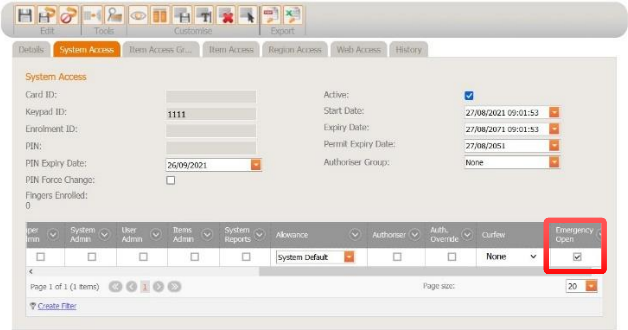
1. To enable the Emergency Open option, select a user from the users' list within TrakaWEB and then select **Edit**.



2. At the **Edit User** screen, select the System Access tab.



3. Towards the bottom of the page, the Emergency Open option will be available. Click on the check box to enable it as shown below.



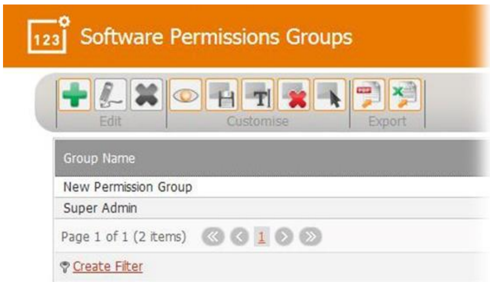
4. Once completed, click on Save & Return.

4.14.2 SOFTWARE PERMISSION GROUP

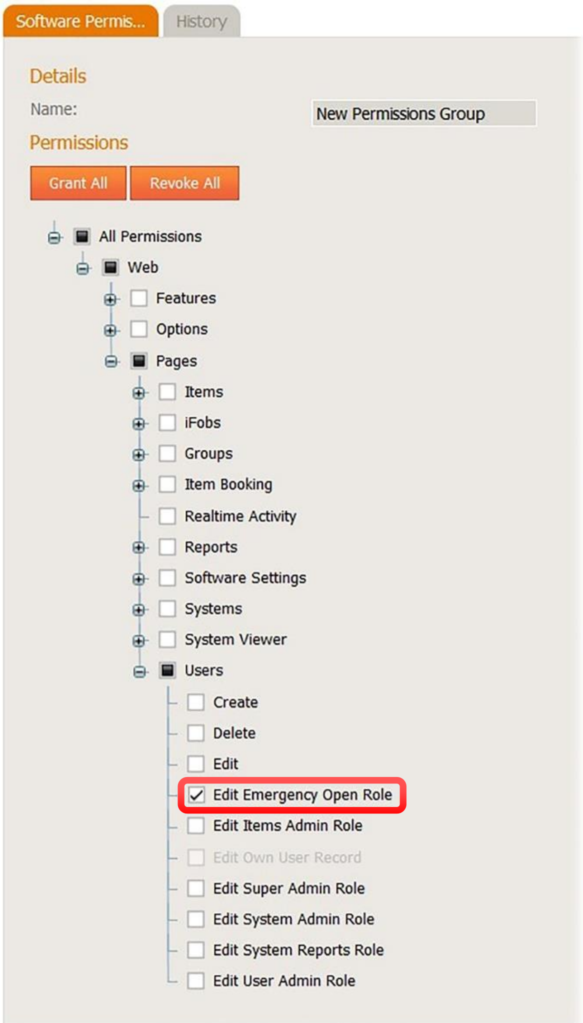
To enable a user to edit the value of the Emergency Open option within TrakaWEB, a user with the Admin role can assign the **Enable Emergency Open Role** within the Software Permission Group.

1. From the Navigation toolbar, select the Software Permissions Groups icon.

2. From the software Permissions Groups page, select the Group you wish to apply the Permission to.



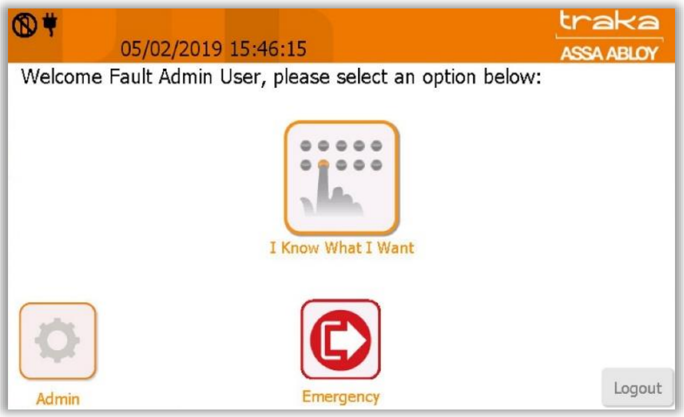
3. At the next page, navigate through the Permissions Group Tree and place a tick in the check box for the **Edit Emergency Open Role.**



4. Once complete, click on **Save & Return**.

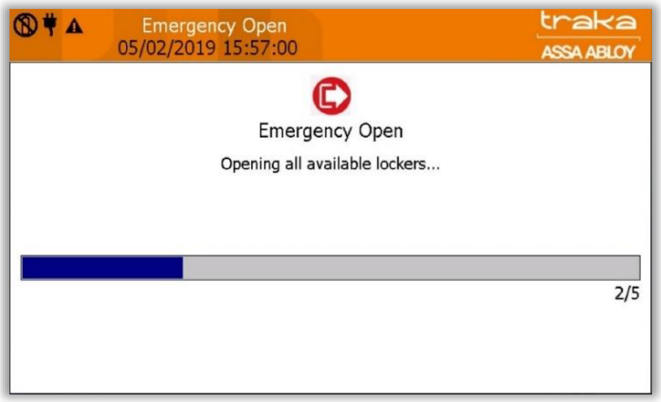
4.14.3 USING EMERGENCY OPEN

With the Emergency Open option enabled, access the Traka Touch system using keypad, fingerprint or card. You will then be presented with the following screen:



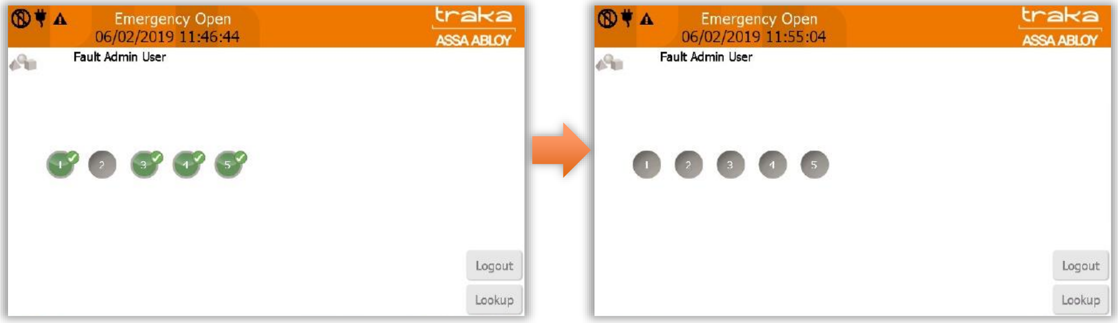
1. Next, select the Emergency icon-  on the Touch screen. All the doors to the Locker system will now open sequentially.

As the doors are opening, a progress bar will display the door count during the process. A flashing **Emergency Open** message will also be displayed at the top of the screen to show that the Emergency Open option has activated.



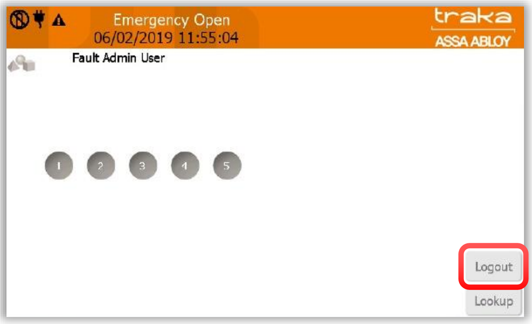
You will now be taken to the 'I Know What I Want' screen. Here you will be shown all the items currently in the system and their status. The item icons will change as the items are removed from the system.

NOTE: Closing all the doors at this stage will automatically log you out and return to the main login screen.



If you choose to select the Logout button on the screen without first closing all the doors, you will remain logged in until all the doors have been closed as detailed below.

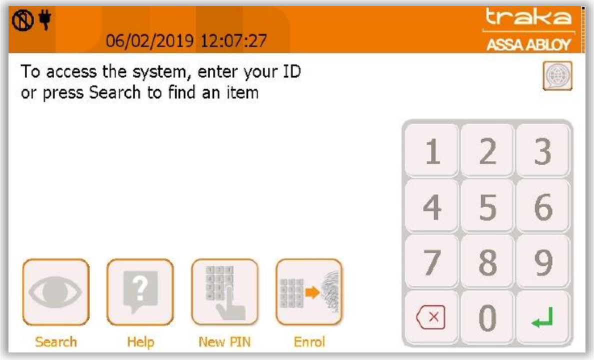
2. Select the **Logout** button to exit.



If 1 or more doors remain open, you will not be fully logged out and you will see the following screen indicating which doors remain open:

NOTE: The Emergency Open message will continue to display on the screen if one or more doors remain open and the configured auto-logout timeout will not apply.

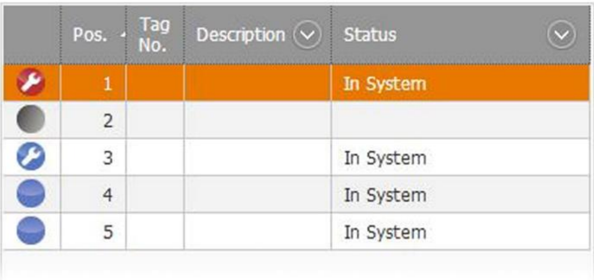
3. Close any open doors as required. You will then be taken back to the main login screen and the Emergency Open will be deactivated.



4.14.4 EMERGENCY OPEN WITH FAULT LOGGING

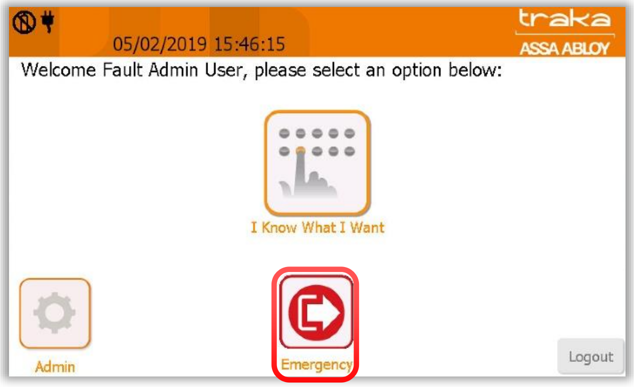
The Emergency Open option with Fault Logging enabled will operate with much the same functionality as with a standard setup Locker system. The main difference will be noted if a Locker contains an item with one or more critical faults logged against it. Lockers containing items with critical faults will not be opened by the Emergency Open process.

The example below shows a Locker system containing non-critical and critical faulty items.



	Pos.	Tag No.	Description	Status
	1			In System
	2			
	3			In System
	4			In System
	5			In System

1. With the Emergency Open option enabled, access the Traka Touch system using keypad, fingerprint or card.
2. Select the **Emergency** icon on the Touch screen.



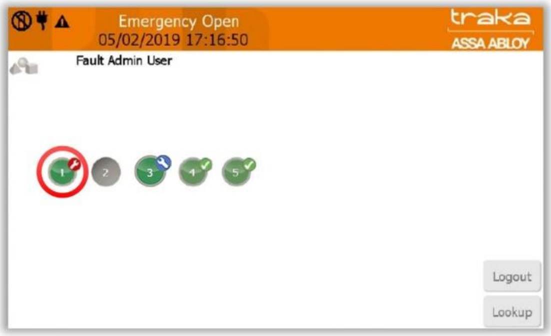
The doors will now open sequentially as described previously, except any doors to compartments containing items with critical faults.

NOTE: The message on the Touch screen will now indicate that 1 item could not be released due to a critical fault.

3. Click on **OK** to continue.

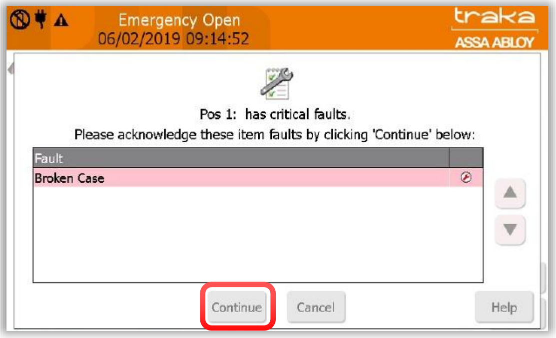
A user with the Fault Logging Admin role will be able to select the item from the touch screen.

4. Select the item with the critical fault.



At the next screen, you will be required to acknowledge that the item has a critical fault.

5. Select the **Continue** button to accept the critical fault.



The door will now open allowing access to the item with the critical fault.

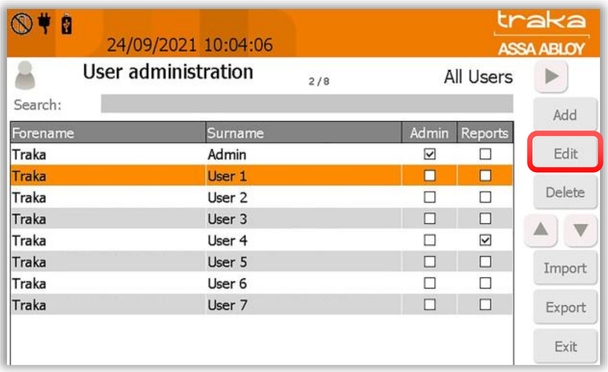
NOTE: As the I Know What I Want screen will continue to display after the Emergency Open procedure, you may also choose to reopen any doors that you may have closed.

Events will be recorded anytime the Emergency Open Feature is activated and deactivated. Events can be viewed in Reports in TrakaWEB.

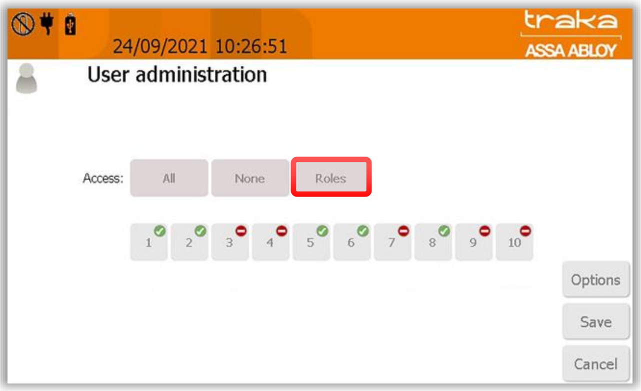
4.15 GRANT/REVOKE EMERGENCY OPEN IN TRAKA TOUCH

If your system is a stand-alone configuration i.e., it is not connected to TrakaWEB, the option to grant or revoke the Emergency Open permission to a User maybe carried out in Traka Touch.

1. After logging in, select the user that you wish to grant the Emergency Open option to and then select **Edit** and then **Access.**

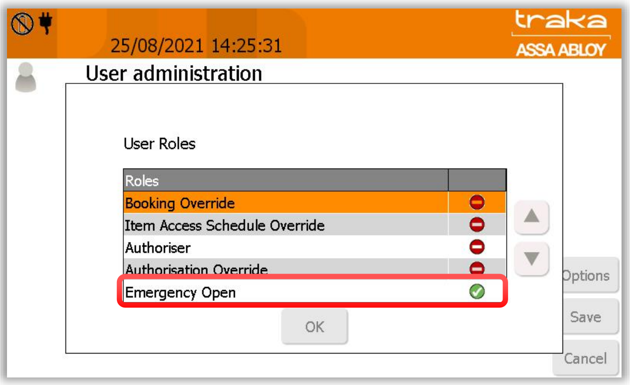


2. At the next screen, select the **Roles** button.



A new window will appear displaying a list of roles.

3. Navigate through the list and select the **Emergency Open** role. The icon will change to a tick as shown below.



4. Once completed, select **OK** and then **Save** and **Exit.**

When the user who has been granted the Emergency Open permission logs into the system, they will see the option for **Emergency Open** available on the screen.

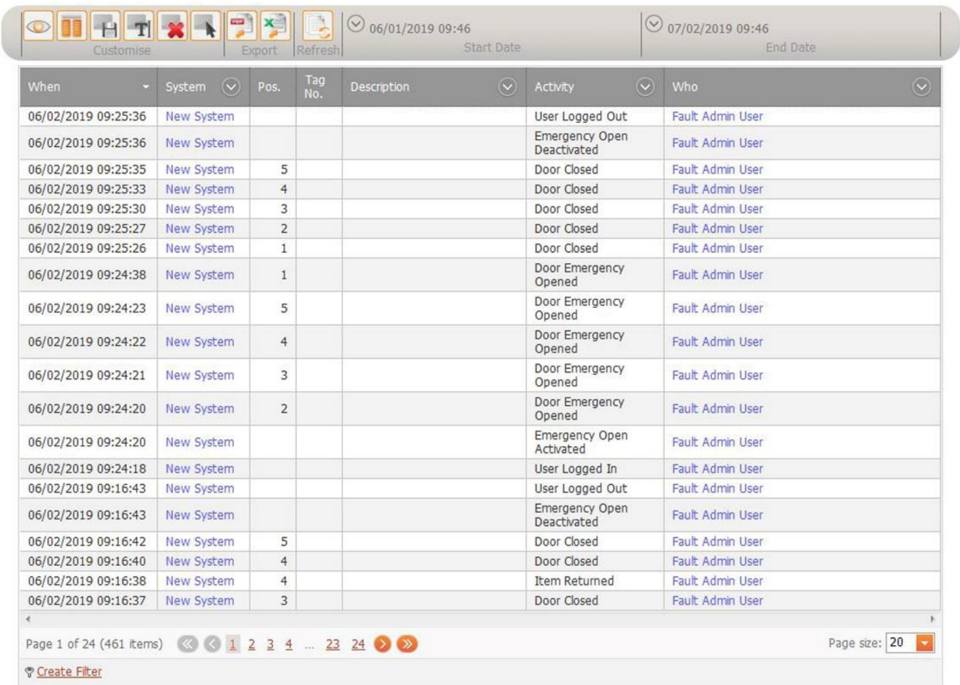
4.15.1 REPORTS

Events will be recorded anytime the Emergency Open feature is activated and deactivated. Events can be seen in Reports within TrakaWEB.

1. From the Navigation Toolbar, Select Reports.

At the Reports page, select the **General** tab followed by the **Activity Report** tab and then select **View This Report**.

The next page will display a list of Activity Events. In the example below, events can be seen generated for instances where the Emergency Open feature was activated and deactivated.



When	System	Pos.	Tag No.	Description	Activity	Who
06/02/2019 09:25:36	New System				User Logged Out	Fault Admin User
06/02/2019 09:25:36	New System				Emergency Open Deactivated	Fault Admin User
06/02/2019 09:25:35	New System	5			Door Closed	Fault Admin User
06/02/2019 09:25:33	New System	4			Door Closed	Fault Admin User
06/02/2019 09:25:30	New System	3			Door Closed	Fault Admin User
06/02/2019 09:25:27	New System	2			Door Closed	Fault Admin User
06/02/2019 09:25:26	New System	1			Door Closed	Fault Admin User
06/02/2019 09:24:38	New System	1			Door Emergency Opened	Fault Admin User
06/02/2019 09:24:23	New System	5			Door Emergency Opened	Fault Admin User
06/02/2019 09:24:22	New System	4			Door Emergency Opened	Fault Admin User
06/02/2019 09:24:21	New System	3			Door Emergency Opened	Fault Admin User
06/02/2019 09:24:20	New System	2			Door Emergency Opened	Fault Admin User
06/02/2019 09:24:20	New System				Emergency Open Activated	Fault Admin User
06/02/2019 09:24:18	New System				User Logged In	Fault Admin User
06/02/2019 09:16:43	New System				User Logged Out	Fault Admin User
06/02/2019 09:16:43	New System				Emergency Open Deactivated	Fault Admin User
06/02/2019 09:16:42	New System	5			Door Closed	Fault Admin User
06/02/2019 09:16:40	New System	4			Door Closed	Fault Admin User
06/02/2019 09:16:38	New System	4			Item Returned	Fault Admin User
06/02/2019 09:16:37	New System	3			Door Closed	Fault Admin User

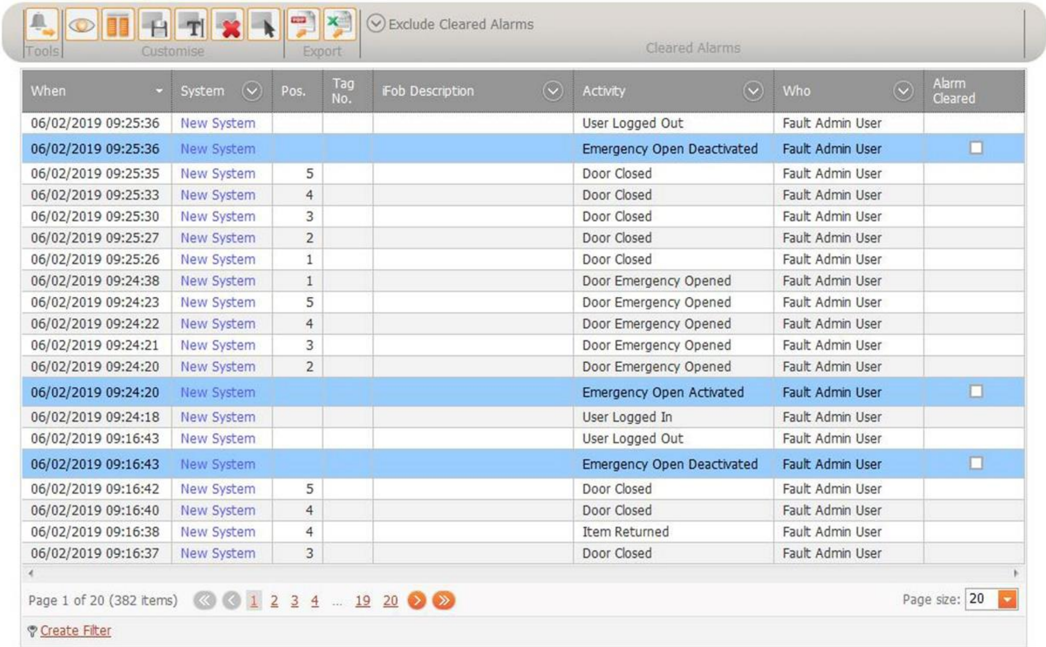
Page 1 of 24 (461 items) 1 2 3 4 ... 23 24 Page size: 20

Create Filter

From the Realtime Activity icon on the Navigation Toolbar, a list of alarms generated from the activation and deactivation of the Emergency Open feature can be viewed.

1. Select the Realtime Activity icon from the Navigation Toolbar.

The next page will now display the list of generated alarms as shown in the example below.



When	System	Pos.	Tag No.	iFob Description	Activity	Who	Alarm Cleared
06/02/2019 09:25:36	New System				User Logged Out	Fault Admin User	
06/02/2019 09:25:36	New System				Emergency Open Deactivated	Fault Admin User	
06/02/2019 09:25:35	New System	5			Door Closed	Fault Admin User	
06/02/2019 09:25:33	New System	4			Door Closed	Fault Admin User	
06/02/2019 09:25:30	New System	3			Door Closed	Fault Admin User	
06/02/2019 09:25:27	New System	2			Door Closed	Fault Admin User	
06/02/2019 09:25:26	New System	1			Door Closed	Fault Admin User	
06/02/2019 09:24:38	New System	1			Door Emergency Opened	Fault Admin User	
06/02/2019 09:24:23	New System	5			Door Emergency Opened	Fault Admin User	
06/02/2019 09:24:22	New System	4			Door Emergency Opened	Fault Admin User	
06/02/2019 09:24:21	New System	3			Door Emergency Opened	Fault Admin User	
06/02/2019 09:24:20	New System	2			Door Emergency Opened	Fault Admin User	
06/02/2019 09:24:20	New System				Emergency Open Activated	Fault Admin User	
06/02/2019 09:24:18	New System				User Logged In	Fault Admin User	
06/02/2019 09:16:43	New System				User Logged Out	Fault Admin User	
06/02/2019 09:16:43	New System				Emergency Open Deactivated	Fault Admin User	
06/02/2019 09:16:42	New System	5			Door Closed	Fault Admin User	
06/02/2019 09:16:40	New System	4			Door Closed	Fault Admin User	
06/02/2019 09:16:38	New System	4			Item Returned	Fault Admin User	
06/02/2019 09:16:37	New System	3			Door Closed	Fault Admin User	

4.16 RRSS (RANDOM RETURN TO SINGLE SYSTEM)

This feature is available from TrakaWEB V2.3.0 and Traka Touch Application V1.6.0.

NOTE: This feature is currently not available for Locker Systems.

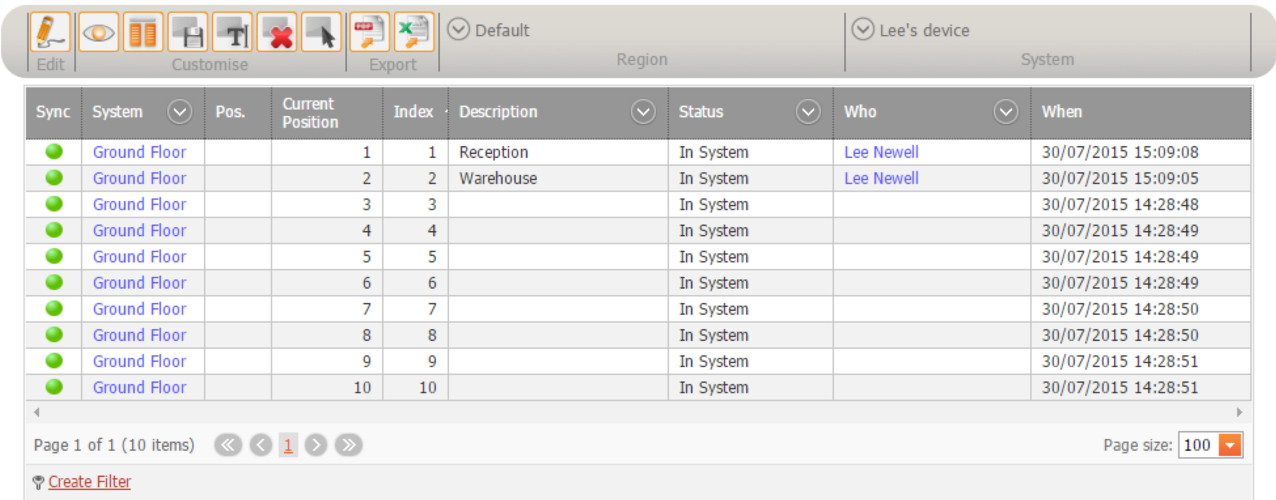
RRSS (Random Return to Single System) allows any iFob belonging to a system to be returned to any position within that system. It will also support more iFobs than receptor sockets (up to a maximum of 720 iFobs in total).

NOTE: To use the RRSS feature you must first have it enabled in the configuration file.

USEFUL TIP: Use the 'I Need To Search' option when removing iFobs for ease of locating required items.

4.16.1.1 IFOB LIST

With the RRSS feature enabled, the iFob list displays an additional column named Index. In addition to this you can enable the Current Position column to allow you to see the current location of each Item.



Sync	System	Pos.	Current Position	Index	Description	Status	Who	When
	Ground Floor		1	1	Reception	In System	Lee Newell	30/07/2015 15:09:08
	Ground Floor		2	2	Warehouse	In System	Lee Newell	30/07/2015 15:09:05
	Ground Floor		3	3		In System		30/07/2015 14:28:48
	Ground Floor		4	4		In System		30/07/2015 14:28:49
	Ground Floor		5	5		In System		30/07/2015 14:28:49
	Ground Floor		6	6		In System		30/07/2015 14:28:49
	Ground Floor		7	7		In System		30/07/2015 14:28:50
	Ground Floor		8	8		In System		30/07/2015 14:28:50
	Ground Floor		9	9		In System		30/07/2015 14:28:51
	Ground Floor		10	10		In System		30/07/2015 14:28:51

NOTE: The 'Pos.' column for RRSS systems is not used.

Index

During the Item Setup process, each iFob is assigned a unique index number. This index number will stay with the iFob for life. It is possible for this index number to be larger than the total number of positions available in the system as the RRSS feature supports more iFobs than receptor sockets.

NOTE: The process for setting up the items at the Traka Touch system can be found in the Traka Touch User Guide (UD0011) in the RRSS section.

4.16.1.2 IFOB REPLACEMENT

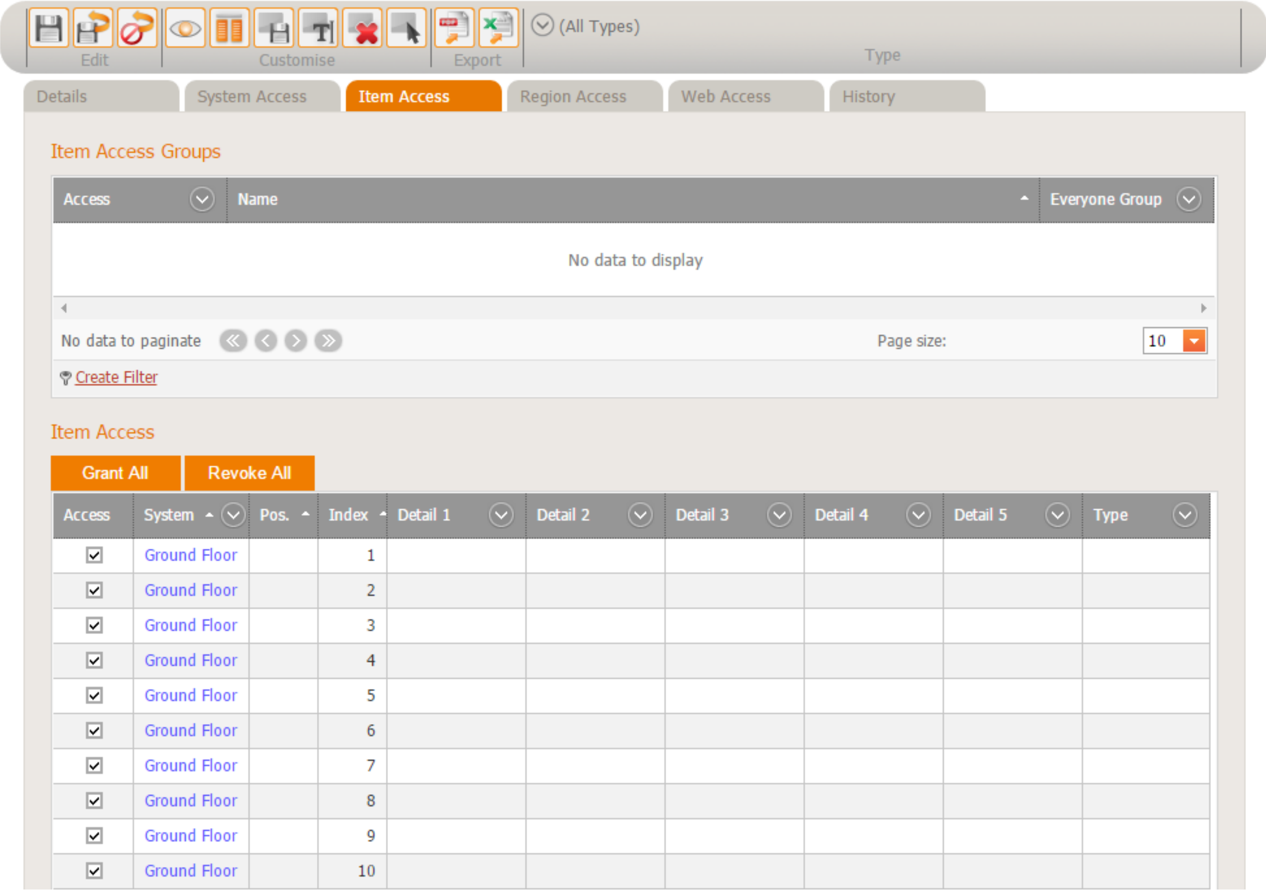
From time to time, you may be required to replace an iFob that has become lost or damaged. During the replacement procedure, TrakaWEB will transfer all allocated items from the old iFob to the new iFob. The old iFob will remain in the iFob List, but as an unallocated iFob. The system will also generate an 'Item Replaced' event.

NOTE: The Item Replacement procedure can be found in the Traka Touch User Guide - UD0011 in the RRSS section.

4.16.1.3 GRANTING ACCESS TO ITEMS

Granting access to items in a RRSS system is carried out in the same way as on a Fixed Return system. The only difference is that the Item List shows the index numbers rather than the position numbers.

Simply navigate to the Item Access tab on the Edit User page and select the Items the user requires access to by ticking the boxes in the Access column.



4.17 ACCESS SCHEDULES

Access Schedules is a cost option that is used within TrakaWEB to impose time restrictions on iFobs/items over and above the normal access rights needed to access them.

Before it can be used, it will need to be enabled on your Traka Touch system by installing a configuration file. This is usually carried out by Traka during production but if need be, you can add the configuration file to your own existing system. Please contact Traka or your distributor for further details.

The functionality of Access Schedules is based on the following requirements:

- To grant/restrict access, any users who are included in a schedule will only be allowed access to iFobs/items when the schedule is active. Outside of this time, they will only have access to no iFobs/items at all.
- The access restrictions will not prevent a user from returning an item, only taking it.
- Locking receptor strips on key cabinets and locker doors will physically restrict access to items however, Non-Locking receptor strips are unable to enforce this.
- If an Item is physically removed outside of the allowed access schedule (e.g. on a non-locking system) then an 'Item Removed outside Schedule' event will be recorded.
- A schedule restriction can be overridden on an Item (not a user) by a special role called 'Item Access Schedule Override'.
- Software permissions will control who can administer the Access Schedules.

NOTE: A best practice would be to keep users and item/iFobs in separate Access Schedules to avoid potential confusion.

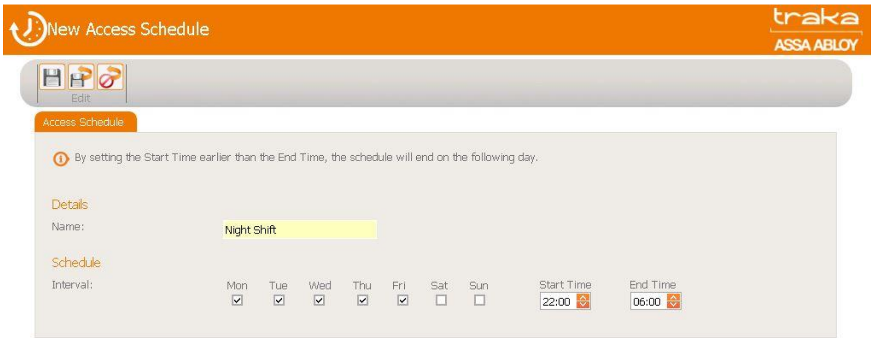
4.18 CREATE A NEW ACCESS SCHEDULE

1. From the Navigation Toolbar, click on 'Software Settings', then locate and click on the Access Schedules icon.

2. At the next page, click on the  **Create** icon

You will now be taken to the **New Access Schedule** page.

3. Add a name for the Access Schedule and then check the required boxes for the schedule interval and create the start and end time. An example is shown below:



NOTE: In the example above, the start time is set for 22:00 and the end time is 06:00. The Access Schedule for Friday will end on Saturday morning even without the check box for Saturday being ticked.

4. Once completed, click on  **Save & Return.**

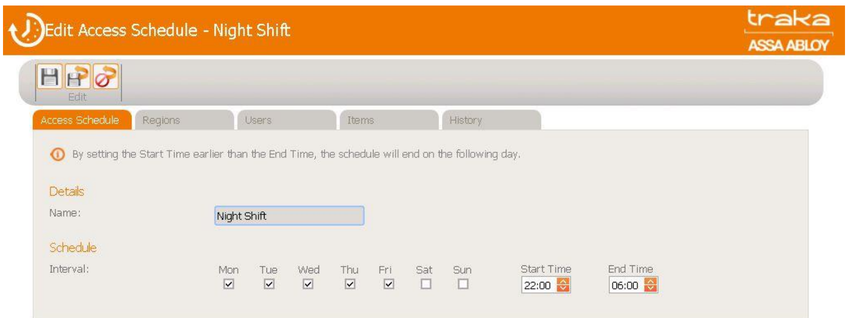
NOTE: Only 1 Access Schedule can be applied to an iFob/Item record.

NOTE: Up to 2 Access Schedules can be applied to a User record per system.

4.19 APPLYING ACCESS SCHEDULES TO USERS AND IFOB/ITEM RECORDS

1. Click on the Access Schedules icon on the Navigation Toolbar.
2. Select the Access Schedule you wish to apply to a User or iFob/Item as shown below.

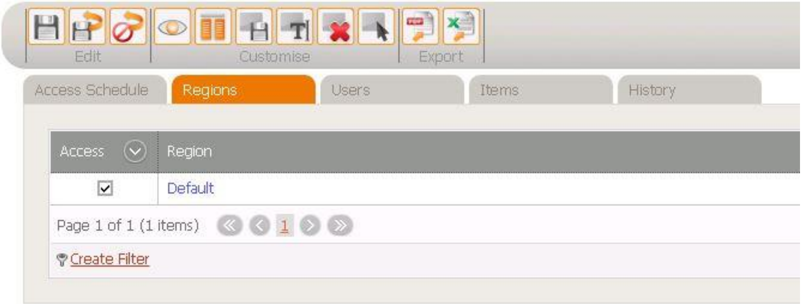
You will now be taken back to the Access Schedule page, displaying the selected Access Schedule.



Selecting the tabs along the top of the page will allow you to control how you wish to apply the Access Schedule.

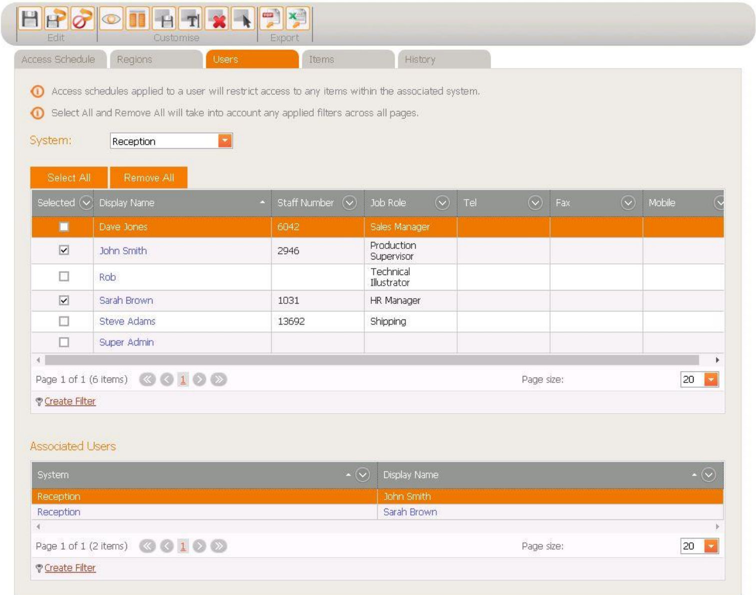
4.19.1 REGIONS

The Regions tab allows you to select different regions, which will be affected by the selected Access Schedule.



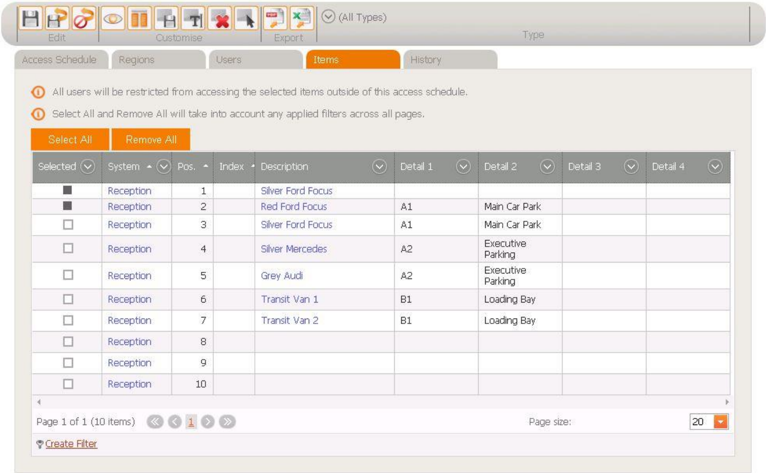
4.19.2 USERS

The Users tab allows you to select individual users that will be affected by the Access Schedule. Selected users will not have access to iFobs/Items outside the specified schedule unless they have been given the Item Access Schedule Override permission.

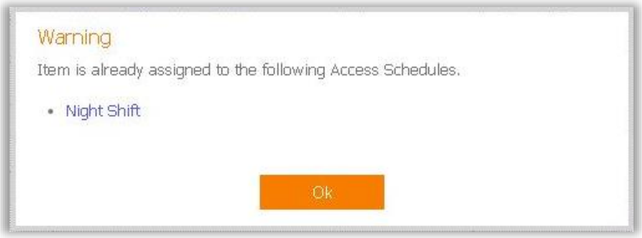


4.19.3 ITEMS

The Items tab will allow you to select which iFobs/items are affected by the specified schedule. All users will be restricted from accessing any selected items outside of the schedule unless they have been given the Item Access Schedule Override permission.



If an item has already been assigned to an Access Schedule, you will be unable to select it within any other schedules. Its check box will appear greyed out. This is because only one access schedule can be applied to an iFob/item. Attempting to click on the check box will display the following message:



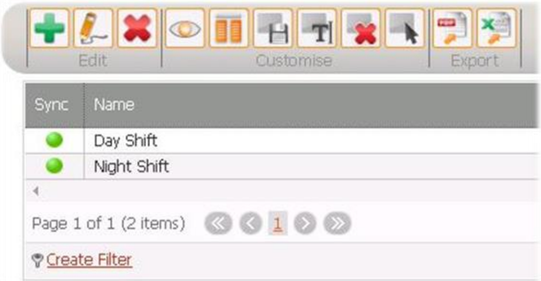
4.19.4 HISTORY

The History tab will display all the recent history of created Access Schedules. An example is shown below:

4.20 EDITING ACCESS SCHEDULES

2. Once the Access Schedule has been created, Click on  **Save and Return.**

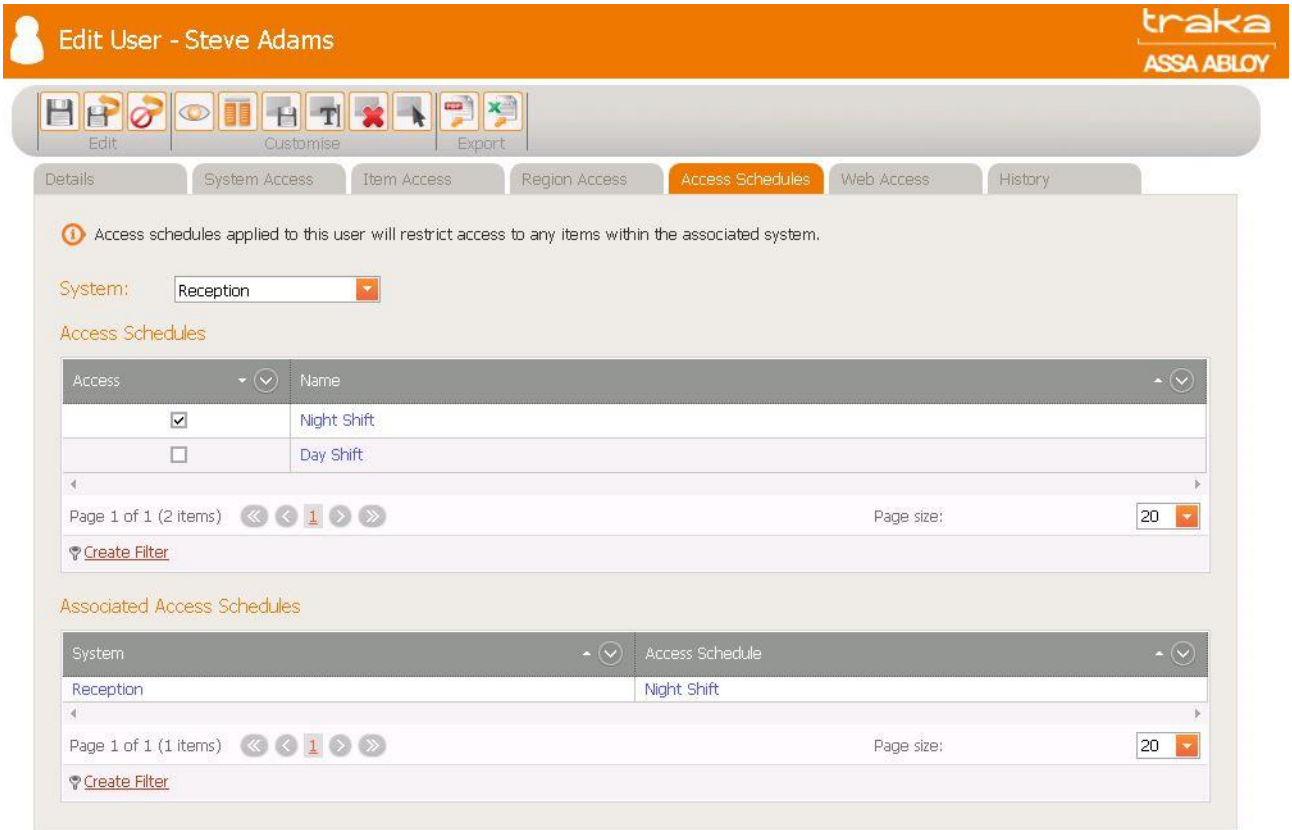
NOTE: The rotating sync icons will now appear green to indicate that the Access Schedules are now in place and have been synced to the relevant Traka Touch systems.



4.20.1 EDIT USER

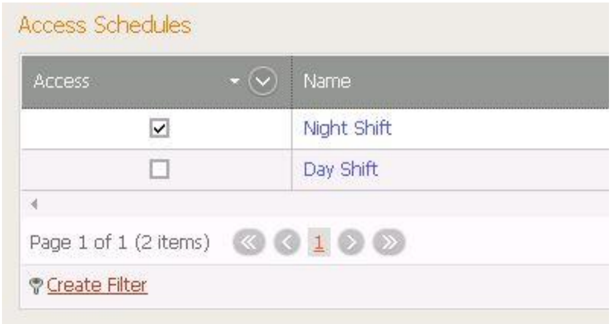
1. To edit an Access Schedule applied to a user, select the user icon from the Navigation Toolbar.
2. At the Users page, double click on the user you wish to edit. This will then take you to the Edit User page for that specific person.
3. Click on the **Access Schedule** tab located at the top of the screen.

The next screen shows the Access Schedules which are currently applied to that user.



Here, you may filter the list of Access Schedules and which systems are affected by them, restricting the user any access to the one currently selected.

To select which Access Schedule/s you wish to apply to the user, select one or more boxes as shown in the example below:



4.20.2 EDIT IFOBS/ITEMS

1. To edit an Access Schedule applied to an iFob/Item, click on the iFob icon on the Navigation Toolbar.
2. At the iFobs page, double click on the description you wish to edit. This will then take you to the Edit iFob page for that specific iFob/item.
3. Click on the **Access Schedule** tab located at the top of the screen.

The next screen shows the current Access Schedules which are currently applied to that iFob/item. Clicking in the check box will apply the restrictions to all users of that system outside of the schedule unless they have the Item Access Schedule Override permission.

4.20.3 EDITING THE TIME PICKER FOR 12 HOUR TIME FORMAT

As the US locale uses the 12hr time format, it is necessary to edit the AM or PM suffix in TrakaWEB manually. For example, instead of changing to 12:00 PM when incrementing from 11:00 AM, the time will go back to 12:00 AM as shown below.

1. To adjust the suffix, click on AM or PM and click on the arrow to adjust the increment.

4.20.4 ITEM ACCESS SCHEDULE OVERRIDE

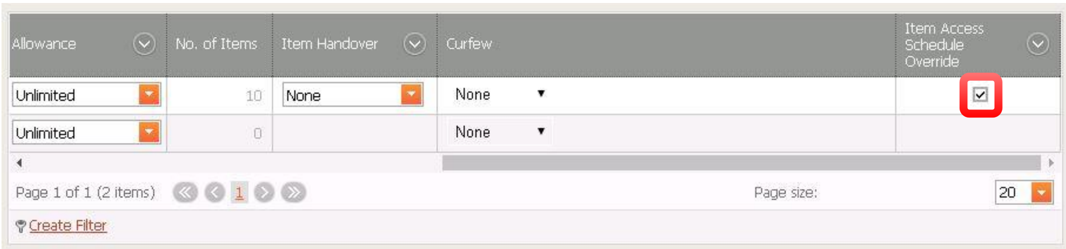
It is possible to allocate a user the Item Access Schedule Override permission. This will allow them to take iFobs/Items regardless of an Access Schedule being in place against the item.

To allocate a user with the permission:

1. Select the user icon from the Navigation Toolbar.
2. Double click on the user you wish to allocate the permission to.
3. At the Edit User screen, click on the System Access tab

You will now be taken to the Edit User, System Access screen.

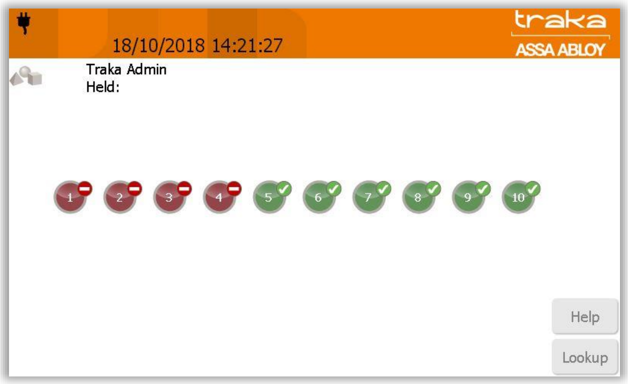
4. Locate the Item Access Schedule Override checkbox by scrolling to the right of the screen.
5. Place a tick in the check box to enable the permission as shown below.



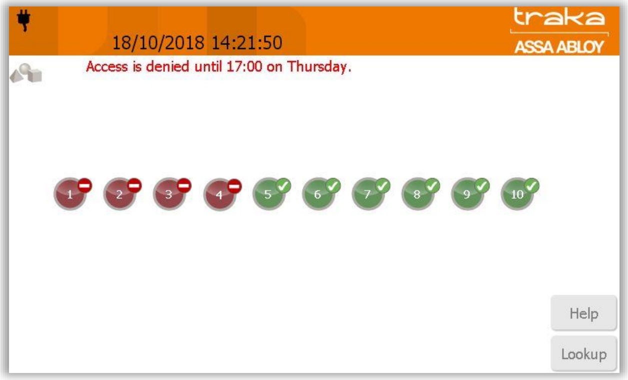
NOTE: If a user, who has the Access Schedule Override permissions, needs to access an item outside of the allowed time and that item is kept in either a FIFO or Advanced FIFO system, that user also needs to have FIFO Override permissions in order to get to the required item. For more information, refer to UD0232 TrakaWEB FIFO and Advanced FIFO User Guide.

4.21 TRAKA TOUCH

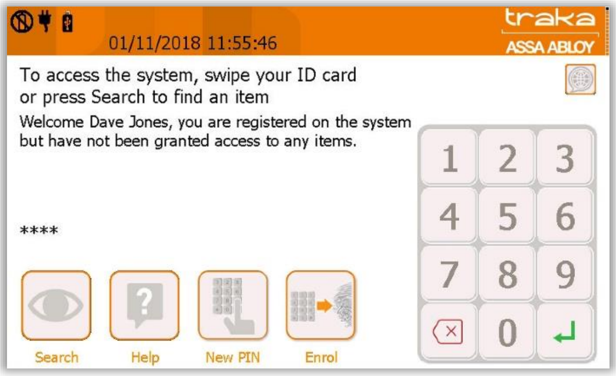
With an access schedule in place, it will not be possible for users to take items displayed as,  outside of the allocated schedule. When a user typically accesses the system and attempts to take an iFob or item, the following screen will be presented:



If the user clicks on a position, they will see the following message:



Any users who are included in a schedule will only be allowed access to iFobs/items when the schedule is active. Outside of this time, they will have access to no iFobs/items at all, and if they are not an admin user or do not have reports access, they will not be allowed to log in and will instead the following message:



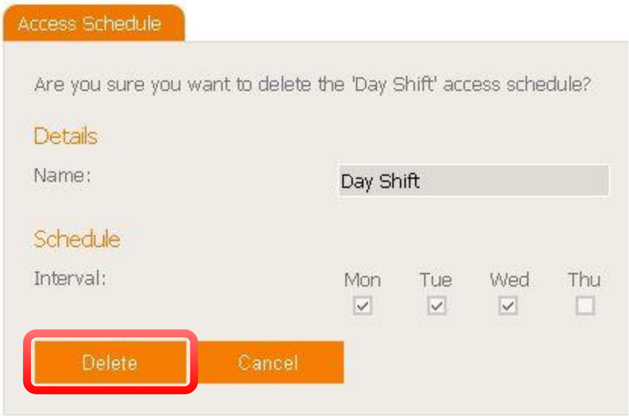
NOTE: During an active schedule, anyone with access may take an item. Outside of the active schedule, only users with the Item Access Schedule Override permission will be able to take items.

4.22 DELETING AN ACCESS SCHEDULE.

1. Click on the Access Schedule icon within the Navigation Toolbar.
2. Select the Access Schedule you wish to delete and click on **Delete**.

You will then be presented with the following screen asking you to confirm that you wish delete the selected Access Schedule.

3. Click on Delete.

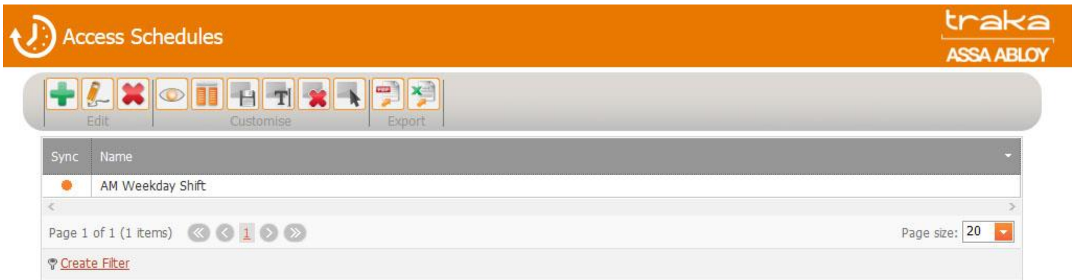


4.23 ACCESS SCHEDULES 'UMBRELLA SYNC STATUS'

The Access Schedule Landing Page displays the sync status of a Schedule for all associated systems. If an Access Schedule is changed, the change will have a direct impact on all systems associated with that schedule.

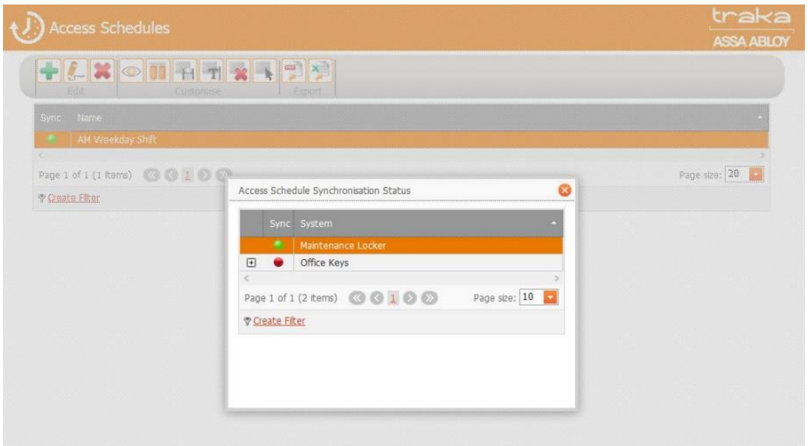
Depending on the number of systems associated with the access schedule, the status icon will reflect the overall current status in relation to the sync process.

- Green icon – sync on all systems successful
- Red icon – sync on all systems unsuccessful
- Orange icon – Combination of both successful and unsuccessful sync
- Spinning icon – Combination of successful, unsuccessful and pending sync



Clicking on the sync status icon will display a window showing all the systems affected by the schedule change and their current sync status.

- Green icon – sync successful
- Red icon – sync failed
- Spinning icon – sync pending



4.24 USB CHARGE STATUS INDICATION

4.24.1.1 USB CHARGE STATUS INDICATION OVERVIEW

This feature can only be used with RFID Locker Systems and is supported from TrakaWEB V2.1.59.1, and Traka Touch Application V1.5.4327.1.

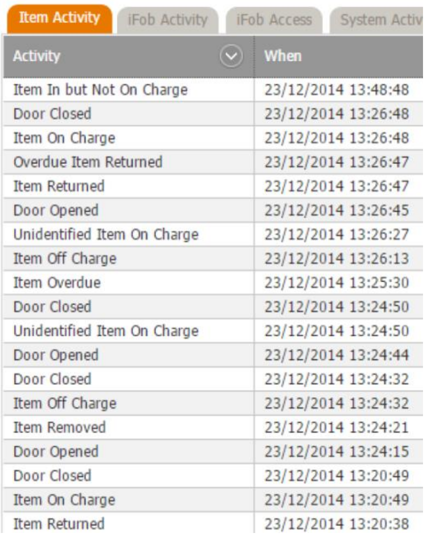
Locker systems can be fitted with optional hardware to allow the charging of USB devices inside locker compartments. This hardware also has the ability to detect whether or not the item in the compartment is currently on charge, if it is fully charged, or if the item has a charge fault.

For more details on how this feature is implemented and used on the Traka Touch Locker System, please refer to the **Traka Touch Lockers User Guide – UD0090.**

4.24.1.2 ACTIVITY AND REPORTS

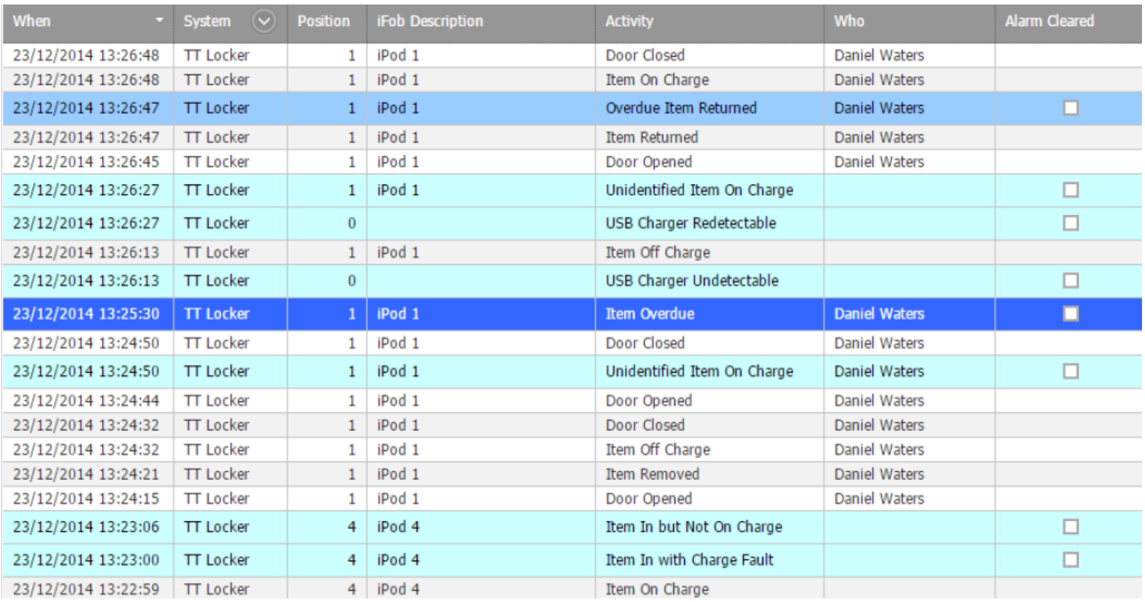
The USB Charge Status Indication feature can generate the following activities. These will all be generated and displayed in the Item Activity grids and on Reports.

- Item On Charge
- Item Off Charge
- Item Charged
- Item In With Charge Fault
- Item In But Not On Charge
- Unidentified Item On Charge
- Unidentified Item Charged
- Unidentified Item Charge Fault
- Unidentified Item Off Charge
- USB Charger Undetectable
- USB Charger Redetectable



Item Activity | iFob Activity | iFob Access | System Activ

Activity	When
Item In but Not On Charge	23/12/2014 13:48:48
Door Closed	23/12/2014 13:26:48
Item On Charge	23/12/2014 13:26:48
Overdue Item Returned	23/12/2014 13:26:47
Item Returned	23/12/2014 13:26:47
Door Opened	23/12/2014 13:26:45
Unidentified Item On Charge	23/12/2014 13:26:27
Item Off Charge	23/12/2014 13:26:13
Item Overdue	23/12/2014 13:25:30
Door Closed	23/12/2014 13:24:50
Unidentified Item On Charge	23/12/2014 13:24:50
Door Opened	23/12/2014 13:24:44
Door Closed	23/12/2014 13:24:32
Item Off Charge	23/12/2014 13:24:32
Item Removed	23/12/2014 13:24:21
Door Opened	23/12/2014 13:24:15
Door Closed	23/12/2014 13:20:49
Item On Charge	23/12/2014 13:20:49
Item Returned	23/12/2014 13:20:38



When	System	Position	iFob Description	Activity	Who	Alarm Cleared
23/12/2014 13:26:48	TT Locker	1	iPod 1	Door Closed	Daniel Waters	
23/12/2014 13:26:48	TT Locker	1	iPod 1	Item On Charge	Daniel Waters	
23/12/2014 13:26:47	TT Locker	1	iPod 1	Overdue Item Returned	Daniel Waters	☐
23/12/2014 13:26:47	TT Locker	1	iPod 1	Item Returned	Daniel Waters	
23/12/2014 13:26:45	TT Locker	1	iPod 1	Door Opened	Daniel Waters	
23/12/2014 13:26:27	TT Locker	1	iPod 1	Unidentified Item On Charge		☐
23/12/2014 13:26:27	TT Locker	0		USB Charger Redetectable		☐
23/12/2014 13:26:13	TT Locker	1	iPod 1	Item Off Charge		
23/12/2014 13:26:13	TT Locker	0		USB Charger Undetectable		☐
23/12/2014 13:25:30	TT Locker	1	iPod 1	Item Overdue	Daniel Waters	☐
23/12/2014 13:24:50	TT Locker	1	iPod 1	Door Closed	Daniel Waters	
23/12/2014 13:24:50	TT Locker	1	iPod 1	Unidentified Item On Charge	Daniel Waters	☐
23/12/2014 13:24:44	TT Locker	1	iPod 1	Door Opened	Daniel Waters	
23/12/2014 13:24:32	TT Locker	1	iPod 1	Door Closed	Daniel Waters	
23/12/2014 13:24:32	TT Locker	1	iPod 1	Item Off Charge	Daniel Waters	
23/12/2014 13:24:21	TT Locker	1	iPod 1	Item Removed	Daniel Waters	
23/12/2014 13:24:15	TT Locker	1	iPod 1	Door Opened	Daniel Waters	
23/12/2014 13:23:06	TT Locker	4	iPod 4	Item In but Not On Charge		☐
23/12/2014 13:23:00	TT Locker	4	iPod 4	Item In with Charge Fault		☐
23/12/2014 13:22:59	TT Locker	4	iPod 4	Item On Charge		

4.25 SAGEM FINGERPRINT READER

The Sagem Fingerprint reader is an optional system that Traka implements to identify a user before allowing access to a system. With the correct operating system version and application version installed, to activate the Sagem MorphoSmart Fingerprint Reader you simply need to plug the reader in. There are no specific reader configuration options that need to be set for the reader to work – it is simply plug & play.

Hardware Requirements

Sagem Reader Models

The following Sagem MorphoSmart Fingerprint Reader models are currently supported.

- MSO CBM 4MB IDENTLITE – 3000 user capacity (up to 2 fingers each) (Sagem Part no:252711976)
- Other variants have **not** been tested.

Traka Touch Operating System

For the Sagem MorphoSmart Fingerprint Reader to work with Traka Touch, the Traka Touch System must have Windows CE build version 1.9 or later installed.

NOTE: If a Traka Touch Base Board or Process Module has to be swapped for any reason, replacements might not have Windows CE version 1.9 installed as default and so please specify Windows CE version 1.9 or later when raising an RMA request!

If you connect a Sagem MorphoSmart Fingerprint Reader to a version of Windows CE less than 1.9, when you plug the reader in you get a Windows CE dialogue pop up requesting the Driver Name.

Traka Touch Application

For the Sagem MorphoSmart Fingerprint Reader to work with Traka Touch, the Traka Touch System must have Traka Touch Application version 01.02.4256.41 (07-Sep-12) or later installed.

4.25.1 ENROLMENT

1. Open the User List and click New to create a new user record. If you already have users in the database, highlight the desired user and click the Edit button.

2. Enter the user credentials as needed and click Access, or if you are editing an existing user simply click Access.

3. Using the on screen buttons, give the user appropriate access to positions in the system and/or admin and report access. If you are editing an existing user simply, click Options.

4. Set the active and expiry dates for the user and their PIN (if applicable) along with the item allowance, item authorisation and PIN changing options, then click Enrol. If you are editing an existing user simply, click Enrol.

The enrolment page will show how many fingers the user currently has enrolled and will allow you to select how many fingers you wish to enrol for that user.

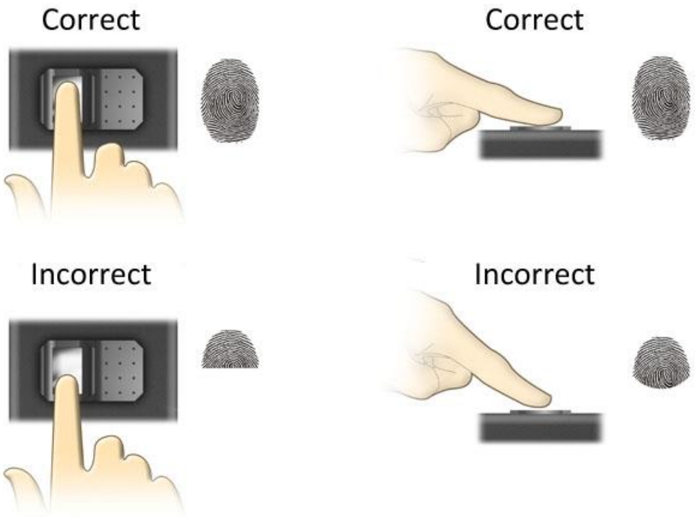
NOTE: You can enrol a maximum of two fingers per user.

5. When you wish to continue, click the Enrol button.

6. The user will then need to place their finger onto the reader.

7. The progress meter will quickly move to 100% and you will see a fingerprint with a green tick, indicating that the capture was successful. You will need to do this three times for each finger you wish to enrol.

When enrolling, it is important you align your finger to the centre of the Enrolment Module and lay your finger flat to receive accurate results.



Do not move finger when enrolling
Do not press too hard
Place your finger on the enrolment module. **Do not** slide **or** roll finger on and off

NOTE: If your finger is not properly positioned the reader may have trouble enrolling you. If this happens, Traka Touch will prompt you to complete one of following actions to help…

8. If the templates have been successfully captured, the message 'Finger Position OK' will be displayed.

If you chose to enrol two fingers, then you will be prompted to place the second finger on the reader and begin the enrolment process again.

NOTE: If you choose to add a second finger to a user record after they have already enrolled with a first, they will be taken through the enrolment process from the beginning, which means they will need to enrol their first finger again.

9. Once the user has enrolled, click the Save button to be taken back to the user list. After 30 seconds, the system will synchronise with TrakaWEB and the user details will be updated.

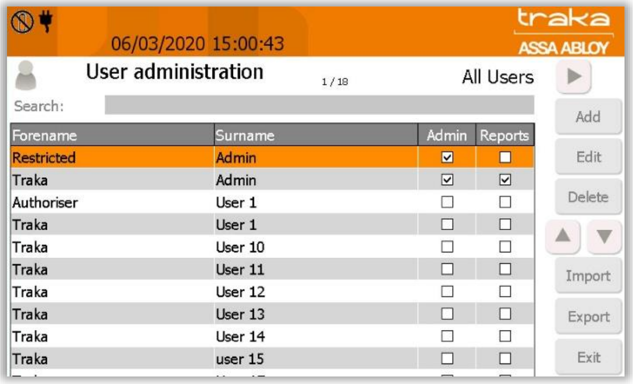
Re-Enrolling
If you wish to change the Fingerprint template that you have saved to the user, simply click the 'Enrol' button and go through the enrolment process again.

Cancel Button
By clicking the Cancel button during enrolment, you will be taken back to the enrol screen where you can select how many fingers to enrol. Doing this will erase any fingerprint templates and information from the specified user.

4.25.2 REMOVING A FINGERPRINT TEMPLATE

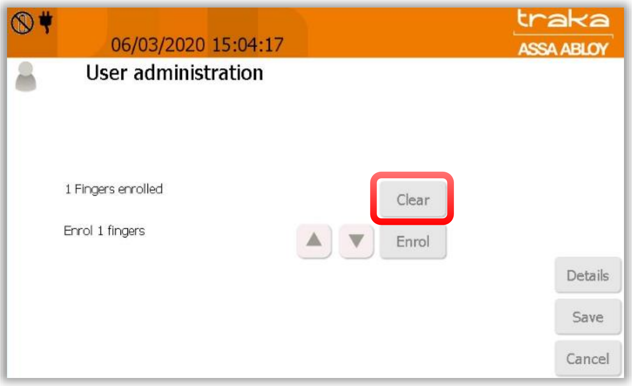
Under GDPR, the organisation must have procedures in place to enable users to withdraw their previous consent for their biometric (finger) data to be used for this process, and users must have been informed of how to initiate this process. Once consent has been withdrawn, the organisation must remove the data from the system. The user will then need a Keypad ID to access the system.

1. Log into the Traka Touch system and navigate to the User Administration page.



2. Select the enrolled user you wish to edit and navigate to the User Administration Enrolment page.

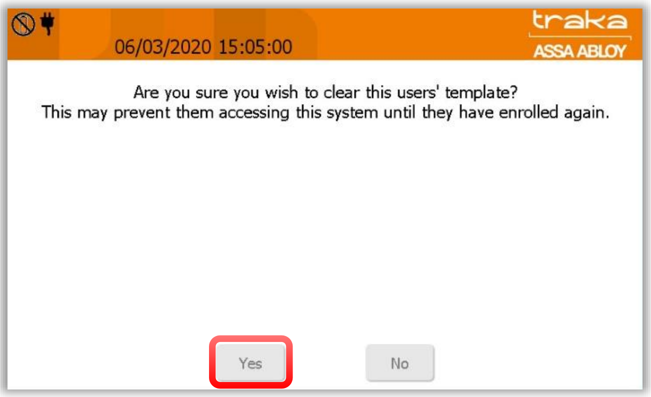
The User Administration page will now display an additional **Clear** button for an enrolled user.



3. Select the **Clear** button.

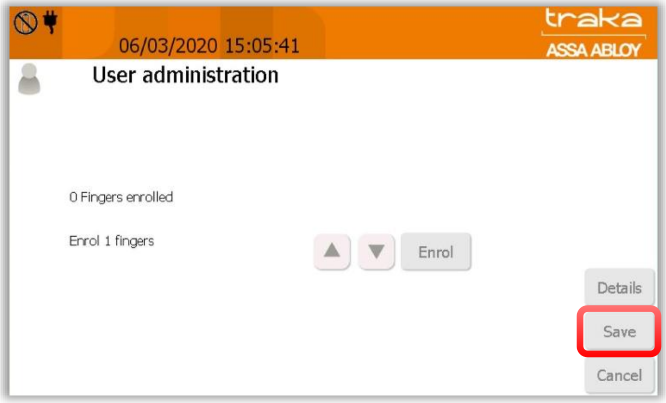
You will be presented with a message warning you that the user may no longer be able to access the system if their template is removed.

4. Select the **Yes** button.



The users' template is now removed from the database. The User Administration page will remain visible should the user require re-enrolling.

5. Once completed, select the **Save** button.



4.25.3 IDENTIFICATION

'Identification' is simply the process of the Traka system recognising a user in normal daily use. The user must be enrolled before they can do this. At the Traka System:-

Fingerprint Only

1. **Touch** the screen to bring the system out of idle mode. The Sagem reader will illuminate red. This will continue until the system moves back into idle mode.

2. **Place** your finger on the reader.

3. Once your ID has been verified, you will be able to continue to remove items or make a selection.

Fingerprint and Keypad ID/Card ID

1. **Touch** the screen to bring the system out of idle mode. The Sagem reader will illuminate red. This will continue until the system moves back into idle mode.

2. **Place** your finger on the reader **or enter** your Keypad ID/**swipe** your Card at the reader.

3. Once your Fingerprint ID and/or Keypad ID/Card ID have been verified, you will be able to continue to remove items or make a selection.

Fingerprint and PIN

1. **Touch** the screen to bring the system out of idle mode. The Sagem reader will illuminate red, this will continue until the system moves back into idle mode.

2. **Place** your finger on the reader.

3. You will then be prompted to **enter** your PIN.

Once your Fingerprint ID and PIN have been verified, you will be able to continue to remove items or make a selection.

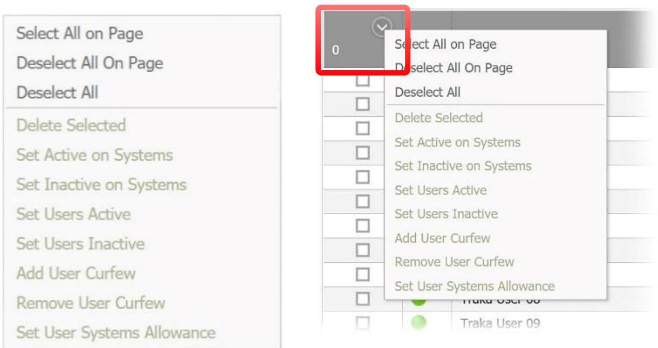
5. MULTI-SELECT/MULTI-EDIT (MSME)

5.1 USERS

The Multi-Select/Multi-Edit or MSME feature within TrakaWEB can significantly reduce the workload of a user with the Administrator role. It provides the user with the ability to add multiple users to Item Access Groups and Systems. It is also an effective method of making users active or inactive on a system as well as deleting them. This is achieved by using the right mouse button to display a context menu, which will allow the user to choose from a number of options.

5.2 THE CONTEXT MENU

The Context Menu is central to the functionality of Multi-Select/Multi-Edit and is available by right clicking the mouse within the grid or left clicking on the down arrow button above the check box column. This will display a menu with a series of options. Greyed-out options will only be made available if one or more users have been selected.



Select All on Page

Selecting this option will enable the user to select all the users listed on the current page at once.

Deselect All on Page

This option will enable the user to deselect all the selected users on the current page at once.

Deselect All

If users are selected on one or more pages, this option will enable them all to be deselected.

Delete Selected

This option will enable the user to delete all selected users over multiple pages.

Set Active on Systems

Choosing this option will display a list of available systems. This will allow any selected users to be set as active on one or more systems.

Set Inactive on Systems

This option will enable a user to remove user activity on one or more systems.

Set Users Active

Selecting this option will set any selected users to Active.

Set Users Inactive

Choosing this option will set any selected users to Inactive.

Add User Curfew

Selecting this option will allow an Absolute or Relative curfew to be added to one or more users.

Remove User Curfew

This option will allow an Absolute or Relative curfew to be removed from one or more users.

Set User Systems Allowance

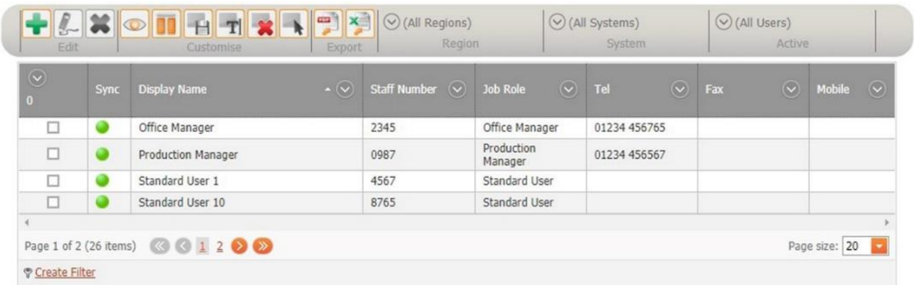
Selecting this option will enable a user to set the System Item Allowance for systems within a selected region for one or more users.

5.2.1 SELECTING USERS

Users can be selected individually or by using the context menu to select them on a page-by-page basis.

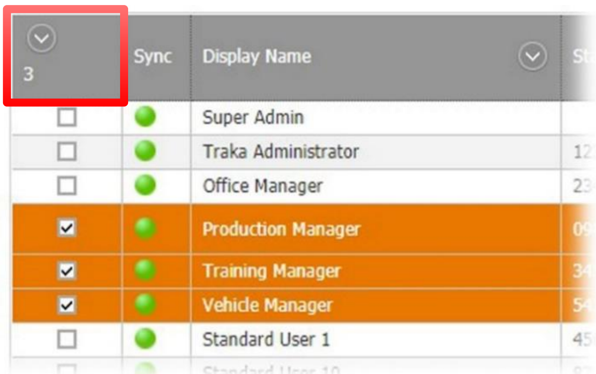
1. From the Navigation toolbar, select Users.

You will then be taken to the Users page. If you already have users set up in your Traka Touch system, then this list will be populated with all of those users along with all the other users in the database. If you have not added any users to your system, you will need to Add Users.



2. To select individual users, click in the check boxes located to the left.

NOTE: Above the column of check boxes, a number will display how many users are currently selected across all pages. This is a useful way of monitoring how many users remain selected, even if there are no users selected on the current page.



3. To select all the users on the current page, right click and choose the option **Select All on Page.**

This will select all the check boxes for all users on the current selected page only. You may also choose to Deselect All on Page or, if there are users selected over multiple pages, you can Deselect All.

NOTE: There is no option to select all users at once. This could potentially lead to a situation where they may be accidentally deleted.

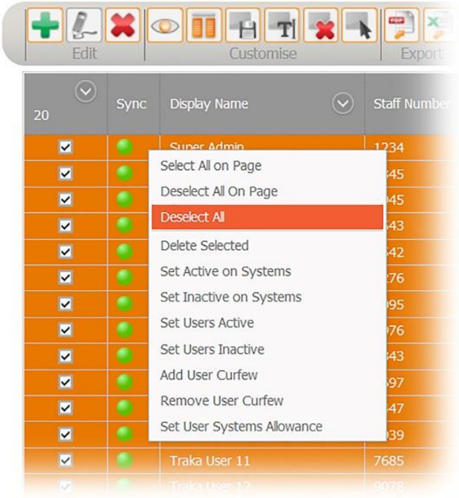
5.2.2 DESELECTING USERS

Users can be deselected individually, on a page-by-page basis or all at once.

1. To deselect an individual user, click on the corresponding check box located to the left.

2. To deselect all the users on the current page, right click and choose the option **Deselect All on Page.** This will have no effect on selected users on other pages.

3. To deselect all the users across all pages, right-click and choose the option: **Deselect All.**

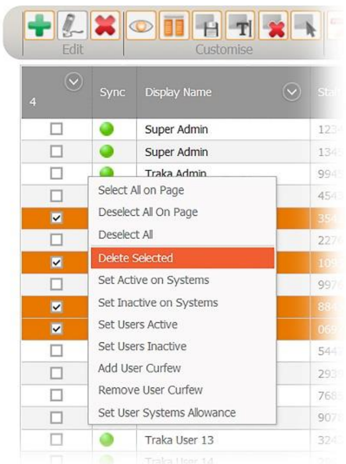


5.2.3 DELETING USERS

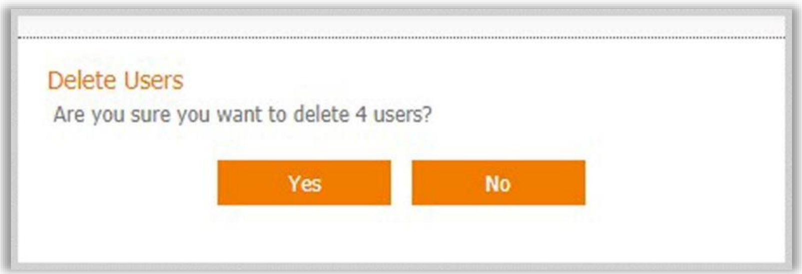
The context menu option for deleting users will only apply when one or more users are selected. This also applies to using the delete button at the top of the page. Once the delete option is selected, a window will appear requesting confirmation.

NOTE: A user will not be able to delete themselves if they are logged into TrakaWEB using their own credentials.

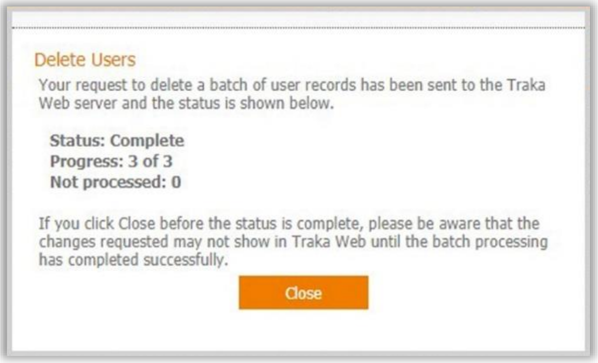
1. To delete the selected users, right click and then choose the option for **Delete Selected.**



A message will appear, requesting conformation that you wish to delete the selected users. Choosing **No** will close the window and return to the Users page. Select **Yes** to start the process.



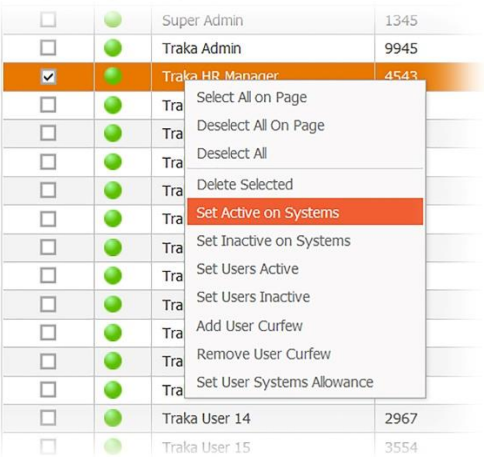
A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, the selected users will be removed.



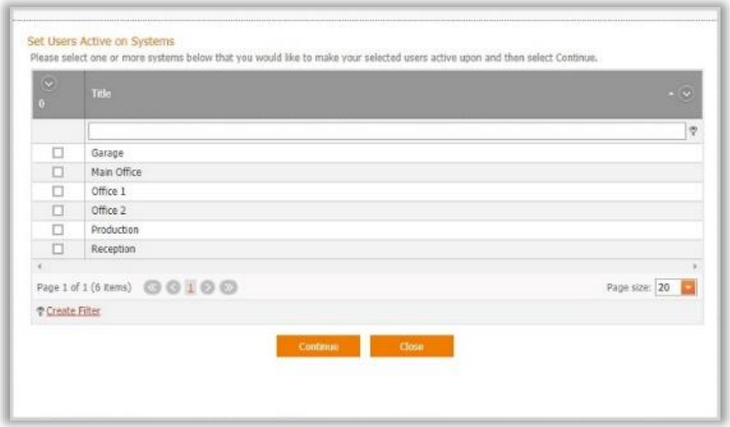
5.2.4 SETTING USERS ACTIVE ON A SYSTEM

Using the context menu to set a user active on a system is a more efficient method than navigating to the System Access tab.

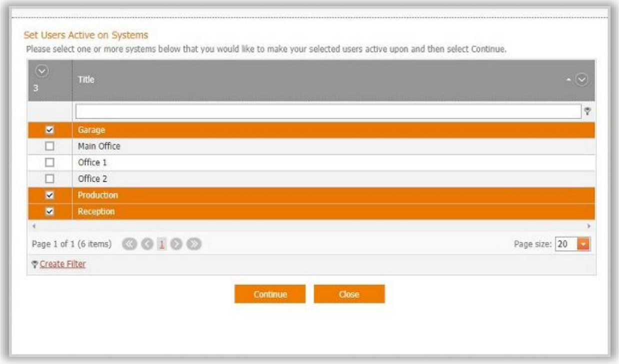
1. Select the user that you wish to set as active on a system by right clicking and choosing the **Set Active on Systems** option.



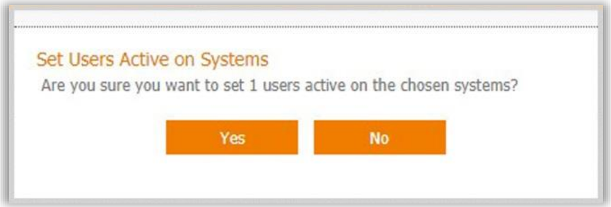
A new window will appear displaying a list of all the available systems.



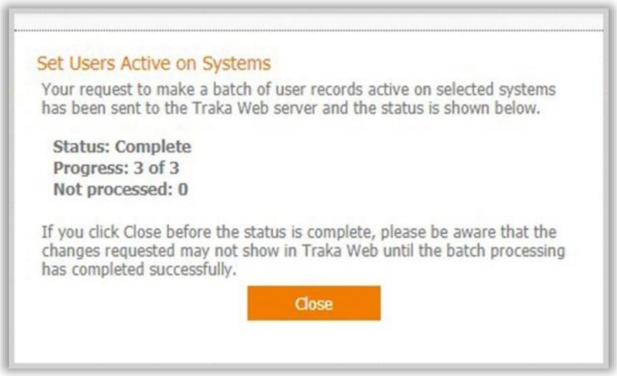
2. Select the systems that you wish to allocate to the user and then click on **Continue.**



A message will appear asking for confirmation that you wish to set the user or users' active on the selected systems. Selecting **No,** will close the message and return to the Users page. Select **Yes** to start the process.

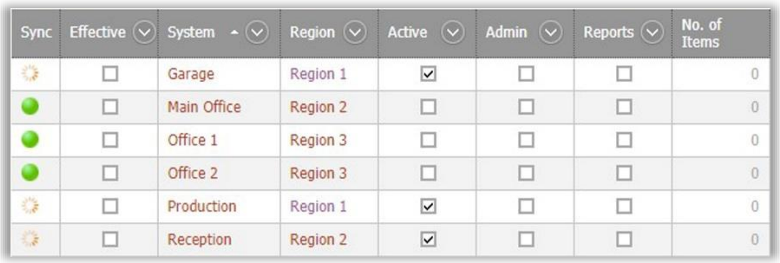


A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, the selected users will be set as active on the assigned systems.



NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run and any changes will not be displayed until the process has completed.

The user will now be set as active on the selected systems as can be seen in the example below.

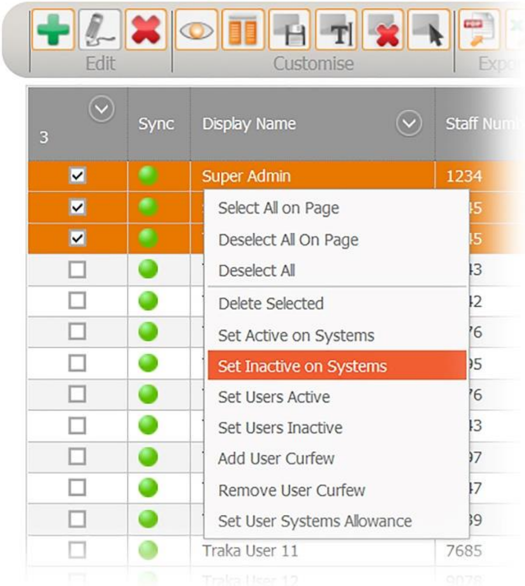


Sync	Effective	System	Region	Active	Admin	Reports	No. of Items
	☐	Garage	Region 1	☑	☐	☐	0
	☐	Main Office	Region 2	☐	☐	☐	0
	☐	Office 1	Region 3	☐	☐	☐	0
	☐	Office 2	Region 3	☐	☐	☐	0
	☐	Production	Region 1	☑	☐	☐	0
	☐	Reception	Region 2	☑	☐	☐	0

5.2.5 SETTING USERS INACTIVE ON A SYSTEM

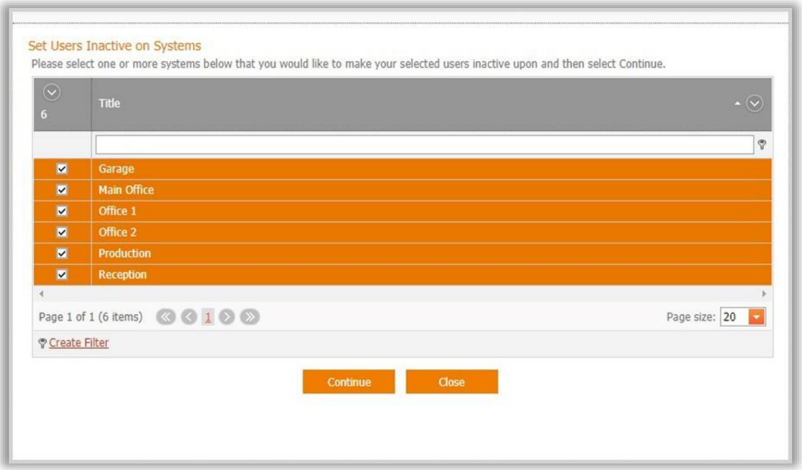
Setting users as inactive on a system will remove their ability to use whichever system or systems are selected from the list of those available.

1. Select the users that you wish to set as inactive on systems. Right click and choose **Set Inactive on Systems** from the context menu.

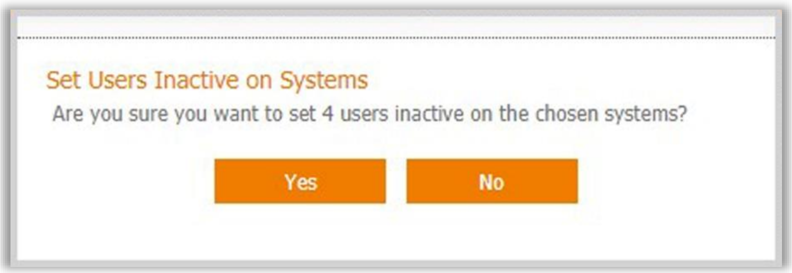


A window will now appear displaying all the available systems.

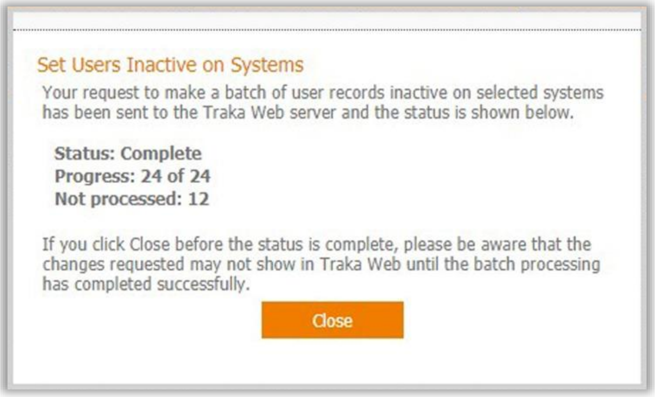
2. Select which systems you wish to set as inactive to the users.



A message will be displayed requesting confirmation that you wish to set the selected users inactive on the chosen systems. Selecting **No** will close the message and you will return to the Users page. Select **Yes** to start the process.



A window will appear, displaying the status of the process. Once completed, click on **Close.** If successful, the selected users will then be set as inactive on the selected systems.



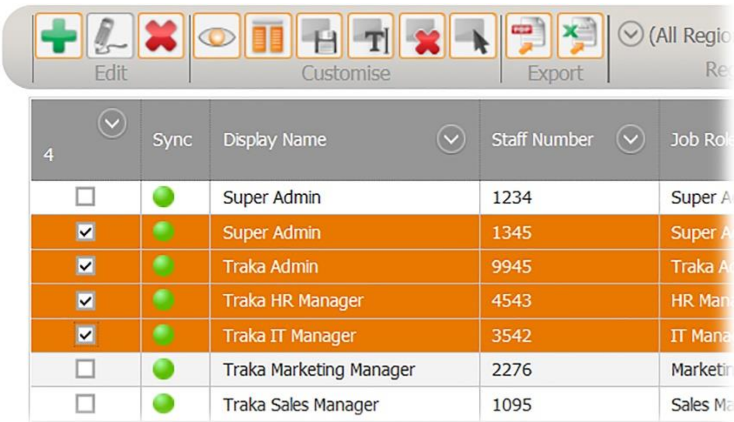
NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run and any changes will not be displayed until the process has completed.

NOTE: In the example above all four users were not assigned to any of the three available regions, therefore the 'Not Processed' result is '12'.

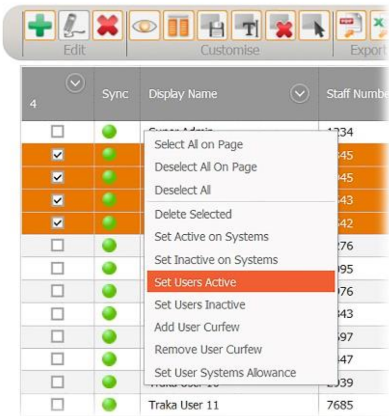
5.2.6 SETTING USERS ACTIVE

Using the context menu through the MSME feature can set a user as Active without having to navigate to the System Access tab.

1. Select the users you wish to set as active.

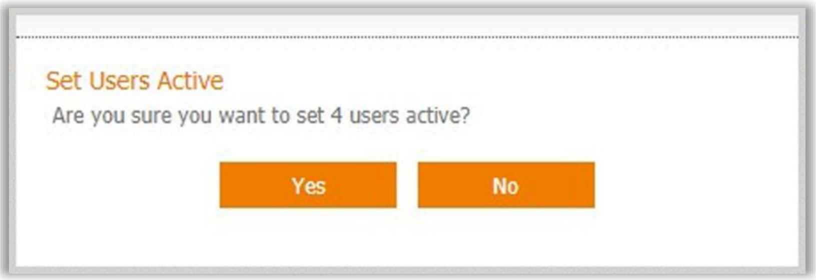


2. Right click and choose **Set Users Active** from the context menu.

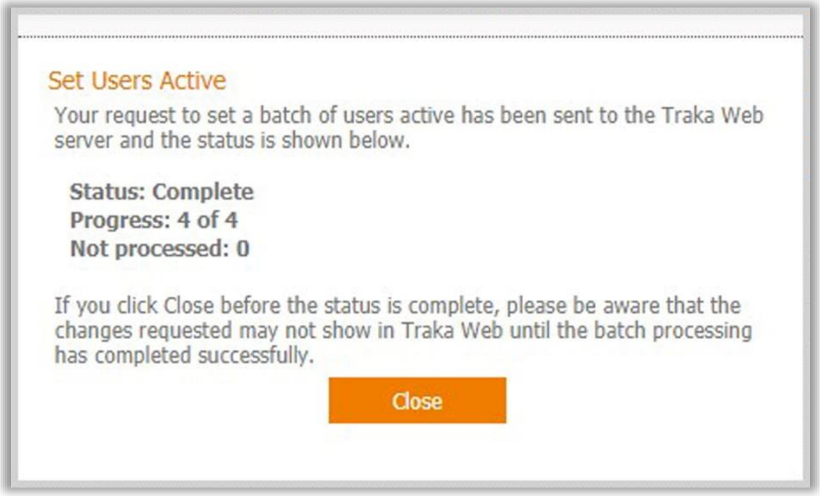


A message will be displayed requesting confirmation that you wish to set the selected users as active. Selecting **No** will close the message and you will return to the Users page.

3. Select **Yes** to begin the process.



A window will appear, displaying the status of the process. Once completed, click on **Close.** If the process was successful, the selected users will then be set as active.

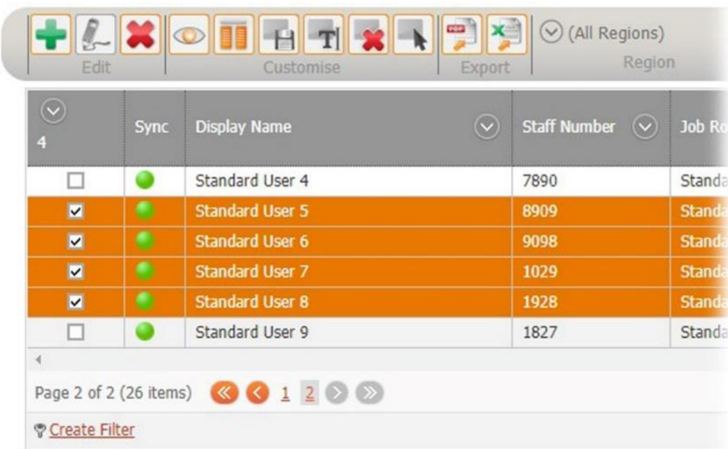


NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run and any changes will not be displayed until the process has completed.

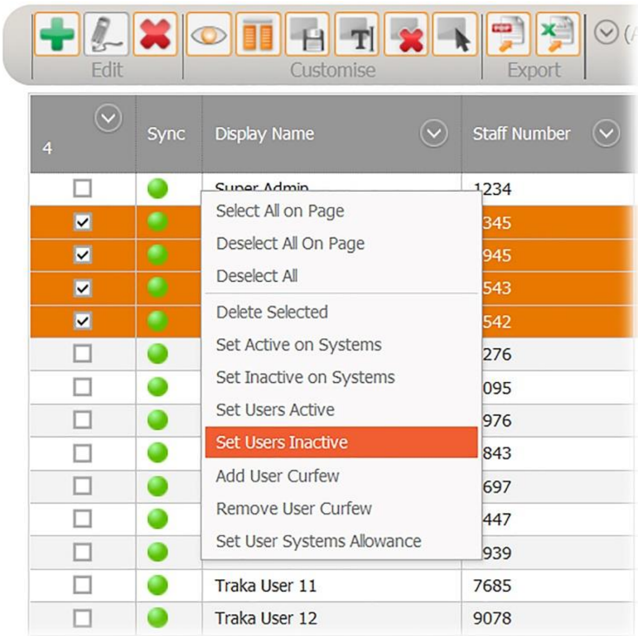
5.2.7 SETTING USERS INACTIVE

Similar to Setting Users as Active, using the context menu through the MSME feature can set a user as Inactive without having to navigate to the System Access tab.

1. Select the users that you wish to set as Inactive.

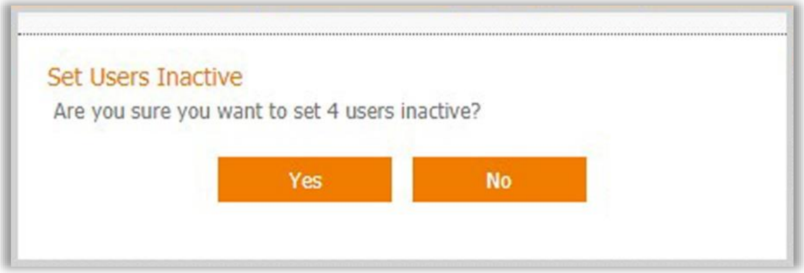


2. Right click and choose **Set Users Inactive** from the context menu.

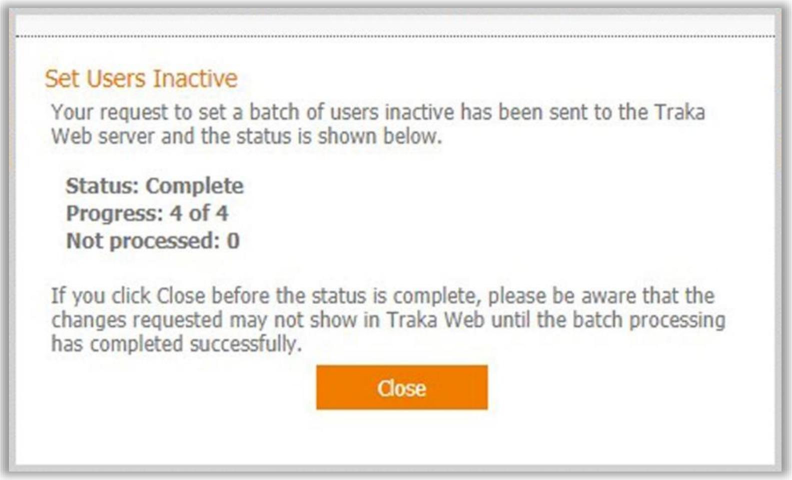


A message will be displayed requesting confirmation that you wish to set the selected users as inactive. Selecting **No** will close the message and you will return to the Users page.

3. Select **Yes** to begin the process.



A window will appear displaying the status of the process. Once completed, click on **Close.** If successful, the selected users will then be set as inactive.

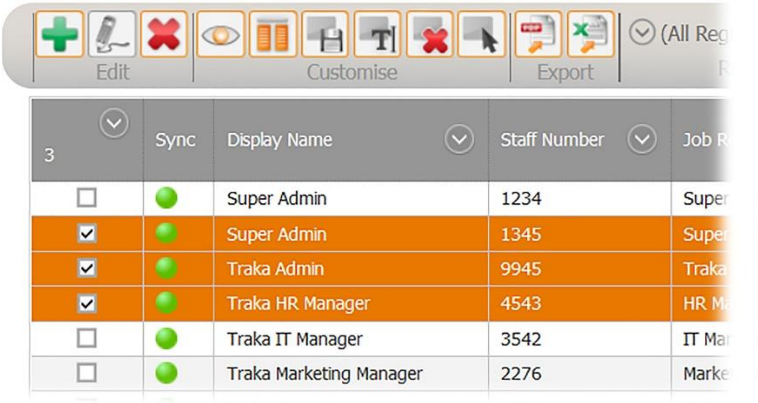


NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run, and any changes will not be displayed until the process has completed.

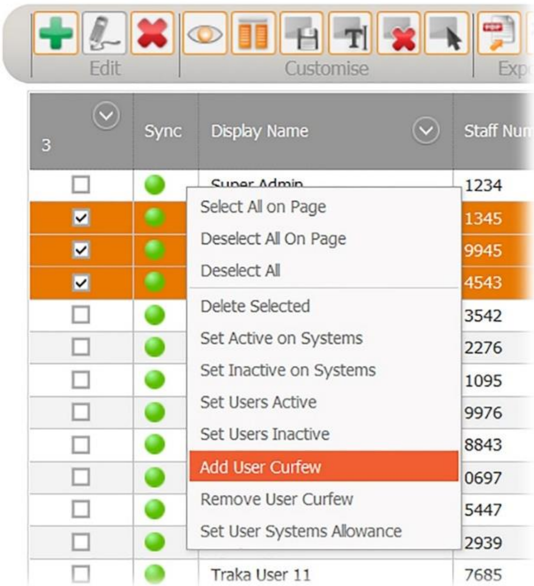
5.2.8 ADD USER CURFEW

The Add User Curfew option will enable you to apply either a relative or absolute curfew to a user and select the region and system on which the user is active.

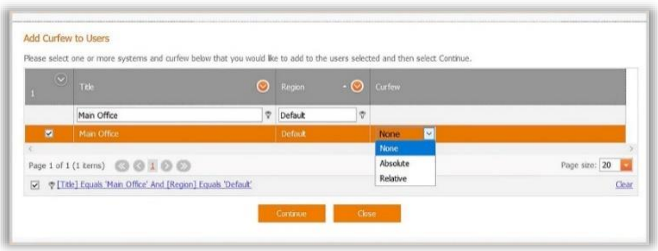
1. Select the user or users to which you wish to apply the curfew.



2. Right click and select **Add User Curfew** from the context menu.



3. A window will now appear. You can now select the system, the region and the type of curfew that you wish to apply.



4. Select Continue to progress with adding the curfew information.

For an **Absolute** curfew, use the arrows to enter the required hours and minutes.

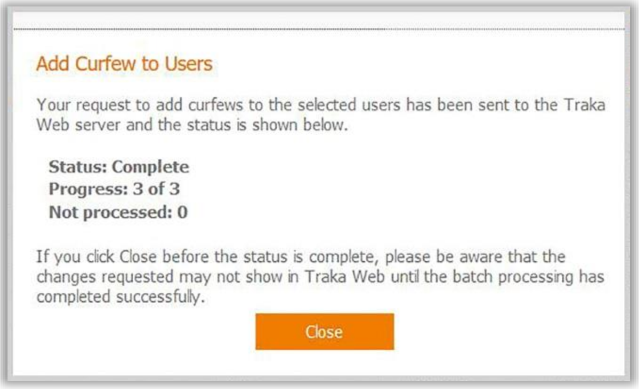
For a **Relative** Curfew, use the arrows to enter the required days, hours and minutes.

5. Once you completed the selection, click on **Continue.**

A message will be displayed requesting confirmation that you wish to add the curfew. Selecting **No** will close the message and you will return to the Users page.

6. Select **Yes** to begin the process

A window will appear displaying the status of the process. Once completed, click on **Close.** If successful, the curfew will be added to the selected users.

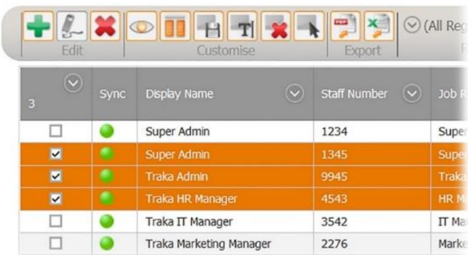


NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run and any changes will not be displayed until the process has completed.

5.2.9 REMOVE USER CURFEW

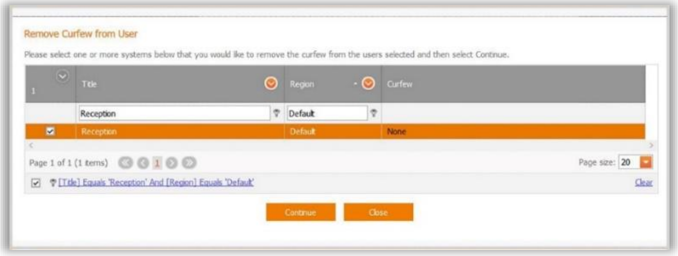
The **Remove User Curfew** will enable you to remove an absolute or relative curfew that has been applied to one or more users.

1. Select the user or users whom you wish to remove a curfew.



2. Right click and select **Remove User Curfew** from the context menu.

A window will now appear. You can now select the system of the region for the curfew that you wish to remove.

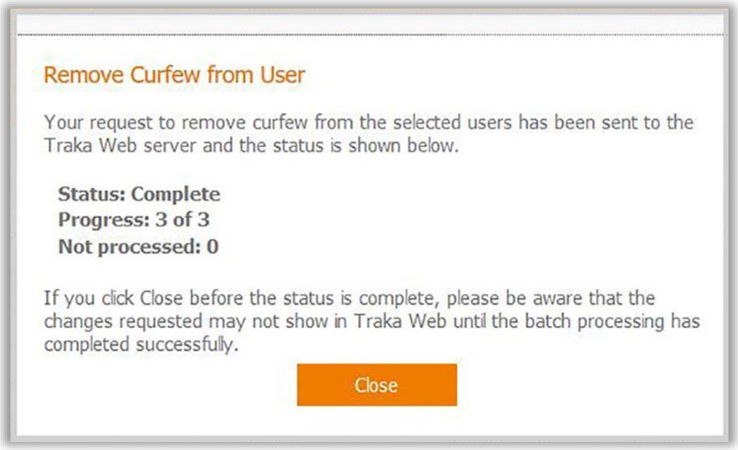


3. Select **Continue** to progress with the curfew removal.

A window will appear requesting confirmation that you wish to remove the curfew from the users.

4. Select **Yes** to begin the process.

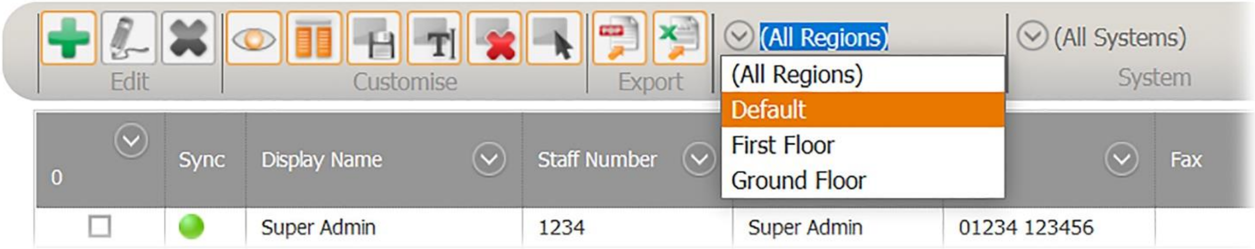
A window will appear displaying the status of the process. Once completed, click on **Close.** If successful, the curfew will be removed from the selected users.



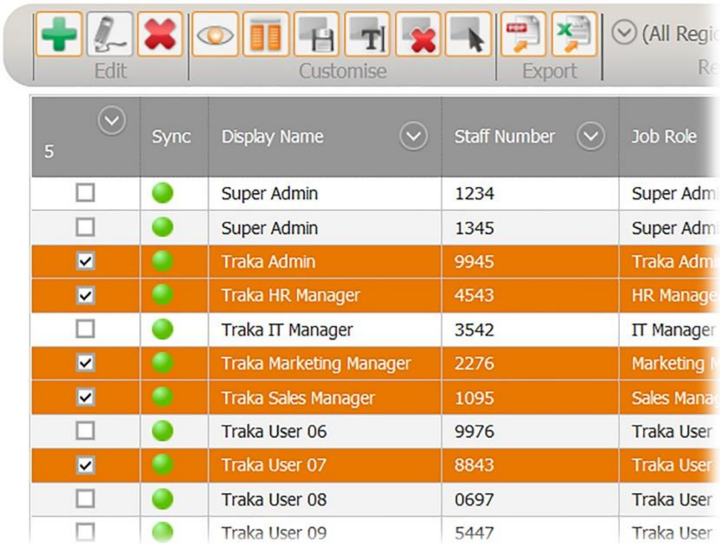
5.2.10 SET USER SYSTEMS ALLOWANCE

The **Set User Systems Allowance** option will enable a user to set the System Item Allowance on systems within a selected region for one or more users.

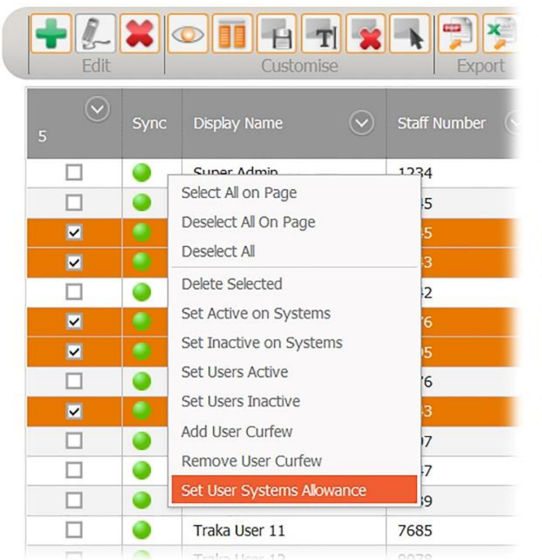
1. From the Users page, select the region that you wish to select the systems for allocating the User Systems Allowance.



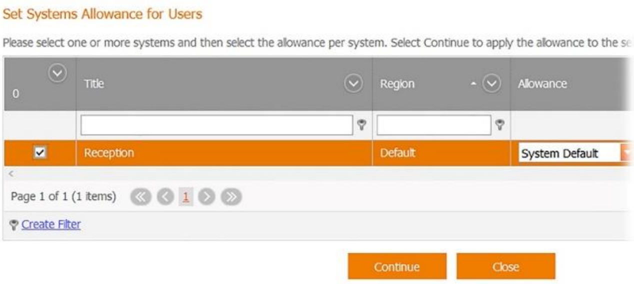
2. Select the user or users that you wish to set the User Systems Allowance.



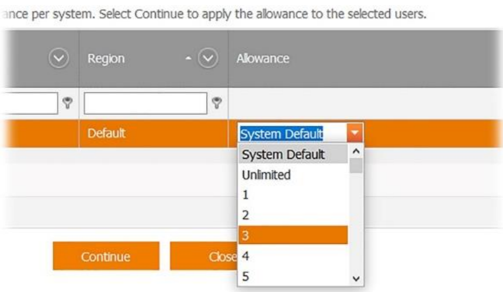
3. Right click within the grid and select **Set Users Systems Allowance** from the context menu.



4. At the next screen, select the system or systems for the selected region by clicking in the checkbox to the left.



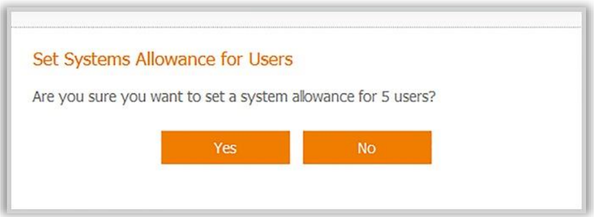
5. Over to the right of the screen, select the drop down menu in the Allowance column and select the Item Allowance for the selected users.



6. Now Select the **Continue** button.

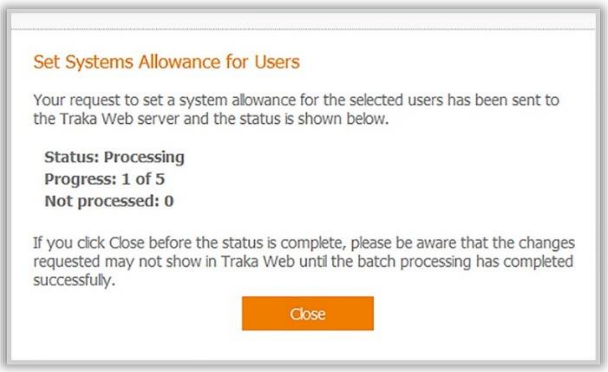
A window will now appear requesting confirmation to Set Systems Allowance for Users.

7. Select **Yes** to continue.



A window will now appear showing the progress and status of the process.

8. Once completed, click on the **close** button.



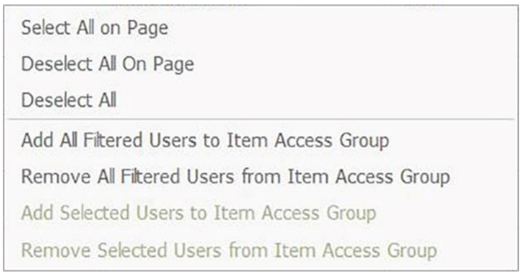
The selected users will now be granted the specified item allowance for the selected system(s) for that particular region.

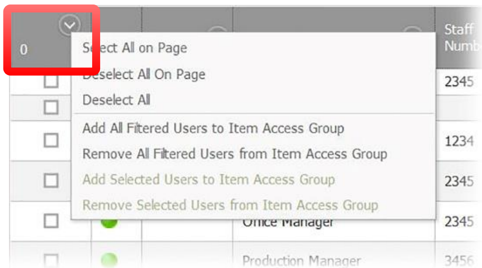
5.3 ITEM ACCESS GROUPS

Using MSME to assign Users and Items to Item Access Groups utilises the same functionality as assigning Users to systems. A User with the Administrator role will be able to select one or more users by using a context menu and selecting which Item Access Group that they will become a member. As well as assigning users to an Item Access Group, they can also be removed.

5.3.1 THE CONTEXT MENU

The functionality of the Context Menu is made available by right clicking the mouse within the grid or left clicking on the down arrow button above check box column. This will display a menu with a series of options. Greyed-out options will only be made available if one or more users have been selected.





Select All on Page

Selecting this option will enable the user to select all the users listed on the current page at once.

Deselect All on Page

This option will enable the user to deselect all the selected users on the current page at once.

Deselect All

If users are selected on one or more pages, this option will enable them all to be deselected at once.

Add All Filtered Users to Item Access Group

With a number of filtered users on a page such as users of the same job description for example, this option will enable you to add those users to a specific Item Access Group.

Remove All Filtered Users to Item Access Group

This option will enable you to remove all the filtered users on the page from a specific Item Access Group.

Add Users to Item Access Groups

This option will enable the user to assign selected users to a specific Item Access Group.

Remove Users from Item Access Group

Choosing this option will enable the user to remove one or more users from a specific Item Access Group.

5.3.2 SELECTING ITEM ACCESS GROUPS

You will be required to have one or more Item Access Groups created to proceed with using the MSME functionality. Information for creating Item Access Groups can be found in the Item Access Groups section.

1. From the Navigation Toolbar, select the Item Access Groups icon from the Items option.

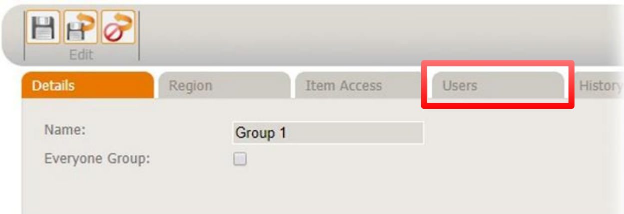
You will then be taken to the Item Access Groups page, showing a list of existing groups.

2. Select a group by double clicking on it or by selecting it and then clicking on the Edit button.

You will now be directed to the Edit Item Access page.

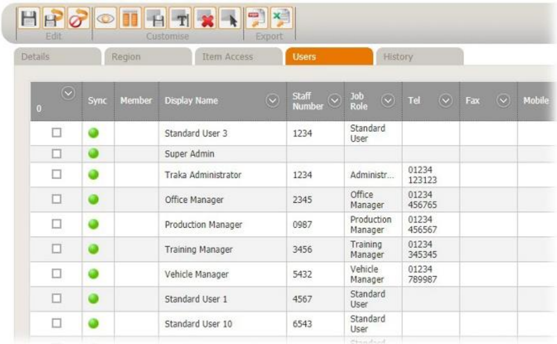
5.3.3 SELECTING USERS TO ASSIGN TO ITEM ACCESS GROUPS

1. From the Edit Item Access Group page, select the Users tab.



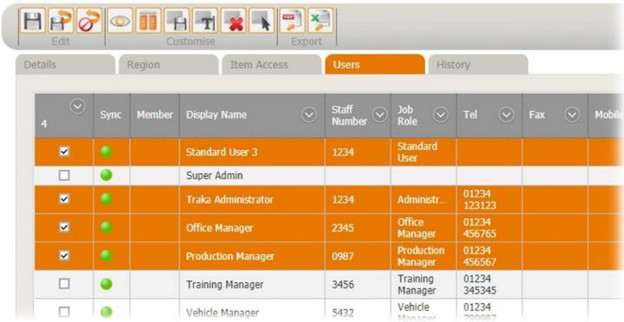
NOTE: If any of the Item Access Groups have the Everyone Group option ticked, the Users tab will not be available.

The next page will display all the available user details.



NOTE: It will be noticed that there is an empty column titled 'Member'. For users that are assigned to groups, the corresponding Member box will be ticked.

2. Select individual users to assign to the Item Access Group by clicking on the check boxes to the left.



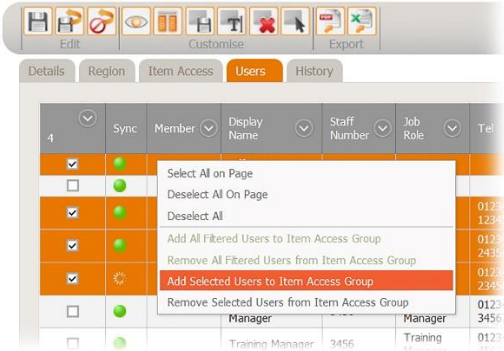
NOTE: Above the check box column, the number of selected users is displayed.

3. If you wish to select all the users on the page, right click and choose **Select All on Page**.

This will select all the check boxes for all users on the current page only. You may also choose to **Deselect All on Page** or, if there are users selected over multiple pages, you can **Deselect All**.

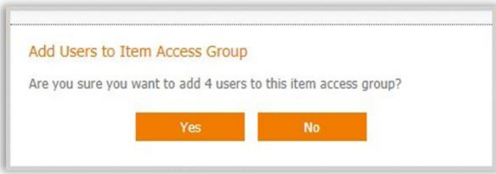
5.3.4 ADD USERS TO ITEM ACCESS GROUPS

1. With the users selected, right click and select **Add Selected Users to Item Access Group.**

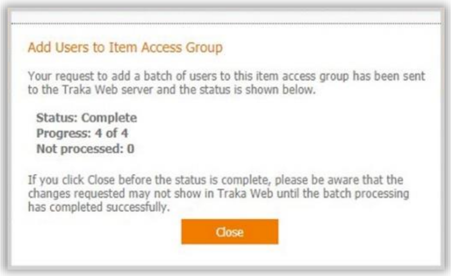


You will be presented with a confirmation window asking if you wish to add the selected users to the Item Access Group. Selecting **No**, will return you to the list of user details.

2. Click on **Yes** to proceed.

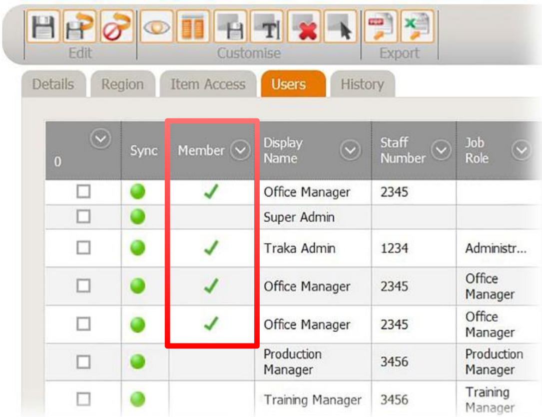


A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, the selected users will be added to the Item Access Group.



NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run and any changes will not be displayed until the process has completed.

The Users page will now be updated. A tick is visible in the Member column for all users assigned to that group.



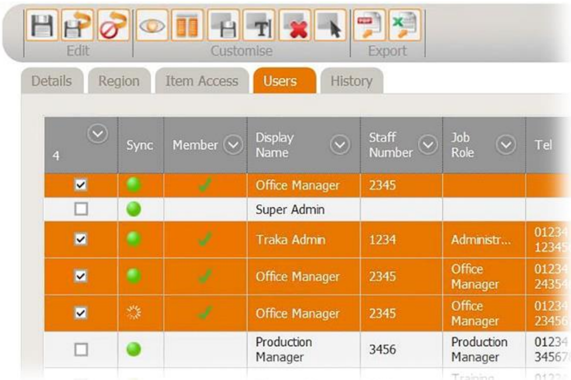
NOTE: The tick in the Member column will only appear for users whom are members of the selected Item Access Group.

The process can then be repeated for assigning users as members of other Item Access Groups.

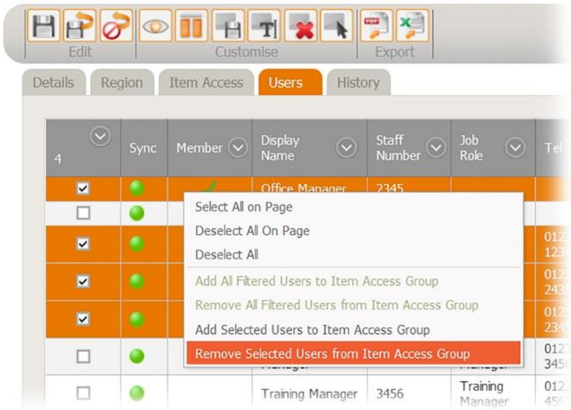
5.3.5 REMOVE USERS FROM ITEM ACCESS GROUP

As well as adding users to an Item Access Group, it may also be necessary to remove one or more users from an Item Access Group.

1. Select the Item Access Group from which you wish to remove user access and then click on the Users tab.
2. Select the assigned users that you wish to remove from that group.

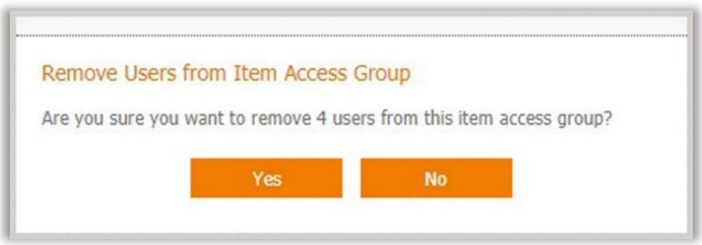


3. Right click and choose the option **Remove Selected Users from Item Access Group.**

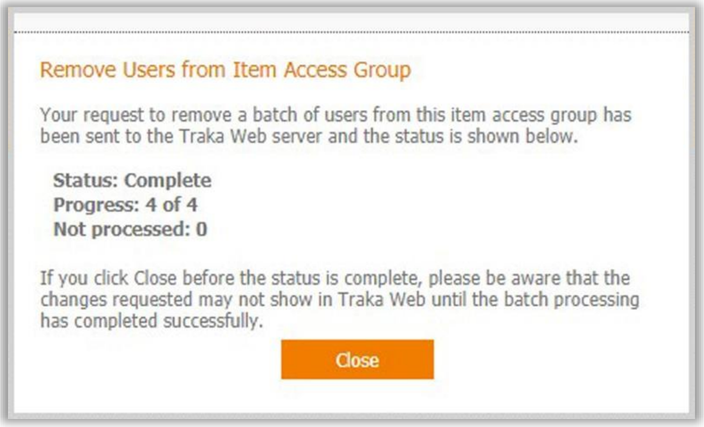


You will be presented with a confirmation window asking if you wish to remove the selected users from the Item Access Group. Selecting **No**, will return you to the user details list.

4. Click on **Yes** to proceed.



A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, the selected users will be removed from the Item Access Group.

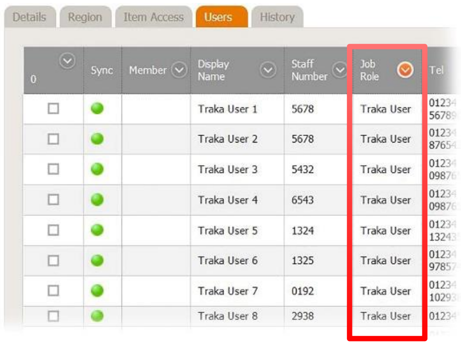


NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run and any changes will not be displayed until the process has completed.

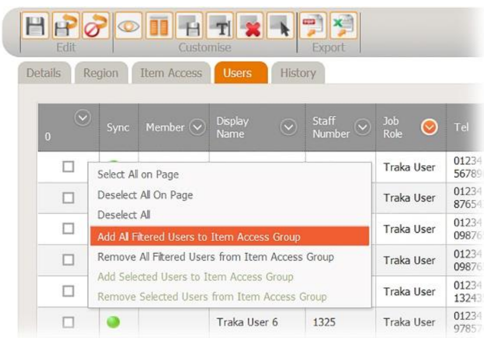
5.3.6 USING THE FILTERING OPTION

Using the filtering option for Users in MSME is very similar to adding and removing selected users. The following is an example of using an applied filter to the Job Role column.

1. Apply the filter to the column. In this example, the job role of Traka User is used.



2. Next, right click within the grid and select the option for **Add All Filtered Users to Item Access Group.**

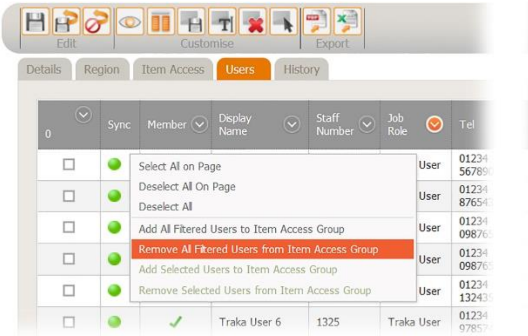


The process for adding will now proceed according to the process used for **Add Selected Users to Item Access Group.**

NOTE: If individual users have been selected from the filtered column, the Add Selected Users to Item Access Group will apply.

Removing filtered users is also very similar to the process for **Remove Selected Users from Item Access Group.**

3. With the filter in place, right click within the grid and select **Remove All Filtered Users from Item Access Group.**



The removal process will now proceed according to the process used for **Remove Selected Users to Item Access Group.**

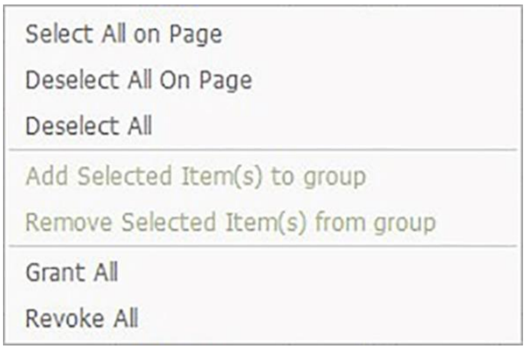
NOTE: If individual users have been selected from the filtered column, the Remove Selected Users from Item Access Group will apply.

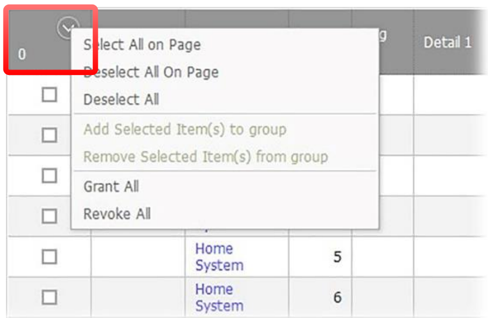
5.4 SELECTING ITEMS TO ASSIGN TO ITEM ACCESS GROUPS

Once the users are assigned to Item Access Groups, it is possible to assign Items in a similar way.

5.4.1 THE CONTEXT MENU

The functionality of the Context Menu is made available by right clicking the mouse within the grid or left clicking on the down arrow button above check box column. This will display a menu with a series of options. Greyed-out options will only be made available if one or more items have been selected.





Select All on Page

Selecting this option will enable the user to select all the items listed on the current page at once.

Deselect All on Page

This option will enable the user to deselect all the selected items on the current page at once.

Deselect All

If items are selected on one or more pages, this option will enable them all to be deselected at once.

Add Selected Item(S) to group

With one or more items selected, this option will enable them to be added to the group.

Remove Selected Item(S) from group

With one or more previously assigned items selected, this option will enable you to remove them from the group.

Grant All

This option will enable you to grant access to all items

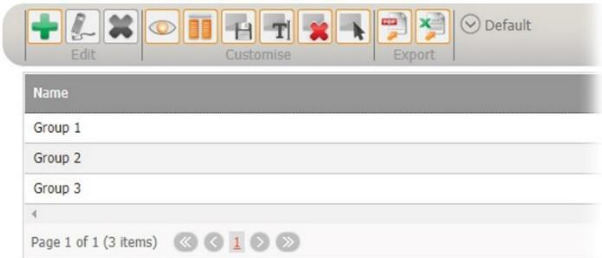
Revoke All

This option will enable you revoke access to all items in the group.

5.4.2 SELECTING ITEM ACCESS GROUPS

You will be required to have one or more Item Access Groups created to proceed with using the MSME functionality. Information for assigning items can be found in the Item Access Groups section.

1. From the Navigation Toolbar, select the Item Access Groups icon from the Items option.



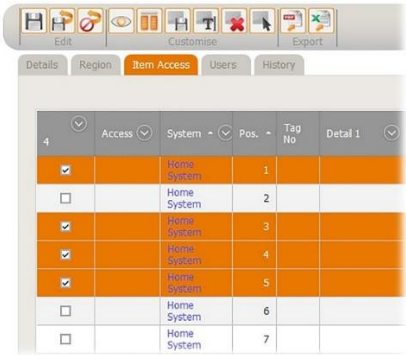
2. Select a group by double clicking on it or by selecting it and then clicking on the Edit button.

You will now be directed to the Edit Item Access page for the selected group.

3. Select the **Item Access** tab.

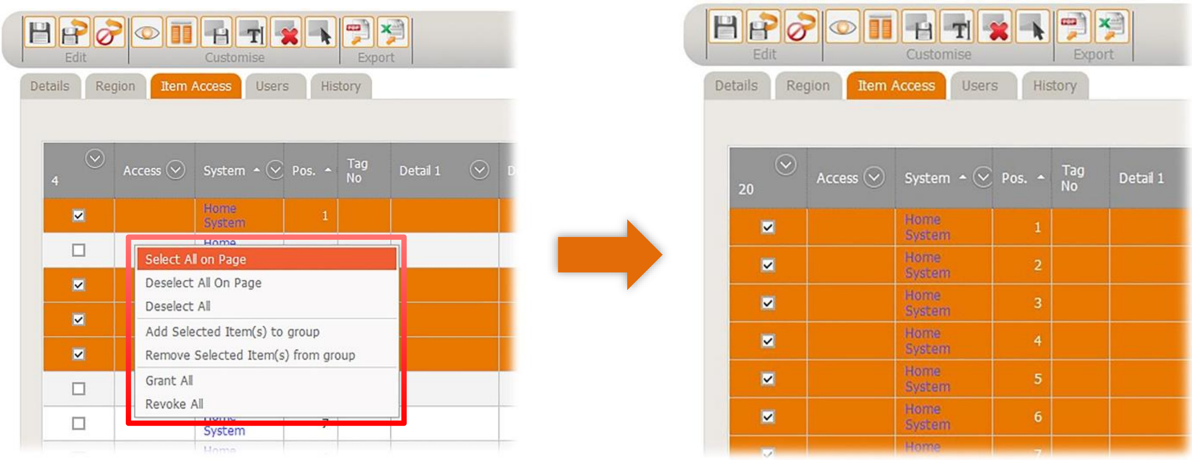
The next page will display a list of the items in the system.

4. Select individual items to assign to the Group by clicking on the check boxes to the left.



NOTE: Above the check box column, the number of selected users is displayed.

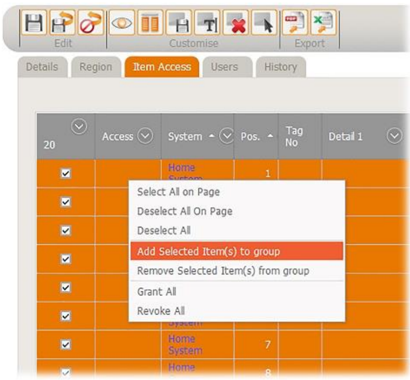
5. If you wish to select all the users on the page, right click and choose **Select All on Page**.



This will select all the check boxes for all items on the current page only. You may also choose to **Deselect All on Page** or, if there are items selected over multiple pages, you can **Deselect All**.

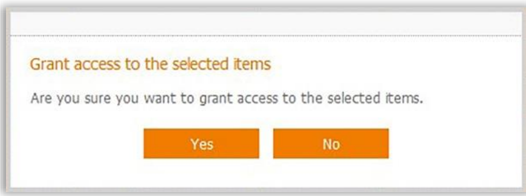
5.4.3 ADD SELECTED ITEM(S) TO GROUP

1. With the items selected, right click and select **Add Selected Item(s) to Group.**

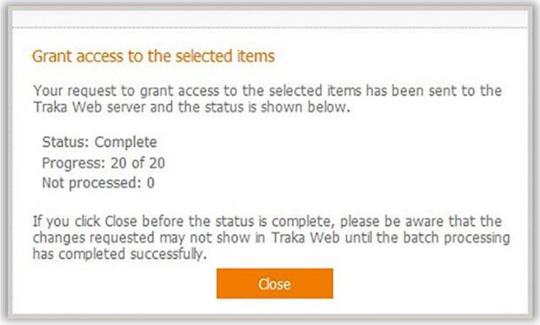


You will be presented with a confirmation window asking if you wish to grant access to the selected items. Selecting **No**, will return you to the list of user details.

1. Click on **Yes** to proceed.



A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, the selected items will be granted access.



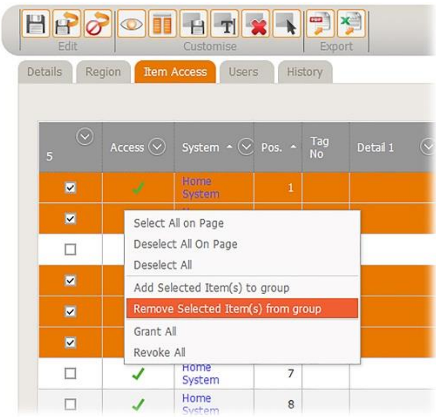
NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run, and any changes will not be displayed until the process has completed.

The page will now be updated. A tick is visible in the Access column for all access granted items in that group.

5.4.4 REMOVE SELECTED ITEM(S) FROM GROUP

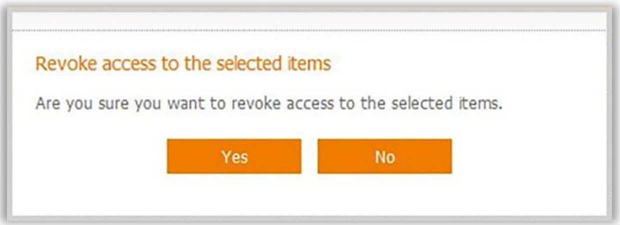
As well as granting access to items for the selected group, it may also be necessary to remove access to one or more items from a selected group.

1. Select the Item(s) from which you wish to remove access, then right click within the grid, and choose **Remove Selected Item(s) from group.**

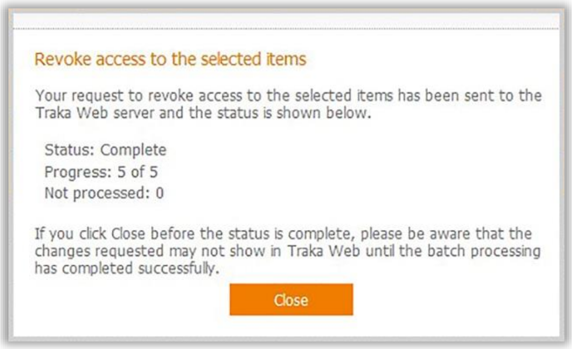


You will be presented with a confirmation window asking if you wish to revoke access to the selected items. Selecting **No**, will return you to the user details list.

1. Click on **Yes** to proceed.



A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, the selected items will have their access revoked.

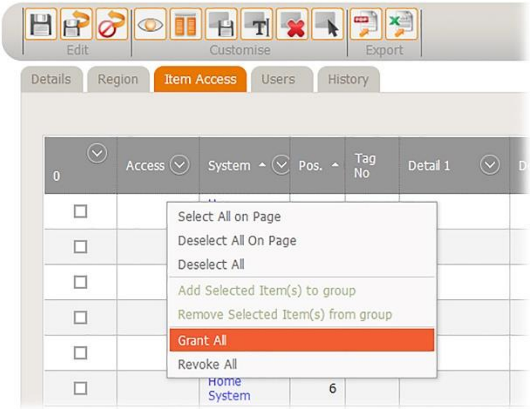


NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run, and any changes will not be displayed until the process has completed.

5.4.5 GRANT ALL

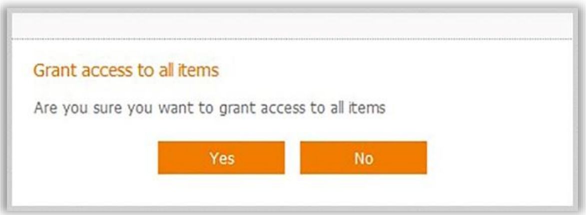
Selecting the **Grant All** option from the context menu will grant access to all items in the selected group.

1. Right click within the grid and select **Grant All** from the context menu.

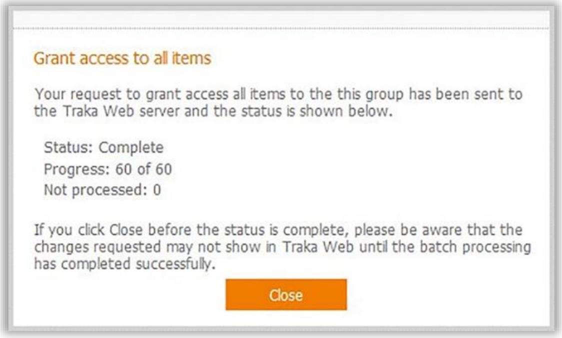


A message will appear requesting confirmation that you wish to grant access to all items.

2. Click on **Yes** to continue.

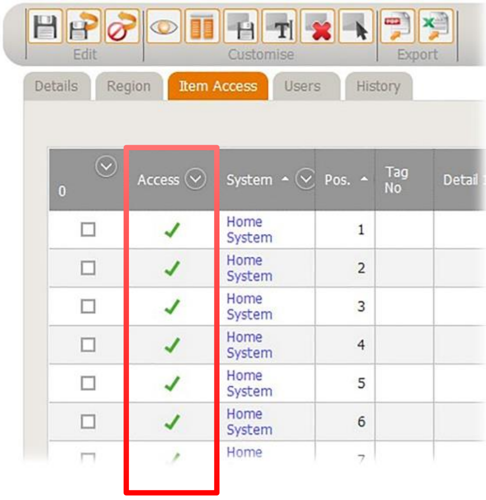


A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, all the items in the system will be granted access.



NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run, and any changes will not display until the process has completed.

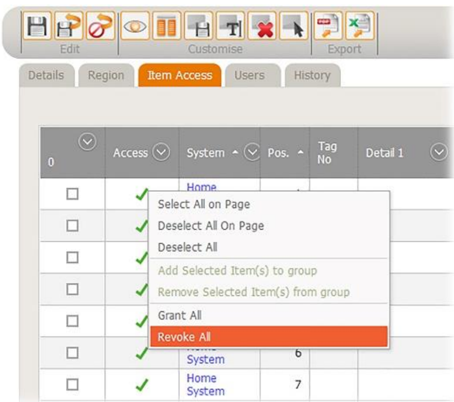
Once completed, a green tick will display in the Access column next to every item listed in the system.



5.4.6 REVOKE ALL

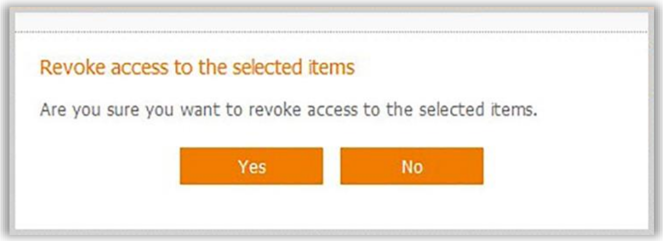
It is possible to revoke access to all items that have access granted to them by selecting the Revoke All option from the context menu.

1. Right click within the grid and choose **Revoke All** from the context menu.

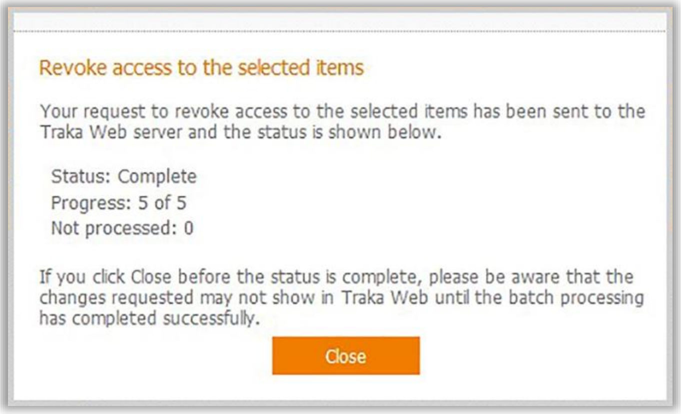


A message will appear requesting confirmation that you wish to revoke access to all items in the group.

2. Click on **Yes** to continue.



A window will appear displaying the progress and status. Once completed, click on the **Close** button. If the process was successful, all the items in the system will have their access revoked.



NOTE: Clicking on Close before the status is complete will not cancel the operation. The batch process will continue to run, and any changes will not display until the process has completed.

6. FEATURE OPTIONS

6.1 FEATURE OPTIONS OVERVIEW

Features are a powerful set of configuration options that can be tailored to suit your needs. They can be enabled or disabled through TrakaWEB Admin and can perform a highly configurable set of functions, depending on your requirements. This guide has been prepared in order to assist you with all aspects of the Feature Options available for TrakaWEB and how to use them in conjunction with your Traka Touch Key Cabinet or Locker system.

NOTE: Please refer to the Traka support site for the latest compatibility information of TrakaWEB and Traka Touch products.

http://support.traka.com

6.2 FAULT LOGGING

Fault Logging is a very powerful feature available for both Key Cabinets and RFID Locker Systems. It allows a user to record faults against items, such as vehicles or laptops. Subsequently, depending on the criticality of the fault, access can be restricted to those items to prevent further damage, wasted time or injury. An example of its use could be for a flat tyre on a vehicle.

Fault Logging can be used in 2 ways:

1. Generate and clear faults at both TrakaWEB and the Traka Touch system.

2. Generate and clear faults using TrakaWEB only.

The way in which Fault Logging is used is determined in the configuration process and will already have been setup at Traka. Should you require a change to this configuration please contact Traka or your Distributor.

6.2.1 ENABLING FAULT LOGGING

The Fault Logging feature will need to be enabled on your Traka Touch system by loading a configuration file. This is normally done by Traka during production, but if you wish to add the feature to your existing system, please contact Traka or your Distributor for further details.

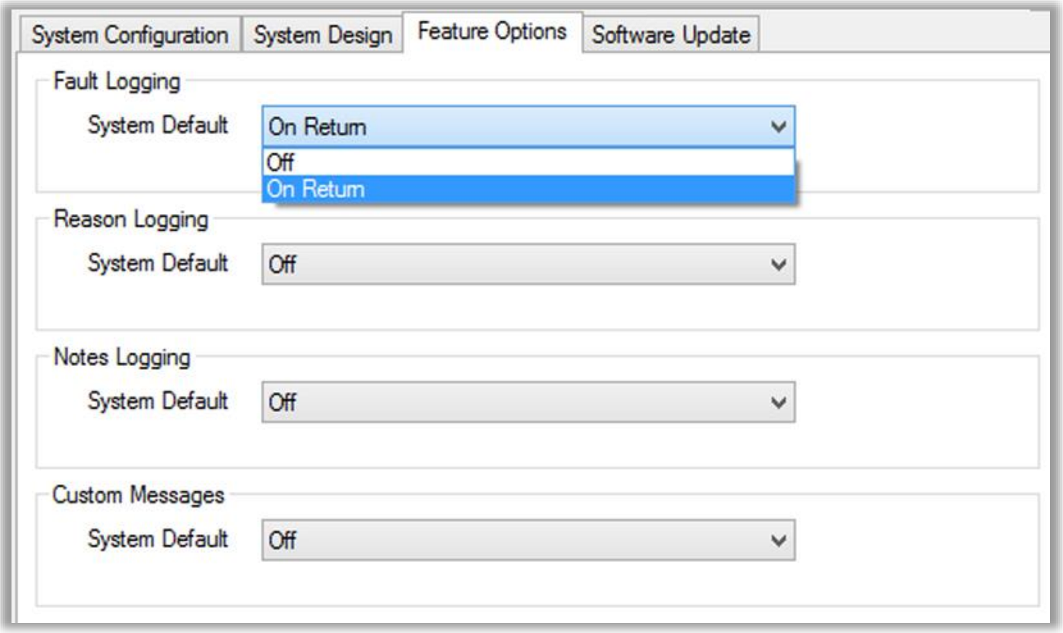
Another configuration option is 'Allow Fault Logging at System', which controls whether faults are able to be added at the Traka Touch by the user of the system. If this option is off, you will only be able to add faults using TrakaWEB. Traka also sets up this sub-option configuration.

Once your Traka Touch system is configured for Fault Logging, you will need to set up additional options using the TrakaWEB Administration application, as follows:

1. Launch the TrakaWEB Admin app, expand the System Management node in the tree on the left and choose the system to be configured.

2. Select the Feature Options tab on the right and check the Fault Logging section. Here you will find the option to set fault logging ON or OFF by default for all iFobs/items in the system.

NOTE: This default can still be overridden on an individual iFob/item basis.



When Fault Logging is first switched on, all iFobs/items are set to: Fault Logging=System Default. This means that you can set all iFobs/items to ON if you change the Fault Logging system default in the Admin App to ON, or alternatively, set all iFobs/items to OFF if the Admin App is set to default: OFF. The table shows configurations for most scenarios:

Requirement	Fault Logging System Default	iFobs/items
All items need Fault Logging	ON	All left at 'System Default'
Most items need Fault Logging	ON	Change iFobs/items that do NOT participate from Default to Fault Logging: OFF
Some items need Fault Logging	OFF	Change iFobs/items that DO participate From Default to Fault Logging: ON
No items currently need Fault Logging	OFF	All left at 'System Default'

6.2.2 ENABLING FAULT LOGGING ON A PER IFOB/ITEM BASIS

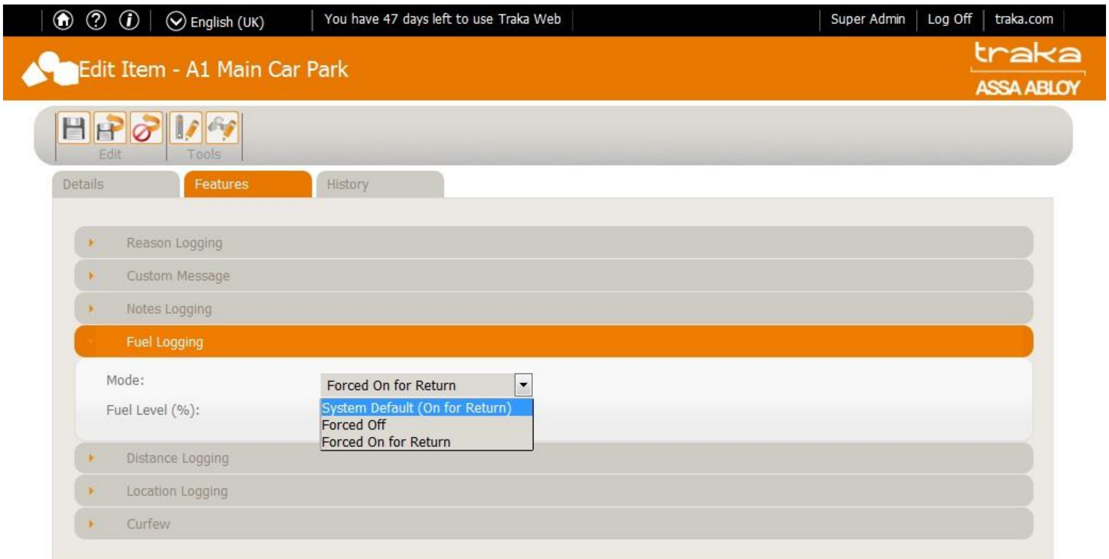
NOTE: This section only applies if your system is configured to allow faults to be logged and cleared at the Traka Touch system.

It is possible to individually enable/disable the fault logging option on a per iFob/item basis.

1. From the system viewer select the desired position and select 'Edit iFob' from the Ribbon Toolbar.
2. Select the Features tab. The example here assumes that during setup, the Fault Logging system default has been set to 'On'. In which case, the following 3 options are available from the Fault Logging drop down.

- System Default (On) – the iFob/item will follow the system default setting
- Forced Off – fault logging for this iFob/item will always be off even if the system default changes to 'ON'
- Forced On for Return – will switch the option on for this iFob/item

NOTE: Fault logging will not operate on an iFob (RFID Tag on lockers) until it has one or more items allocated to it and the item type of those items has faults defined. Once an item is allocated, it then has an Item Type. Refer to the section Adding an Item to an iFob for more details.

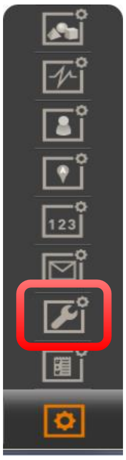


6.2.3 CREATING AND EDITING FAULT DEFINITIONS

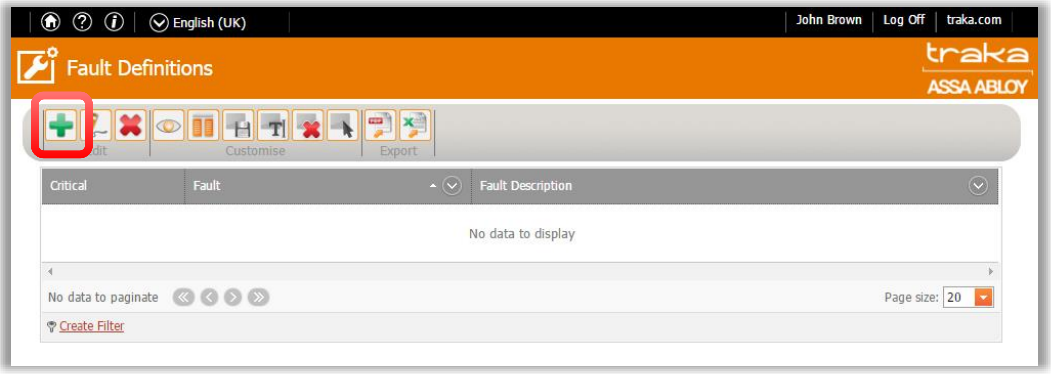
When a Fault is logged against an item, the fault type must be selected from a predefined list of Fault Definitions. These Fault Definitions may include faults such as 'Brakes Faulty', if referring to a vehicle, or 'Cracked Screen' if referring to a Laptop, and any other fault that could occur to any type of item in your system.

NOTE: To create Fault Definitions the user must first have the correct Software Permissions. Refer to the Fault Logging Software Permissions section for more details.

1. To create a Fault Definition, select 'Software Settings>Fault Definitions' from the Navigation Toolbar.

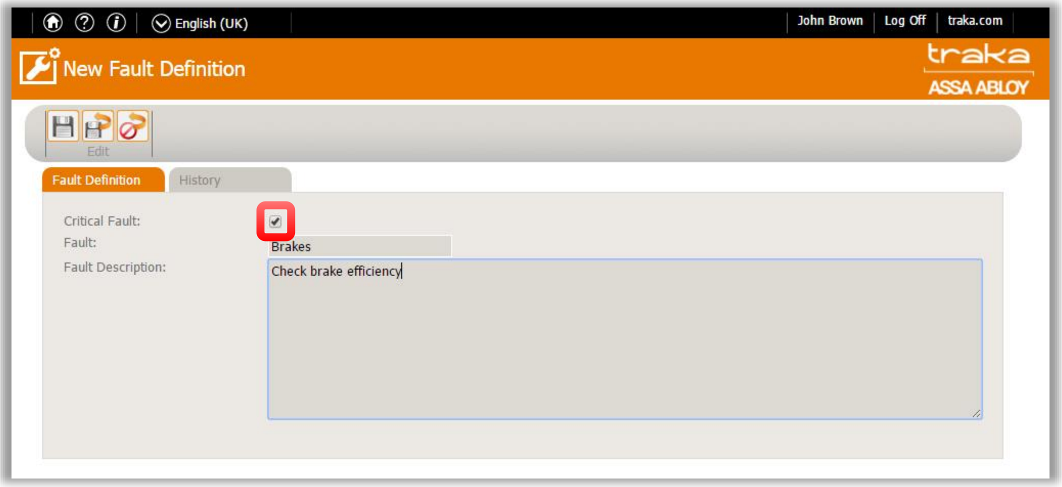


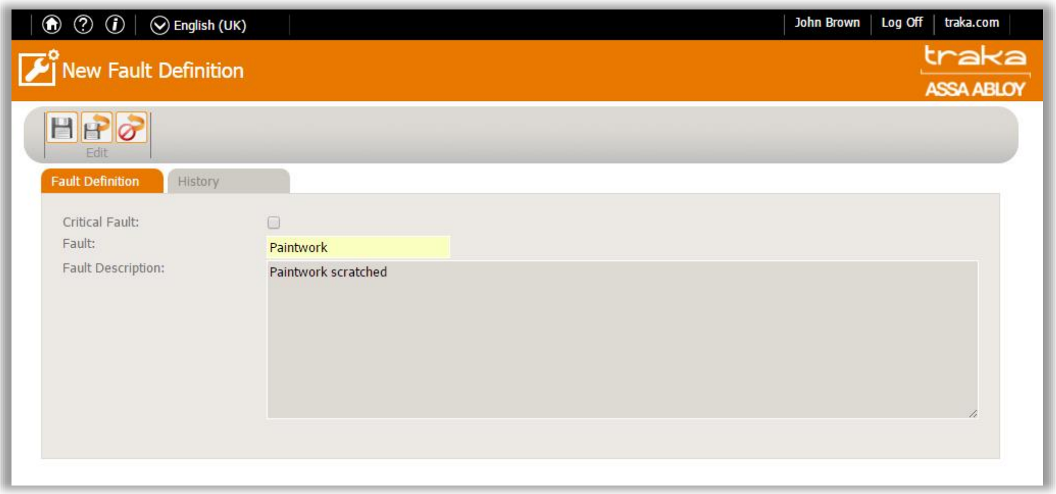
2. Click the 'Add' button and the Fault Definition Details window will appear. From here, you can define a name and any additional descriptions for the fault.



You can also select whether or not the fault is a 'Critical Fault'. A Critical Fault, once logged against an item, restricts that item from being removed from the system unless the user has specific permissions. See the section Define Users That Can Take Critically Faulted Items for further details.

The following two images show examples for the creation of Critical and non-critical Fault Definitions.

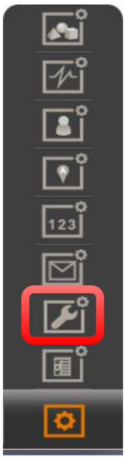




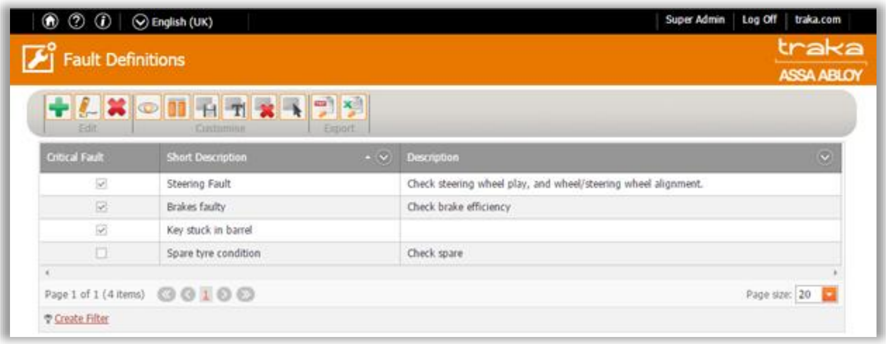
3. Once you have finished creating the Fault Definition click ‘Save’. You can repeat this process for all Fault Definitions you wish to create.

To enable the Fault Definitions to be selectable when logging a fault against an item, they must be assigned to an item type. Refer to the section Selecting Fault Definitions for Item Types for more details.

All the Fault Definitions created will be stored in the Fault Definitions List. To access the Fault Definition List, select ‘Software Settings>Fault Definitions’ from the Navigation Toolbar.



From here, you can Edit, Delete, or Add new Fault Definitions.



NOTE: If a user has removed an item from the system that has a 'normal' fault, and that fault definition is then changed to 'Critical' in TrakaWEB, the Event Report will look like the user removed a critically faulted item without the correct permissions (if that user does not have permission to remove critically faulted items). It is best to edit the 'Critical' status of a Fault Definition when no items currently have that fault logged against them. To check all current outstanding faults, refer to the Outstanding Faults List.

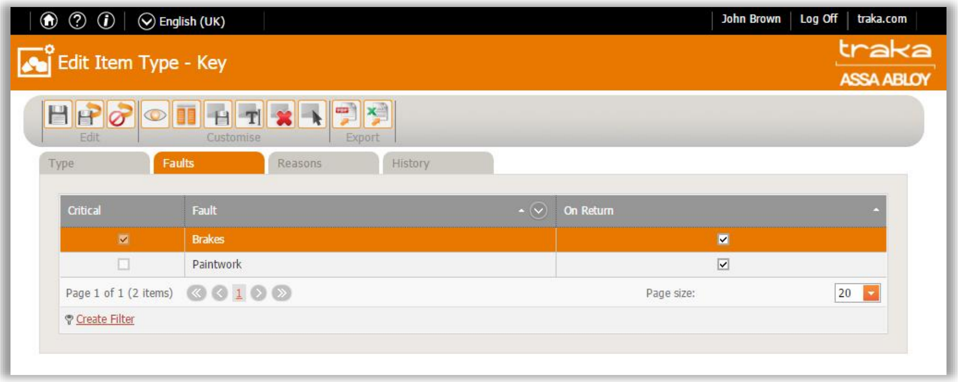
6.2.4 SELECTING FAULT DEFINITIONS FOR ITEM TYPES

In order for a Fault type to be selectable when returning an item to the system, it must first be assigned to an Item Type. Up to 20 Fault Definitions can be assigned to a single Item Type.

1. Select 'Software Settings' and then 'Item Types' from the Navigation Toolbar.

2. Select the desired Item Type and click 'Edit' from the Ribbon Toolbar.

3. Select the Faults tab. A list of all created Fault Definitions will be displayed here. Select the Faults that are applicable to this type of item by ticking the corresponding box in the 'On Return' column.



4. The Preselected Fault column can be added in from the custom columns. This option allows you to select a Fault Definition that will automatically be selected upon the return of an item of that type. Only one preselected fault can be selected for each item type.

NOTE: See Show/Hide Grid Columns for details on how to show custom columns.

6.2.5 DEFINE USERS THAT CAN TAKE CRITICALLY FAULTED ITEMS

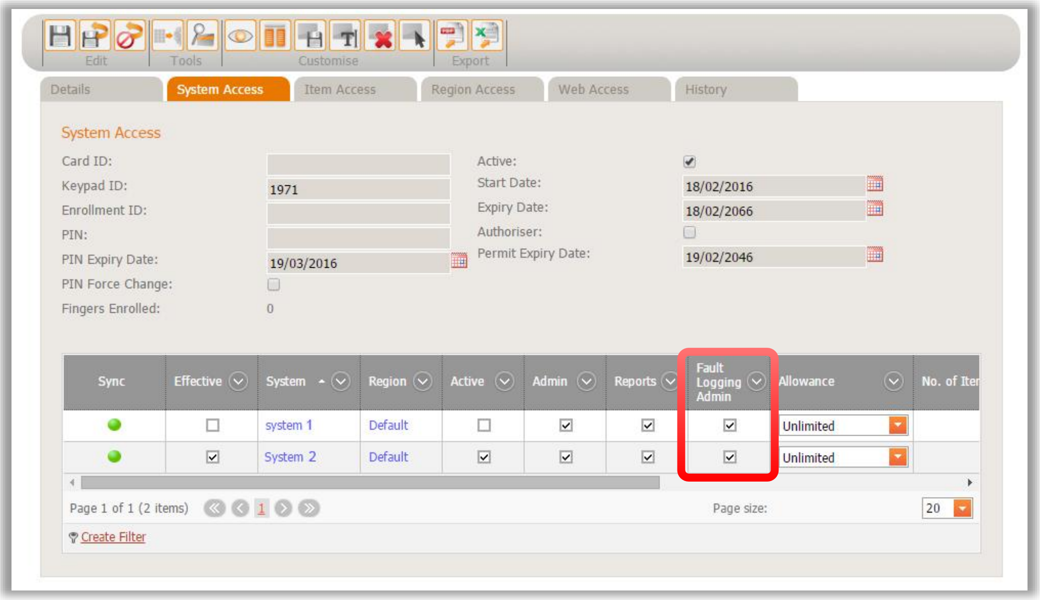
In order for a user to be able to take an item that has had a critical fault logged against it, the user must first be given Fault Logging Admin permissions.

1. Select 'Users' from the Navigation Toolbar.

2. Highlight the user you wish to give Fault Logging Admin permissions to and select 'Edit'.

3. Select the System Access tab. In the system list grid at the bottom of the page will be a Fault Logging Admin column. Tick the box in this column against the corresponding system(s) for which you wish the user to have Fault Logging Admin permissions.

NOTE: The user must also have been granted access to the item in order to take out a critically faulted item (this includes RFID tags in lockers).



NOTE: If a user, who has the Fault Logging Override permissions, needs to access a faulty item and repair it and the system they are accessing is either a FIFO or Advanced FIFO system, that user also needs to have FIFO Override permissions in order to get to the required item. For more information, refer to UD0232 FIFO and Advanced FIFO User Guide.

6.2.6 RETURNING AN ITEM WITH A FAULT

NOTE: This section only applies if your system is configured to allow faults to be logged and cleared at the Traka Touch system.

When returning an item with a fault to a Locker System, the user will be required to enter any fault details before being granted access to the locker compartment.

NOTE: The fault will not be logged if the item is not returned to the locker compartment when the door is closed, even after the user has entered any fault details. The fault details will not be saved if the item is not actually returned.

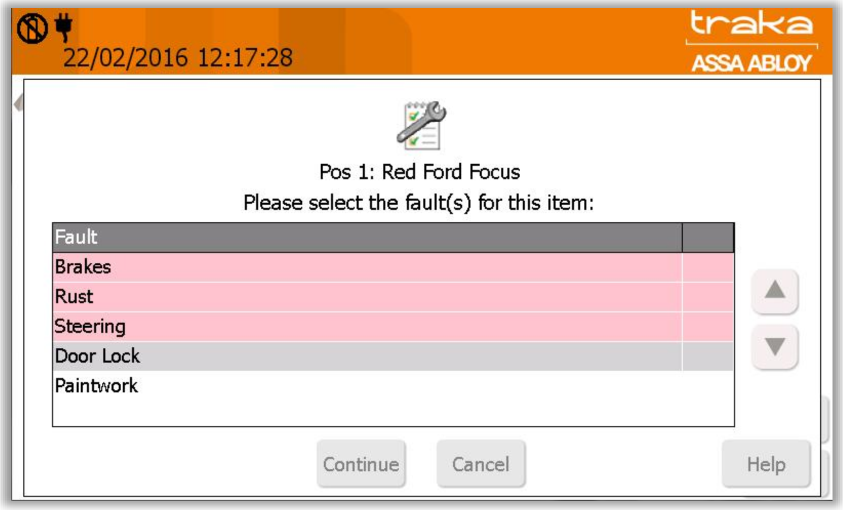
NOTE: Should a situation arise where the tag cannot be read, or the item is damaged to the extent that it will not physically fit in the locker, the fault must be logged at TrakaWEB against an empty locker compartment. Refer to section 4.1.13 'Creating Faults Using TrakaWEB' for more information.

When returning an item that has Fault Logging enabled, if the item does not have any existing faults, you will be presented with the following screen:

Pressing 'No' will skip the fault selection screen and return to the item selection screen.

If the Auto Timeout expires on this screen, the cabinet door is closed (on key cabinets) or the user otherwise logs out, this will skip the fault selection screen and return to the item selection screen.

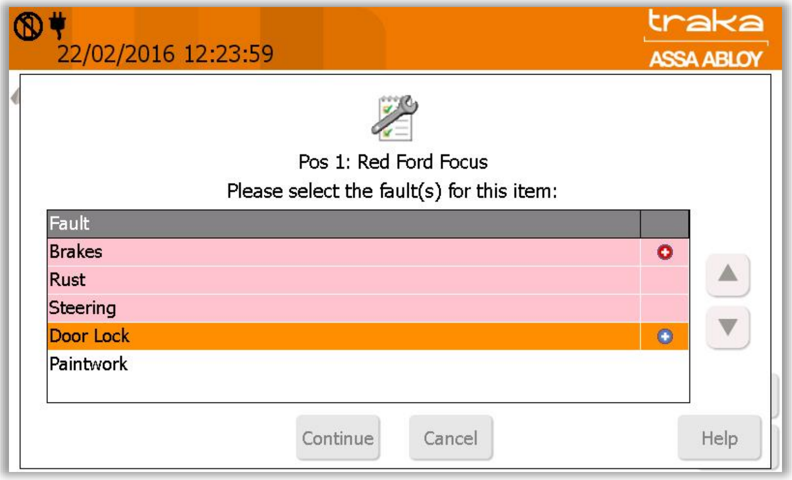
If you choose 'Yes' to select faults, you are presented with the following screen:



A list of the predefined Fault Definitions for the item type being returned is displayed here. Clicking the rows toggles them between unselected and selected. The icon on the right will indicate with a plus sign which faults have been chosen. Up to 20 faults may be shown in the list against an item.

If a preselected fault has been nominated and the item does not have any existing faults, then this preselected fault will be automatically selected and displayed at the top of the list.

Critical faults will be shown with a light red background colour and red icon; non-critical faults will be displayed on a white and grey background with a blue icon as shown below.



Once any faults have been chosen, clicking ‘Continue’ will accept the new fault(s) and the system will generate a ‘Fault Entered’ event and create an Outstanding Fault record for each one chosen.

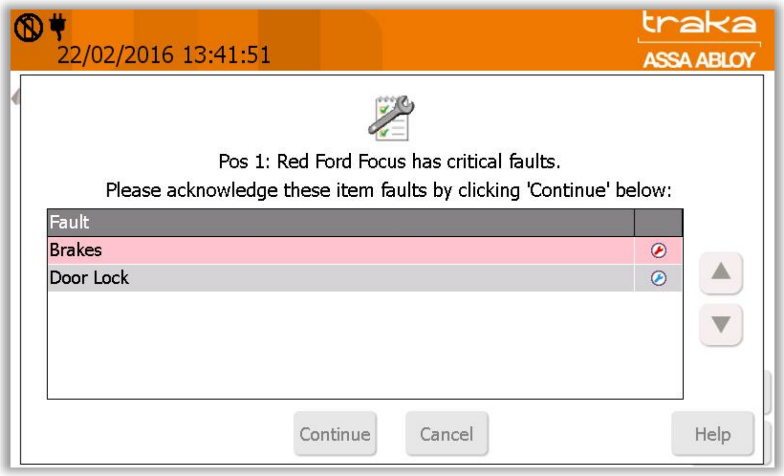
If the Auto Timeout expires on this screen or the cabinet door is closed (on key cabinets) or the user otherwise logs out, a Fault Not Entered event will be generated.

6.2.7 REMOVING A FAULTY ITEM

Any user can remove items with non-critical faults providing they have been granted access to that item in the usual way.

Items with one or more critical faults can only be taken by users who have Fault Logging Admin permissions selected in their user record.

In either case, if an item with faults is requested (or just taken from a non-locking system), the user will have to acknowledge any faults as follows:



Clicking ‘Continue’ will generate a ‘Fault Acknowledged’ event for each fault in the list.

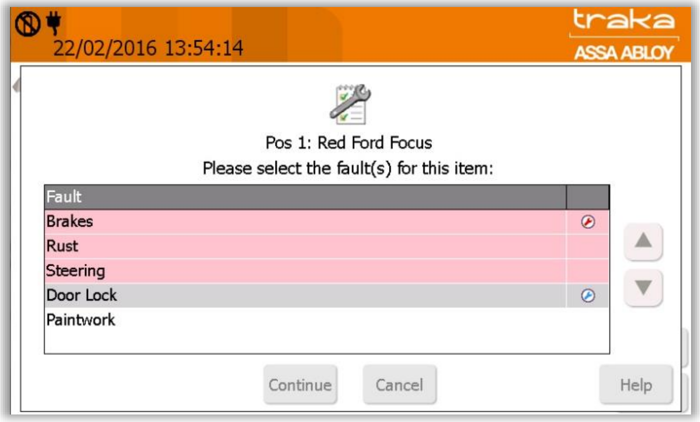
On a non-locking Key Control system or a Locker system where the door is already open, if the user removes the item and the user clicks the 'Cancel' button, the system will generate a 'Fault Not Acknowledged' event for each fault in the list.

On a locking Key Control system or if the door is not open on a Locker system, clicking 'Cancel' or timing out will result in the item not being released or the door not being opened on a locker system.

6.2.8 CLEARING AND ADDING ADDITIONAL FAULTS AT TRAKA TOUCH

NOTE: This section only applies if your system is configured to allow faults to be logged and cleared at the Traka Touch system. Refer to the section Enabling Fault Logging for more details.

If a faulty item is taken out of the system by an authorised person and then returned (perhaps after some repairs have been carried out), the system will show the fault list with any outstanding faults indicated at the top. The 'Does the item have any faults' question will not be asked in this case.



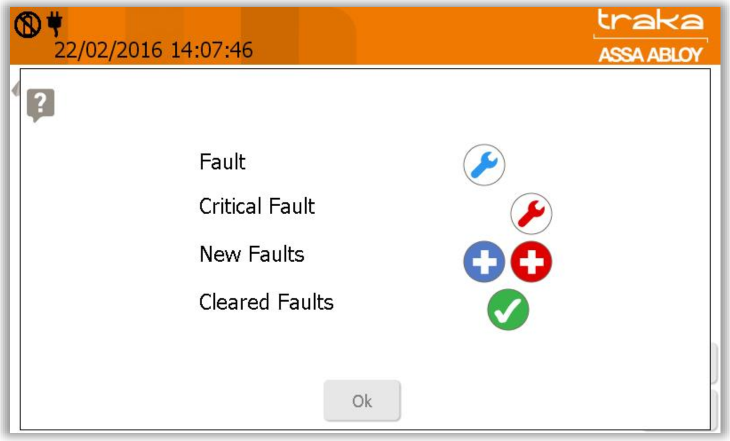
You then have three options as follows:

1. **Clearing**: Existing faults can then be cleared by just clicking them in the list. For each fault deselected, the fault list icon will include a green tick to indicate its cleared status. When the 'Continue' button is pressed you will be asked to enter optional notes for each of the cleared faults in turn. See below for details.

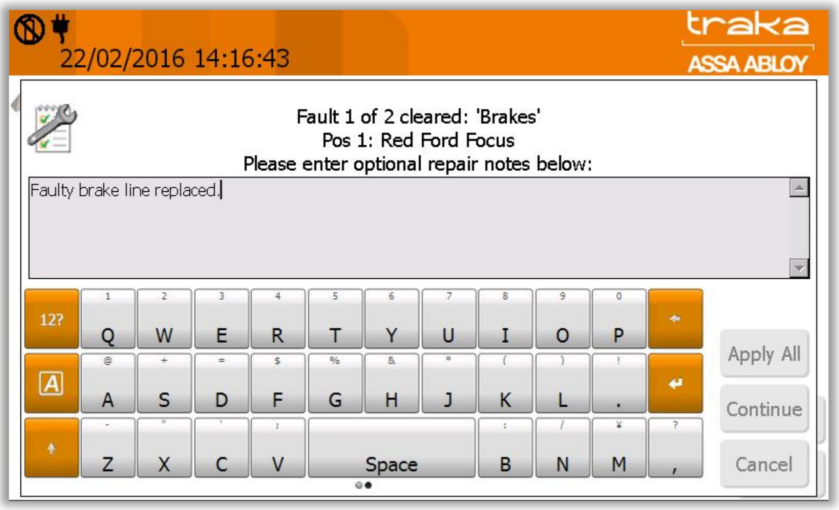
2. **Adding**: If, for example, more faults are found when physically repairing a reported fault, more faults can be added by selecting additional rows. For each fault added, the system will generate additional 'Fault Entered' events and create new Outstanding Fault records.

3. **No change**: Accept that the existing faults have not changed by doing nothing else except pressing the 'Continue' button.

Clicking the 'Help' button will present you with the following screen:



For option 1, the below screen is presented for each cleared fault allowing you to enter optional repair notes. Any existing fault notes that may have been entered from TrakaWEB will also be displayed here.



Clicking 'Apply All' will assign the same entered notes to all of the cleared faults.

Clicking 'Continue' will save the entered notes and either move on to the next cleared fault, or continue to the next feature questions (if applicable).

If 'Cancel' is pressed, the notes being edited will not be saved, the displayed fault and any remaining faults selected to be cleared will not be cleared and will remain on the item. If 'Cancel' has been pressed by mistake, remove and return the item(s) to repeat the process.

Once finished, a 'Fault Cleared' event will be generated for each one, and the entered notes will be updated in the appropriate fault records in TrakaWEB.

6.2.9 ITEM SELECTION SCREEN WITH FAULTS

This is an example of how the Item Selection Screen might look on a system with Fault Logging enabled:

Position 1:  - Item in with one or more critical faults

Position 2:  - Item in with one or more non-critical faults

Position 3:  - Item held with one or more critical faults

Position 4:  - Item held with no faults

Position 5:  - Item in with no faults

6.2.10 SYSTEM VIEWER FAULT DISPLAY

This is an example of the system viewer within TrakaWEB showing the different fault statuses. When you select a position that has faults entered against it, the item status panel will show up to five fault names. Clicking any fault hyperlink will take you to the corresponding fault record page.

The Icons and their meanings are shown below:

 - White spanner on blue background: Item is in and has one or more faults. No critical faults are present.

 - White spanner on red background: Item is in, and has one or more faults and at least one is a critical fault.

 - White spanner on purple background: Item is in, and has all faults marked as 'repaired' but not 'cleared'.

 - White spanner on grey background: Item is out and has one or more faults. No critical faults are present.

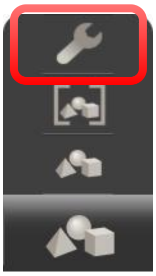
 - White spanner on grey background: Item is out, and has one or more faults and at least one is a critical fault.

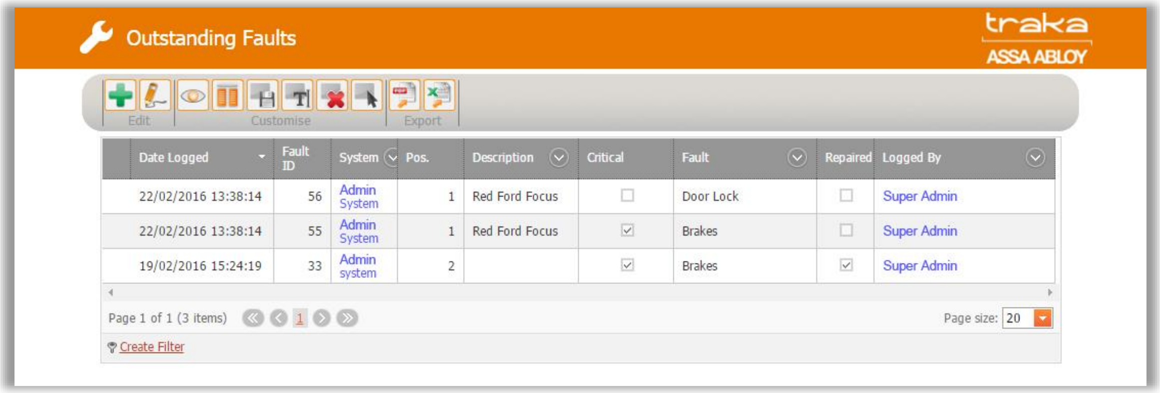
 - White spanner on grey background: Item is out, and has all faults marked as 'repaired' but not 'cleared'.

NOTE: 'Out' fault statuses are only shown on Fixed Return systems.

6.2.11 OUTSTANDING FAULTS LIST

The Outstanding Faults List can be found by selecting 'Items>Outstanding Faults' from the Navigation Toolbar.





The example above shows the default columns that are presented in the Outstanding Faults List. These include details such as who logged the fault and when, the system and position number, the fault name and whether or not it is a critical fault, and if the fault has been repaired.

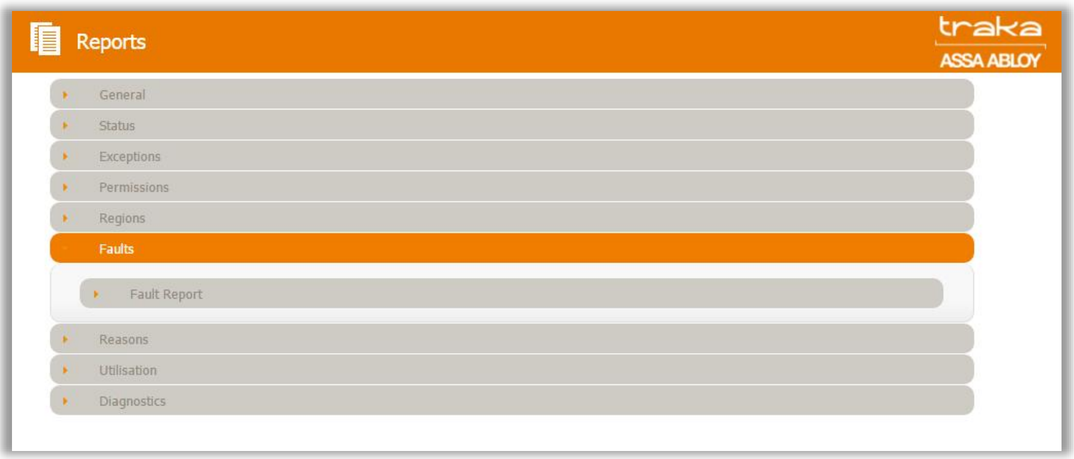
Optional columns can be added using the Show/Hide Grid Columns feature. These include:

- Fault Definition Long Description
- Item Detail 1-11
- User Detail 1-11
- Repaired By
- Repaired Date

NOTE: There is no option to delete a fault. Faults will no longer show when they are cleared.

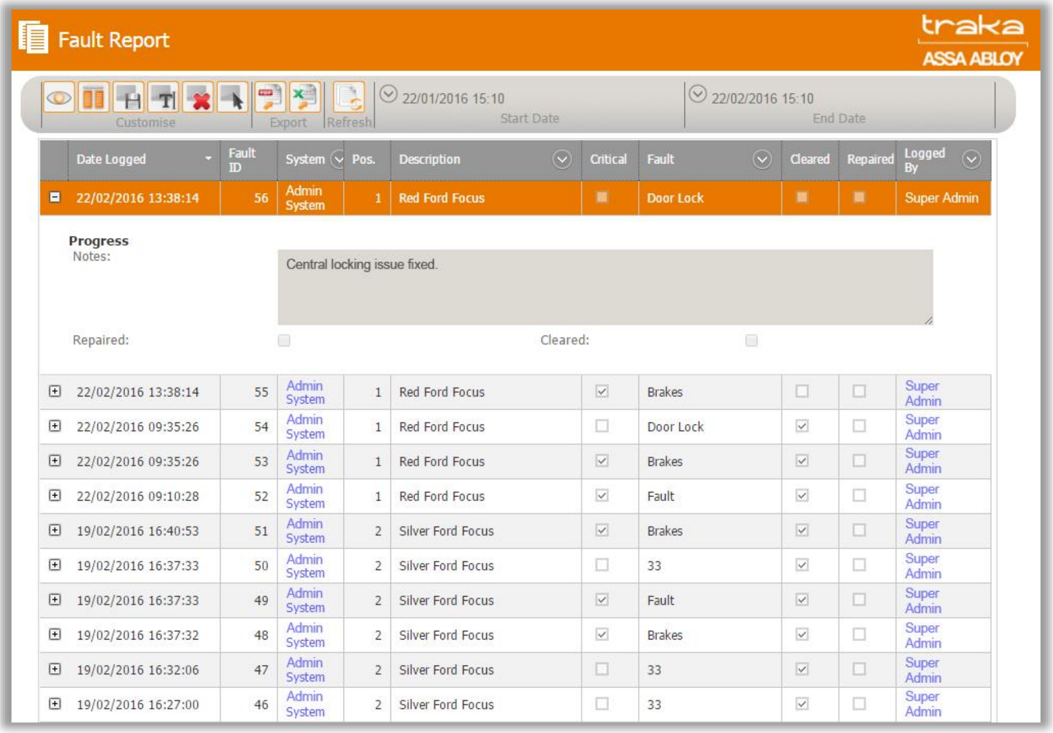
6.2.12 FAULT REPORT

To access the Fault Report, select 'Reports' from the Navigation Toolbar and then select 'Fault Report'.



The Fault Report shows 'cleared' faults as well as outstanding faults. Various default columns are displayed containing information about each fault, including any repair notes that may have been entered when the fault was cleared. Optional columns can also be added. These include:

- Fault Definition Long Description
- Item Detail 1-11
- User Detail 1-11
- Repaired By
- Repaired Date



6.2.13 CREATING FAULTS USING TRAKAWEB

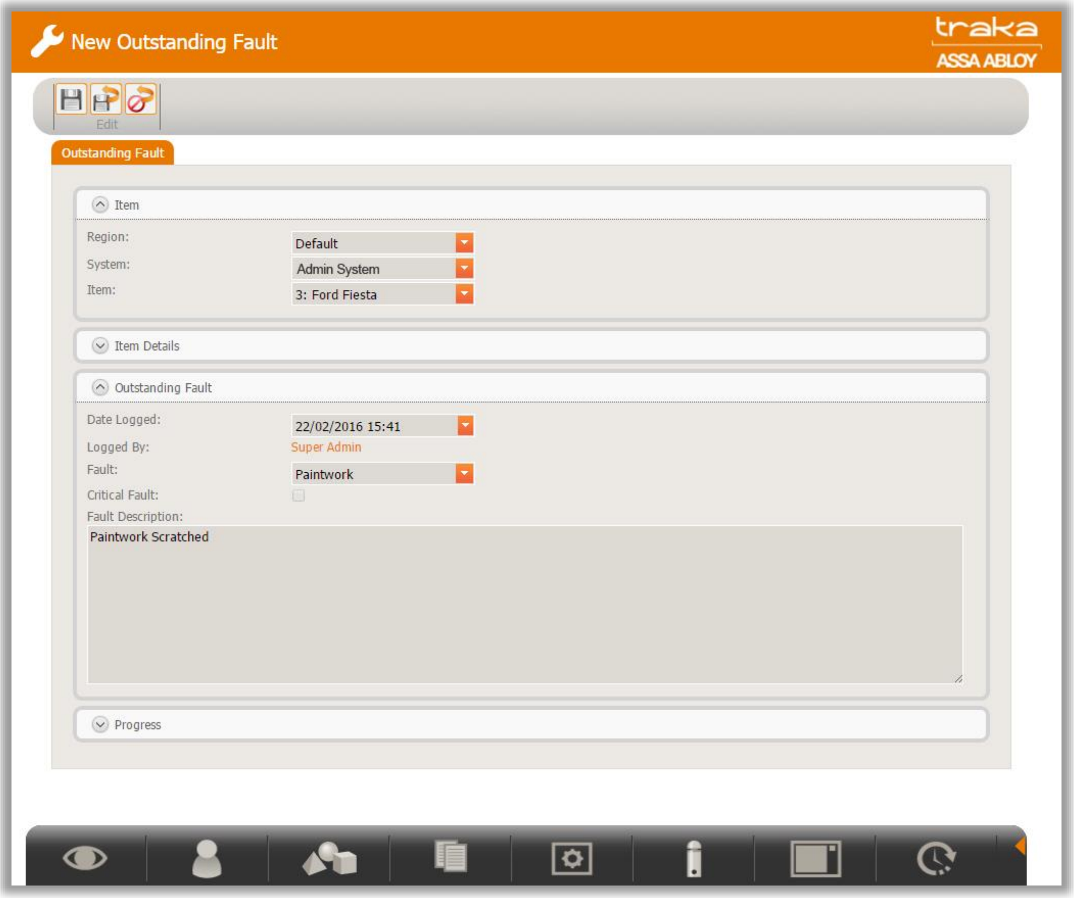
NOTE: TrakaWEB users must have the correct permissions in order to create faults using TrakaWEB. Refer to the section Fault Logging Software Permissions for further details.

NOTE: When returning an item to a locker, the fault must be registered at Traka Touch before the door will open, allowing access to the compartment. If the item is not returned to the compartment, Traka Touch will not record the fault. So in the situation where the RFID tag cannot be read, or the item is damaged to the extent that it will not fit in the compartment, the fault must be registered at TrakaWEB.

1. To create a Fault within TrakaWEB, select 'Items>Outstanding Faults' from the Navigation Toolbar.

2. Click the 'Add' button in the Ribbon Toolbar.

3. Using the dropdown boxes in the Item window, select the Region, System and Item you wish the fault to apply to. Once the item has been selected, a list of possible faults will be available to choose from in the Outstanding Fault window. Select the fault you wish to add from the list.



4. Enter any fault/repair notes in the Notes field under the 'Progress' section.

5. Once complete, click 'Save' from the Ribbon Toolbar.

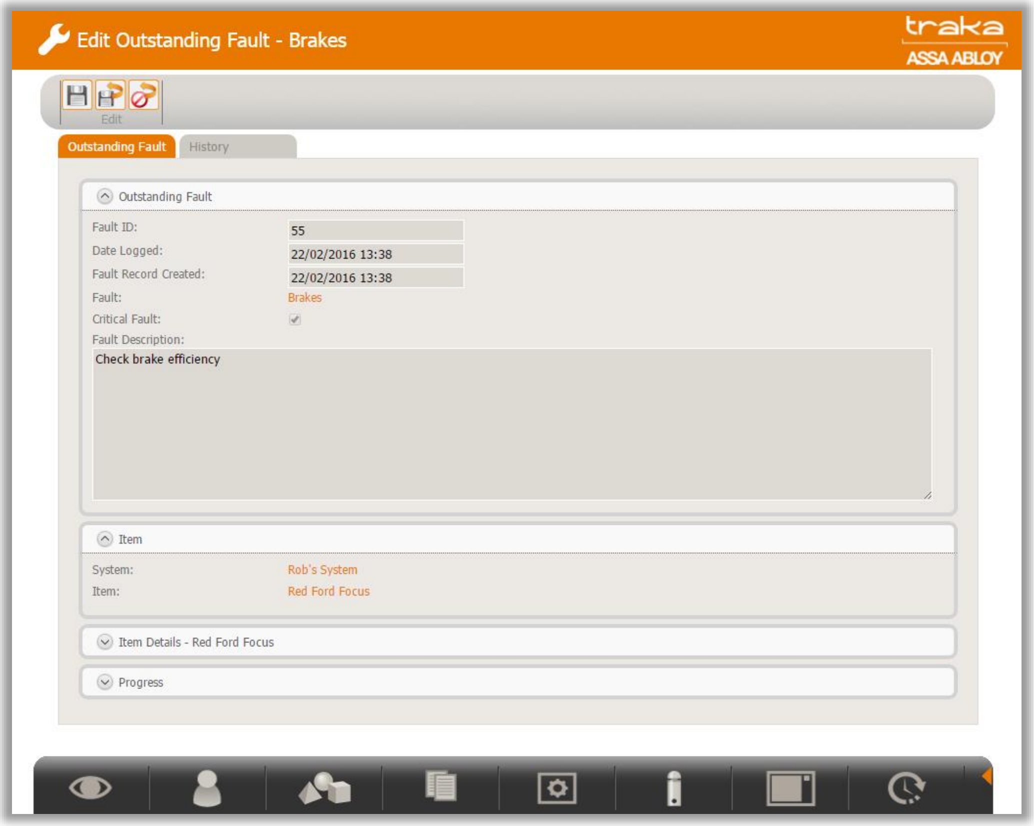
6.2.14 EDITING AND CLEARING AN OUTSTANDING FAULT

Outstanding faults may be edited and optionally marked as repaired and/or cleared in TrakaWEB.

Once cleared, the fault will no longer appear in the Outstanding Faults List, but can be seen in the Fault Report.

1. To edit an outstanding fault, select 'Items>Outstanding Faults' from the Navigation Toolbar.

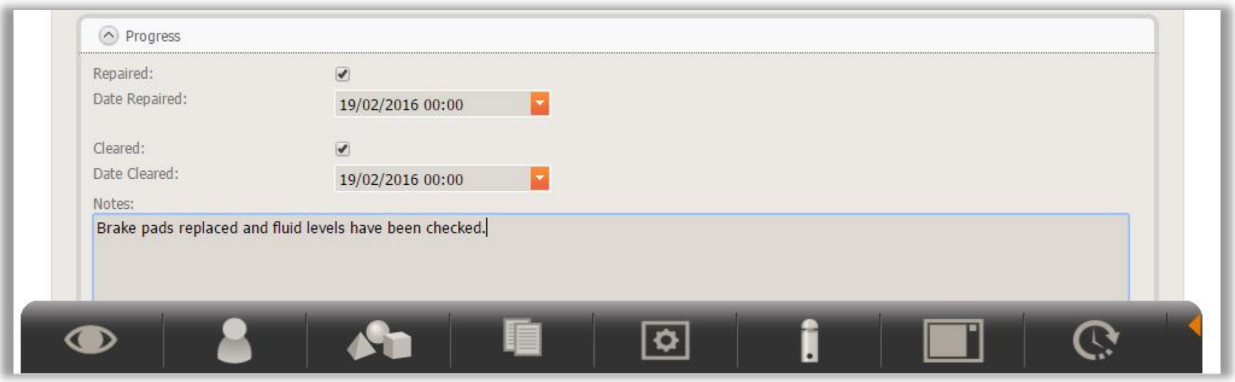
2. Highlight the desired fault and click 'Edit' from the Ribbon Toolbar. A window will appear displaying various details for the selected Fault.



3. Expanding the Progress sections will reveal options to update the status of the fault as 'Repaired' or 'Cleared' and also enter a date and time using the drop down calendar. You can also enter notes for the progress of the Fault.

If you select 'Repaired', the Fault will remain in the Outstanding Faults List but the icon in the System Viewer will change to highlight the fault has been repaired.

If you select 'Cleared', the fault will be removed from the Outstanding Faults List and the icon in the System Viewer will show no faults. The fault record will still be visible in the Fault Report.



Users must have the correct software permissions to be able to select the Fault Cleared or Fault Repaired tick boxes. Without these permissions, the tick boxes will be read only. Please refer to the section Fault Logging Software Permissions for further details.

NOTE: The Fault Repair functionality using the 'Repair' tick box is currently only available using TrakaWEB. The 'Repaired' status cannot be viewed or modified on the Traka Touch.

6.2.15 FAULT LOGGING EMAIL NOTIFICATIONS

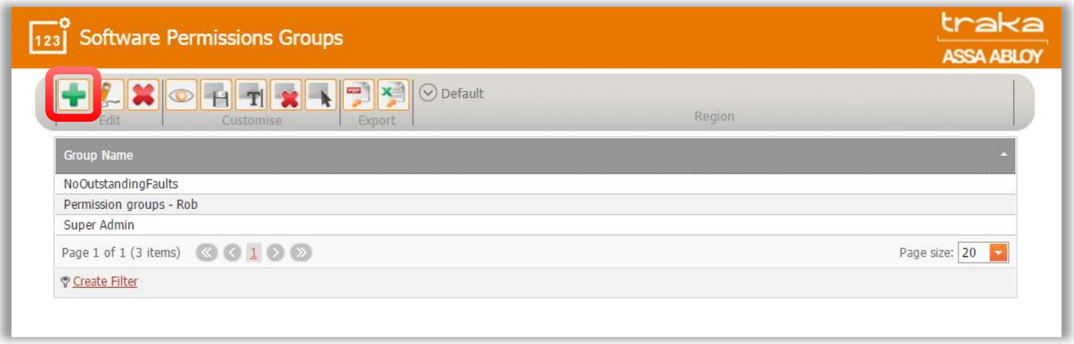
In addition to creating and viewing faults in TrakaWEB, it is also possible to create a notification using the email Notification Feature Option. For more information on email notifications, refer to section 5.6.

6.2.16 FAULT LOGGING SOFTWARE PERMISSIONS

To enable a user to create, edit and delete Fault Definitions, or to create/edit and repair/clear faults, they must be given the correct software permissions.

1. Select 'Software Settings>Software Permissions Groups' from the Navigation Toolbar.

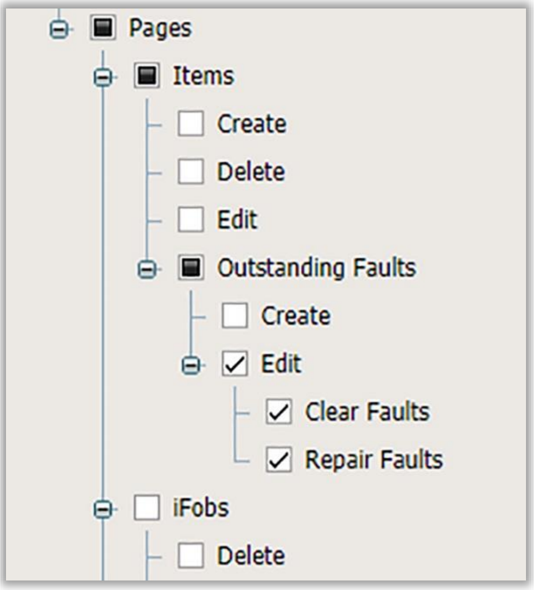
2. Either edit an existing group you wish to give permissions to by selecting the group and clicking 'Edit', or alternatively create a new group by clicking the 'Add' button.



NOTE: An option for allocating Fault Logging software permissions might be to create 2 groups; one called 'Fault Admin' for users who can create/edit/delete Fault Definitions, and another called 'Fault Repairer' for users who can create/edit and repair/clear faults.

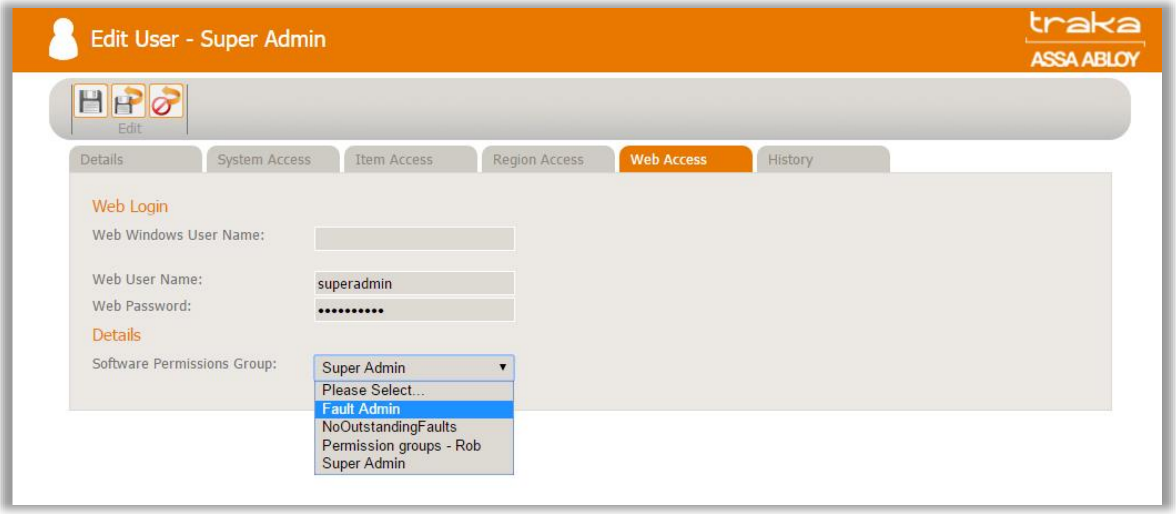
3. The permissions for the ability to create/edit/delete Fault Definitions can be found by expanding Web/Pages/Software Settings/Fault Definitions.

4. The permissions for the ability to create/edit, and repair/clear faults can be found by expanding Web/Pages/Items/Outstanding Faults.



5. To assign users to the Software Permissions Groups select 'Users' from the Navigation Toolbar.

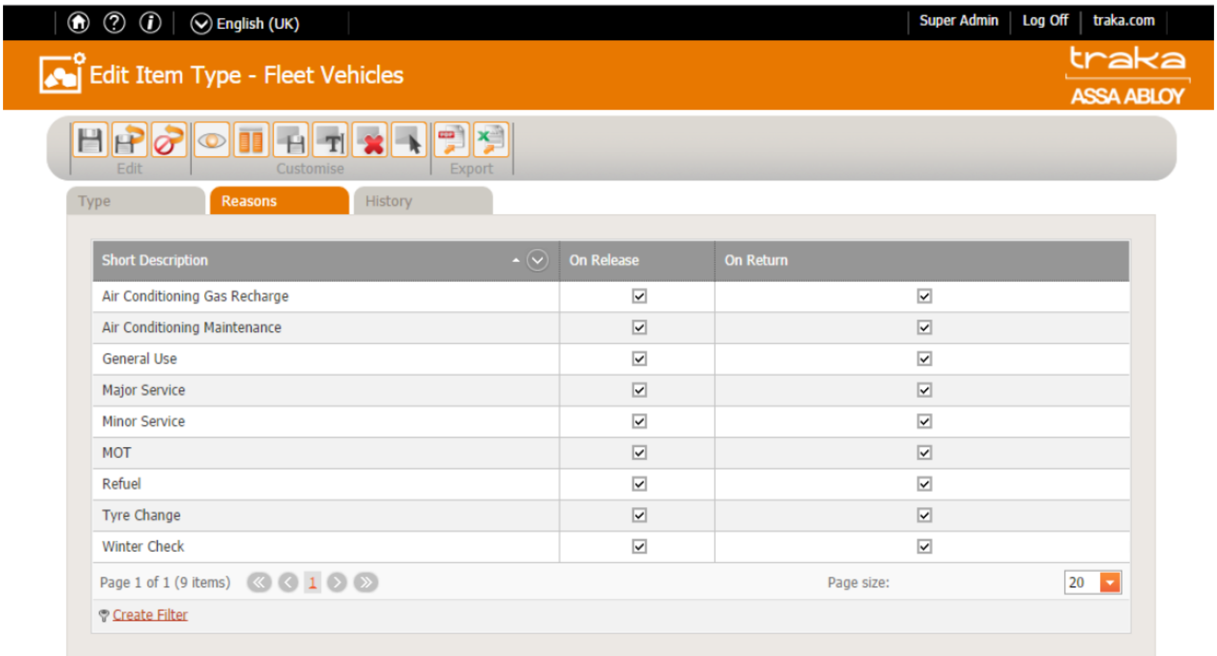
6. Select the desired user and click 'Edit'. Select the Web Access tab and select the required group from the Software Permissions Group dropdown box. Click 'Save' from the Ribbon Toolbar.



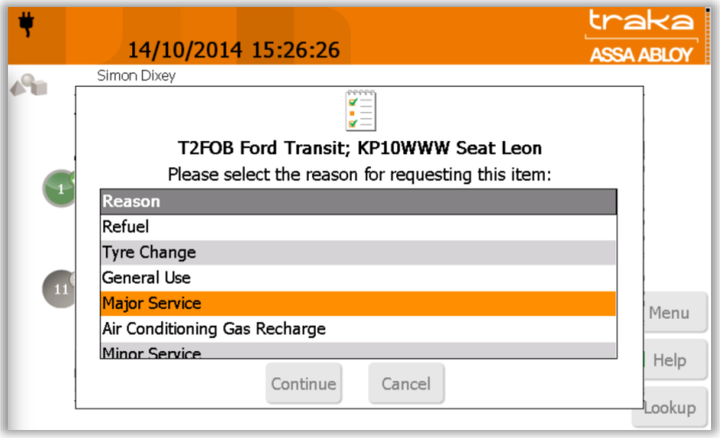
6.3 REASON LOGGING

Reason logging is a cost option that allows a user to log a 'reason' against the removal or return of an item. Reasons are created within TrakaWEB, and are then selectable from a list at the Traka Touch system when either removing or returning an item.

The example below shows how a Reason List in TrakaWEB might look for a Traka System containing keys for a fleet of vehicles.



Once set up, the user will be prompted to select a Reason for removing and/or returning the item depending on how the Reason options have been configured.



The reason selected by the user is shown in the activity grid and can also be viewed in the Reason Reports.

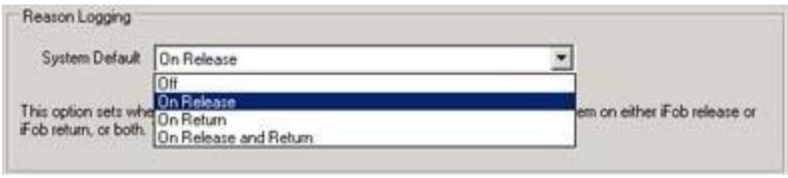
Please read the following section for more detailed information and the process for setting up and configuring the Reason Logging options to best suit your requirements.

6.3.1 ENABLING THE OPTION

Reason Logging will need to be enabled in the system configuration and the Admin Application before it is usable in TrakaWEB. To have it enabled within the configuration, you will need to contact Traka or your Distributor for further details.

1. Enabling the option at its base level within the Admin Application will apply to all positions within the system. An administrator who has the appropriate access to the Admin Application will need to select the desired system and navigate to the Feature Options tab.

2. The Reason Logging section has a drop down box that consists of the following four options.



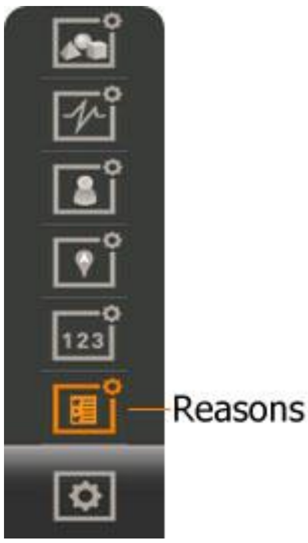
- **Off** - will deactivate the option completely
- **On Release** - will activate the option when removing an item
- **On Return** - will activate the option when returning an item
- **On Return and Release** - will activate the option when returning and removing an item

3. Select the desired option and click the Save button at the bottom of the application. This will update the Traka Touch system as well as TrakaWEB.

It is possible to change the effect of the option on a per iFob/item basis. Please see the appropriate section below for further instructions.

6.3.2 CREATING REASONS

To create a Reason, select the Software Settings button from the Navigation Toolbar and click the Reasons button as shown below.



The current reasons list will then be displayed. If this is your first time using reason logging, then the grid will be empty and have no information populating it.

1. Click the Add button.

2. A new form will appear allowing you to enter both a short and long description. The short description has a maximum of 50 characters and acts as a summary on the Traka Touch screen when removing/returning the item and in TrakaWEB system viewer. The long description has a maximum character length of 500 and allows for a more detailed description, which is used for reports.

3. Once you have finished, click the Save & Return button.

4. The list will now have the new Reason you just added.

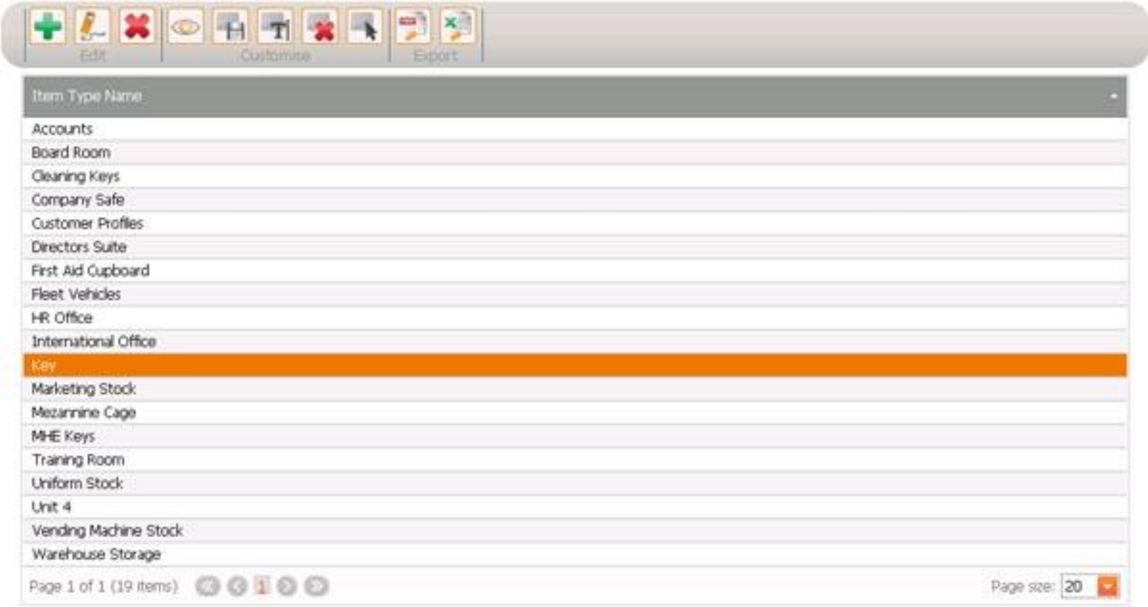
6.3.3 ADDING THE REASON TO YOUR ITEM TYPE

Before you can begin to use this option, you must ensure that each position you wish to use with Reason Logging has an item defined. To assign an item to a position, please refer to the Adding an Item to an iFob topic.

Once an item has been defined, you will need to assign a Reason to the Item Type.

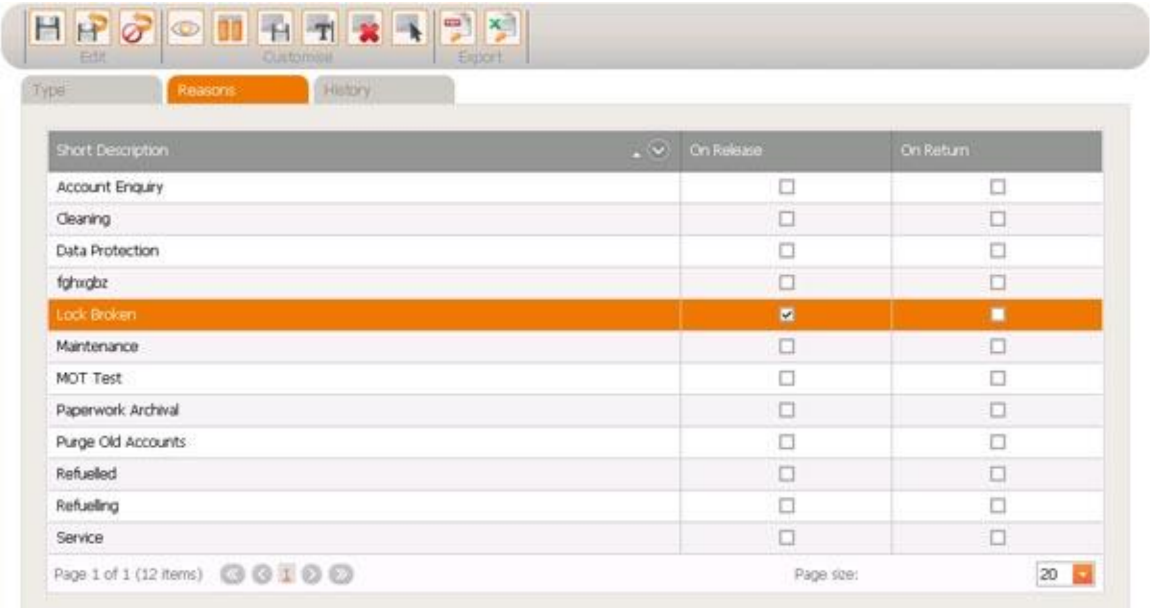
1. From the Navigation Toolbar select software settings, then click item types.

2. TrakaWEB will then display all the current item types that exist within the database. Highlight the desired item type.



3. Select the Edit button.

4. The item details form will open allowing you to change its information. Select the Reasons tab.



The reasons that you have created will be listed here. There are two columns - ‘On Release’ and ‘On Return’. Ticking the appropriate boxes will determine which Reasons are available to be selected on either the removal or return of the selected item type. The reasons that you have created will be listed here.

6.3.4 CHANGING THE OPTION ON A PER IFOB BASIS

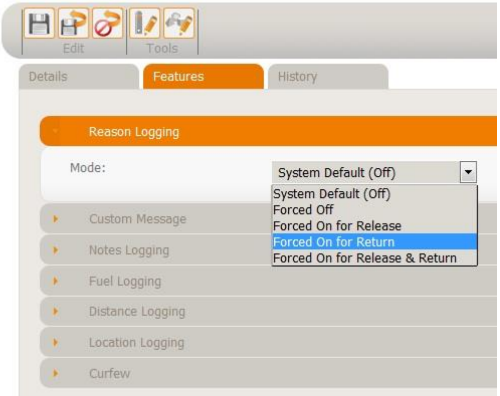
NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' in a Locker System.

To alter the option on a per iFob basis is simple and easy to do.

1. From the system viewer, highlight the desired iFob and click the Edit iFob button from the Ribbon Toolbar.
2. Select the Features tab.
3. From the Reason Logging drop down box, make the appropriate selection, e.g. Forced On for Release, Forced On for Return etc.

NOTE: This will override the settings that have been applied in the Admin Application and will only apply to this iFob.

NOTE: Selecting the system default will revert to the settings applied in the Admin Application. The settings are displayed in brackets.



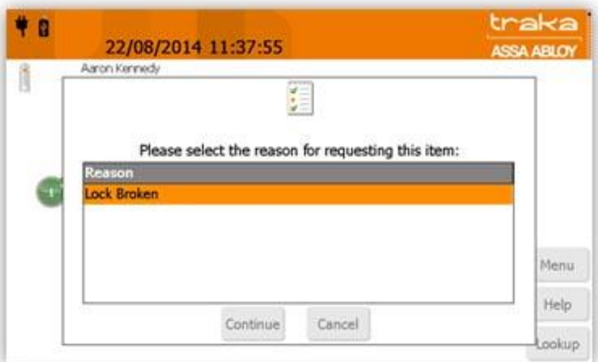
4. Once you have selected the desired option click the Save and Return button.

6.3.5 TRAKA TOUCH

Users with access to the required item will need to identify themselves to the system and navigate to the item selection screen.

1. Select the item they wish to remove.
2. A dialogue box will appear requesting that you select a reason for requesting the item. Select the reason and click Continue.

NOTE: Clicking cancel will take the user back to the item selection screen.



3. The item will now release from the system.

6.3.6 ACTIVITIES

The system viewer displays a grid that holds the last 30 days of activities for the selected iFob/item in the system. When a user selects a reason at the Traka Touch system when releasing/returning an item and clicks the Continue button, a 'Return Reason Entered' and/or 'Release Reason Entered' activity will be generated in the Item Activity tab.

Item Activity | iFob Activity | iFob Access | System Activity | Items

Activity	When	Who
Return Reason Entered	29/08/2014 09:40:55	Aaron Kennedy
Item Returned	29/08/2014 09:40:46	Aaron Kennedy
Item Removed	29/08/2014 09:27:09	Aaron Kennedy
Release Reason Entered	29/08/2014 09:27:07	Aaron Kennedy

1 Page size: 20

If a user returns an item and they do not select a reason and close the door, a 'Release Reason Not Entered' activity will be generated.

Item Activity | iFob Activity | iFob Access | System Activity | Items

Activity	When	Who
Return Reason Not Entered	29/08/2014 09:39:59	Aaron Kennedy
Item Returned	29/08/2014 09:39:53	Aaron Kennedy
Item Removed	29/08/2014 09:33:36	Aaron Kennedy
Release Reason Entered	29/08/2014 09:33:34	Aaron Kennedy

1 Page size: 20

You can also see the Release/Return Reason in the detail panel on the system viewer. The reason is selectable, and clicking it will take you to the Edit Reason page where you can edit the long and short description.

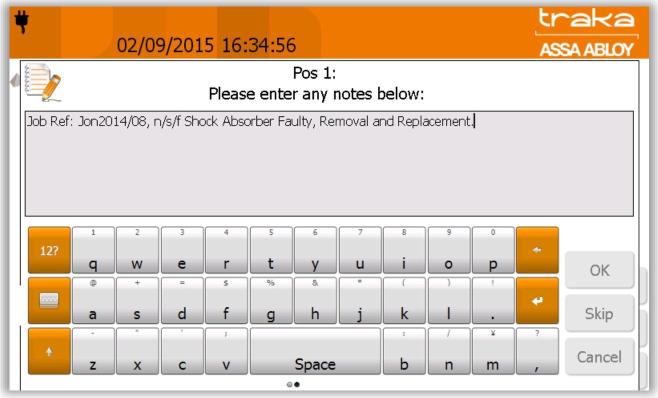
6.3.7 REPORTS

You can run various reports to see which items have been removed/returned with what 'reason' logged against them. Please refer to the Reason Reports section.

6.4 NOTES LOGGING

Notes Logging is a cost option that allows a user to enter a note into an on-screen dialogue box at the Traka Touch system when removing or returning an item. A maximum of 255 characters can be entered at any one time.

With Notes Logging enabled, when a user removes and/or returns an item, a window with a keyboard will pop up allowing them to enter a note. An example is shown below.



The activity grid will display whether or not a note has been entered, and the entered note can be viewed from the Notes Report in TrakaWEB.

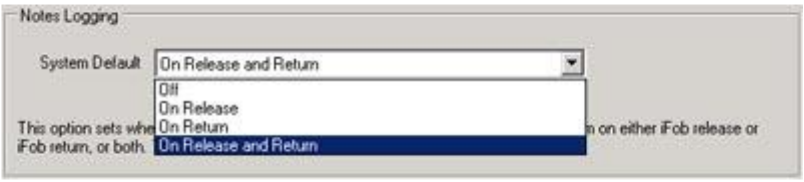
Please read the following section for more detailed information and the process for setting up and configuring Notes Logging.

6.4.1 ENABLING THE OPTION

Notes Logging will need to be enabled in the system configuration and the Admin Application before it is usable in TrakaWEB. To have it enabled within the configuration you will need to contact Traka or your Distributor for further details.

1. To enable the option at its base level within the Admin Application will apply to all positions within the system. An administrator who has the appropriate access to the Admin Application will need to select the desired system and navigate to the Feature Options tab.

2. The Notes Logging section has a drop down box that consists of the following four options:



- **Off** - will deactivate the option completely.
- **On Release** - will activate the option when removing an item.
- **On Return** - will activate the option when returning an item.
- **On Return and Release** - will activate the option when returning and removing an item.

3. Select the desired option and click the Save button at the bottom of the application. This will update the Traka Touch system as well as TrakaWEB.

It is possible to change the effect of the option on a per iFob/item basis. Please see the appropriate section below for further instructions.

6.4.2 CHANGING THE OPTION ON A PER IFOB BASIS

NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' in a Locker System.

To alter the option on a per iFob basis is simple and easy to do.

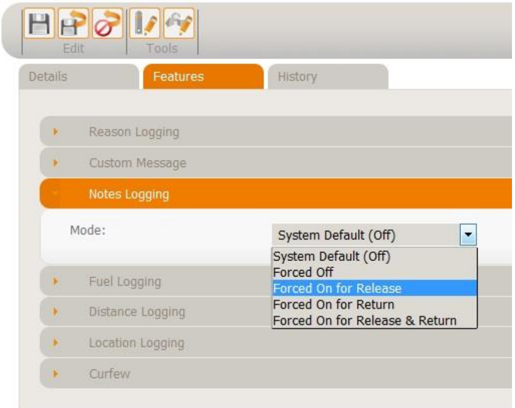
1. From the system viewer, highlight the desired iFob and click the Edit iFob button from the Ribbon Toolbar.

2. Select the Features tab.

3. From the Notes Logging drop down box, make the appropriate selection, e.g. Forced On for Release, Forced On for Return etc.

NOTE: This will override the settings that have been applied in the Admin Application and will only apply to this iFob.

NOTE: Selecting the system default will revert back to the settings applied in the Admin Application. The settings are displayed in brackets.



4. Once you have selected the desired option click the Save and Return button.

6.4.3 TRAKA TOUCH

1. Users with access to the required item will need to identify themselves to the system and navigate to the item selection screen.

2. Select the item they wish to remove.

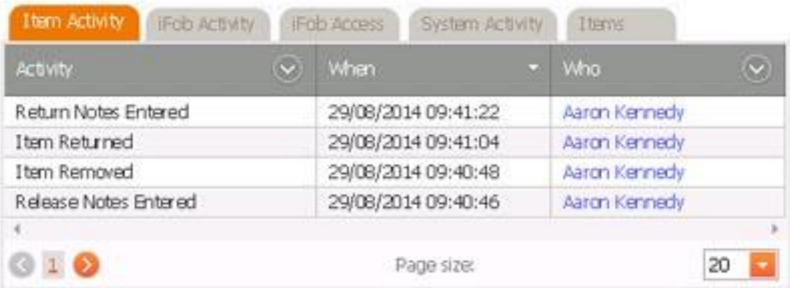
3. A dialogue box will appear allowing the user to enter a note relating to the item.

NOTE: If the user selects Skip button, the item will be released but no notes will be entered against the item.

Click **OK**. The item will now be released from the system.

6.4.4 ACTIVITIES

The system viewer displays a grid that holds the last 30 days of activities for the selected iFob/item in the system. When a user enters a note at the Traka Touch system when releasing/returning an item, and clicks the OK button, a 'Return Notes Entered' and/or 'Release Notes Entered' activity will be generated in the Item Activity tab.



If a user returns an item, they do not enter a note, and they select OK/Skip or close the door, a 'Release Notes Not Entered' activity will be generated.

NOTE: No activity will be generated when a user removes and item and does not enter a note.

You can also see the Release/Return Note in the detail panel on the system viewer.

6.4.5 REPORTS

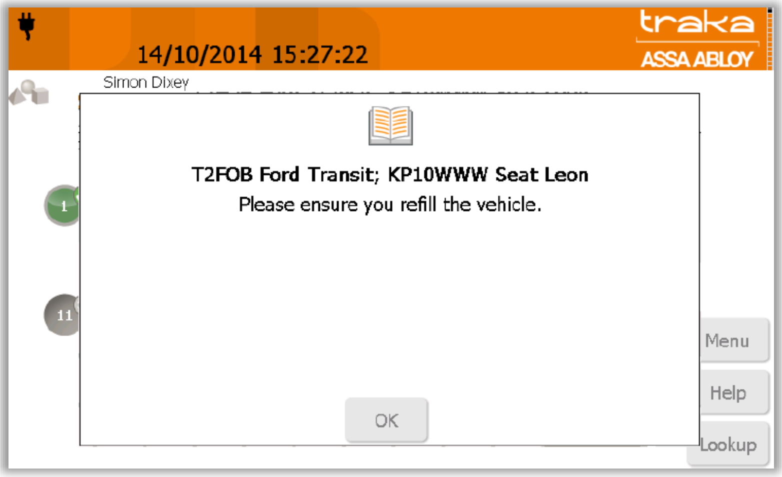
You can run various reports to see which notes were entered against an item and when it was released or returned. Please refer to the Note Reports section.

6.5 CUSTOM MESSAGES

6.5.1 CUSTOM MESSAGES

Custom Messages is a cost option that allows the Traka Touch to display a definable message to the user when they remove or return an item. This message can be defined for each individual position in the system. This ensures that the user is aware of any special condition that must be met in relation to the item.

Once setup, the message will be displayed when a user removes and/or returns an item depending on how the Custom Messages have been configured. An example is shown below.



The user can acknowledge the message by clicking **OK**. The activity grid will display whether or not this message has been acknowledged.

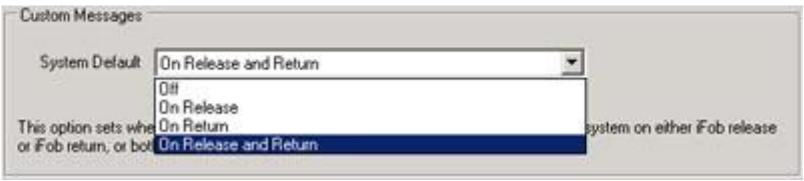
Please read the following section for more detailed information and the process for setting up and configuring Custom Messages.

6.5.2 ENABLING THE OPTION

Custom Messaging will need to be enabled in the system configuration and the Admin Application before it is usable in TrakaWEB. To have it enabled within the configuration you will need to contact Traka or your Distributor for further details.

1. To enable the option at its base level within the Admin Application will apply to all positions within the system. An administrator who has the appropriate access to the Admin Application will need to select the desired system and navigate to the Feature Options tab.

2. The Notes Logging section has a drop down box that consists of the following four options:



- **Off** - will deactivate the option completely
- **On Release** - will activate the option when removing an item
- **On Return** - will activate the option when returning an item
- **On Return and Release** - will activate the option when returning and removing an item

3. Select the desired option and click the Save button at the bottom of the application. This will update the Traka Touch system as well as TrakaWEB.

It is possible to change the effect of the option on a per iFob basis. Please see the appropriate section below for further instructions.

6.5.3 CHANGING THE OPTION ON A PER IFOB BASIS & CREATING A CUSTOM MESSAGE

NOTE: If your system is an RFID Locker System, it will not contain iFobs. However, this section will still be relevant and the term 'iFob' will be referring to the 'RFID Tag' in a Locker System.

1. From the system viewer highlight the desired iFob.

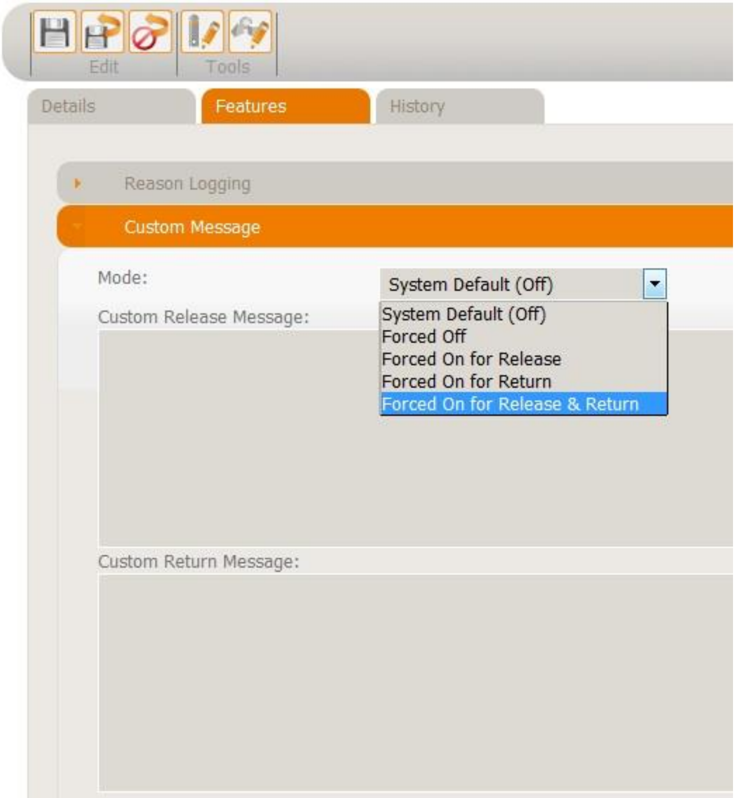
2. Click the Edit iFob button.

3. Navigate to the Features tab.

4. From the Custom Messages drop down box make the appropriate selection, e.g. Forced On for Release, Forced On for Return etc.

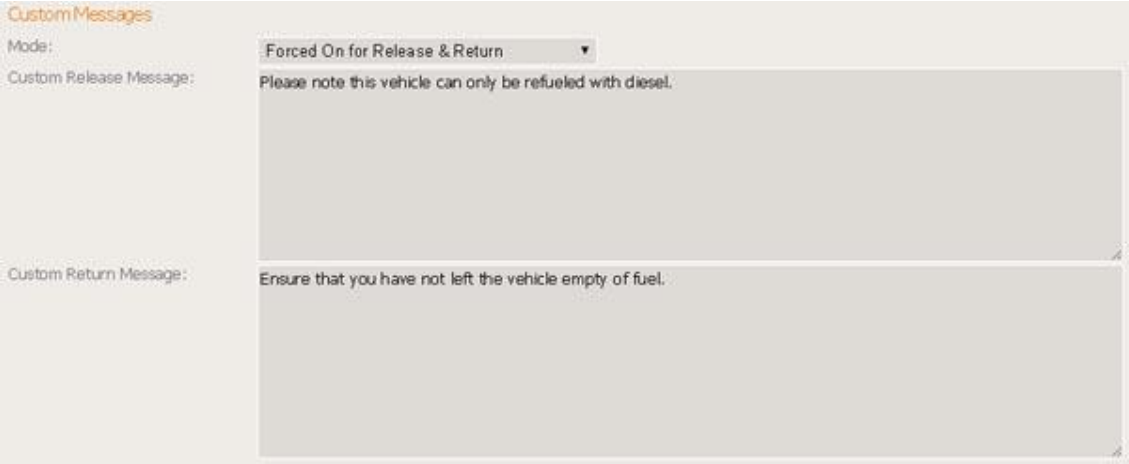
NOTE: This will override the settings that have been applied in the Admin Application and will only apply to this iFob.

NOTE: Selecting the system default will revert back to the settings applied in the Admin Application. The settings are displayed in brackets.



5. In the example below, 'Forced On for Release & Return' has been selected. This will display a message to the user when they remove and return the item. You will now be able to enter the desired message into both fields.

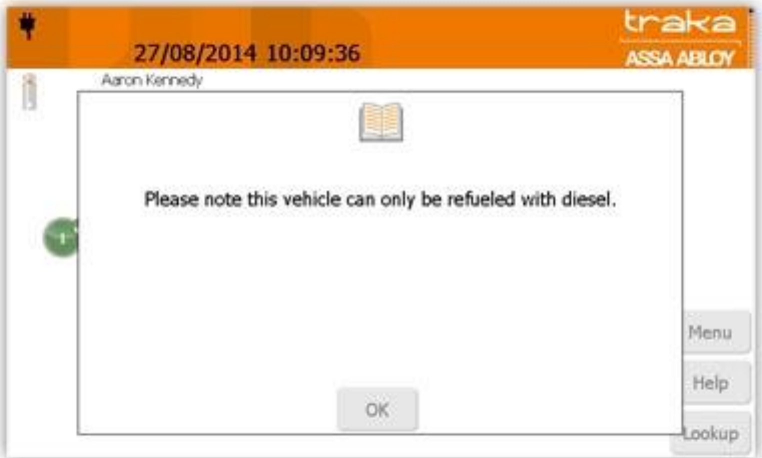
NOTE: The message fields have a maximum character length of 200.



6. Once you have finished, click the Save or Save and Return button.

6.5.4 TRAKA TOUCH

1. Users with access to the required item will need to identify themselves to the system and navigate to the item selection screen.
2. Select the item they wish to remove.
3. A dialogue box will appear displaying the message that was previously entered in TrakaWEB.

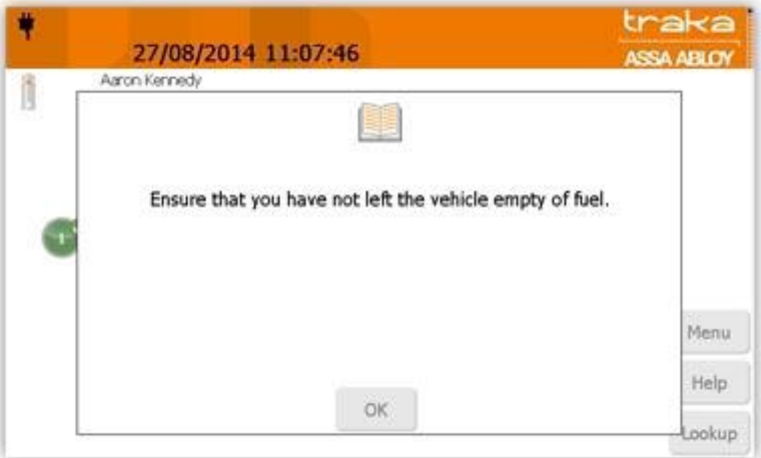


4. Click OK to continue.

NOTE: The item will not be released unless the user selects the OK Button. If the user does nothing, the message will disappear, allowing the user to make another item selection.

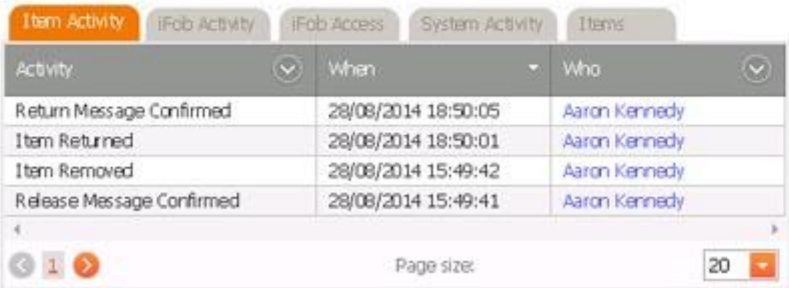
The item will now release from the system.

5. If you have the system setup to show a custom message when the item is returned, the user will access the system in the usual way, return the item to the correct position and receive the message on screen.

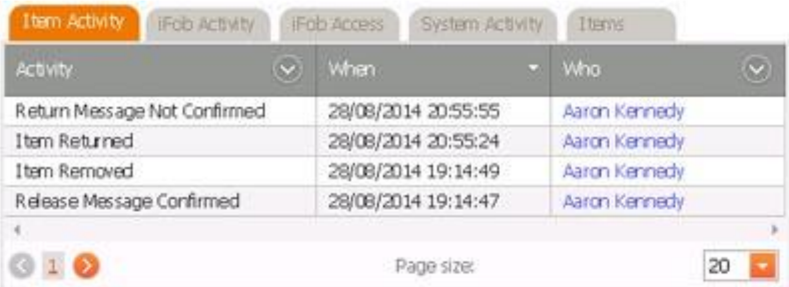


6.5.5 ACTIVITIES

The system viewer displays a grid that holds the last 30 days of activities for the selected iFob/item in the system. When a user selects the OK button after removing/returning an item with a custom message, a 'Return Message Confirmed' and/or 'Release Message Confirmed' activity will be generated in the Item Activity tab.



If a user returns an item that has a custom message and they do not select the OK button when the message appears, a 'Return Message Not Confirmed' activity will be generated.



6.6 EMAIL NOTIFICATIONS

6.6.1 EMAIL NOTIFICATION OVERVIEW

The Email Notification System allows an email to be sent to one or more users when certain system conditions are met. For example, this feature is useful to notify administrators if items are not returned on time, or to send a receipt to a user who has taken an item.

The Email notification will need to be configured in the Business Engine before it is usable in TrakaWEB. For detailed information on how to configure this, please review the 'Email Configuration' section in the latest version of the **TrakaWEB Installation & Configuration Guide – TD0013.**

6.6.2 NOTIFICATION DETAILS

This section explains how to configure the email that will be sent upon a notification being triggered. This includes a range of details such as types of trigger, recipient(s), subject, and the content of the email.

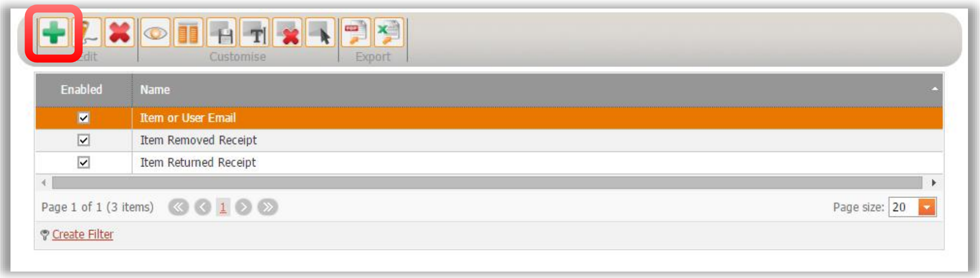
1. From the navigation toolbar at the bottom of the screen, select the Software Settings button.

2. Next, click the Notifications button.

3. You will then be taken to the Notifications page. Here is where all the notifications that you create will be listed.

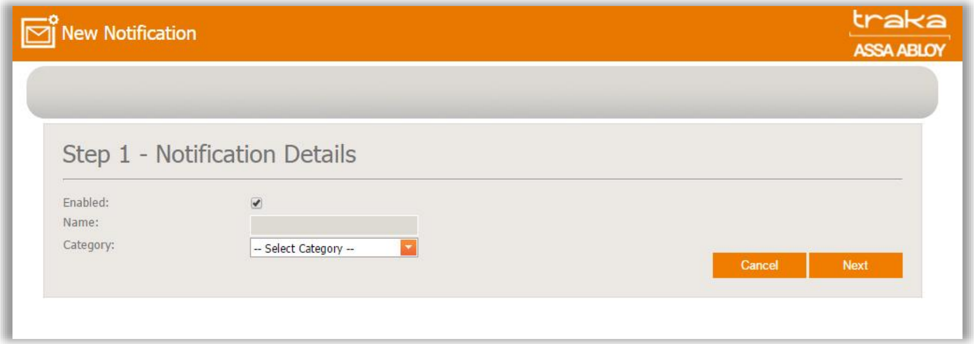
6.6.3 CREATING A NEW EMAIL NOTIFICATION

1. To create a new notification click on the 'Add' icon.



6.6.3.1 NEW NOTIFICATION DETAILS

1. The 'New Notifications' window will appear allowing you to enter specific details.



Enabled: Tick this box to enable the notification.

Name: Enter the name you wish to give the notification.

Category: The drop down box will present you with 5 options.

Each option within the 'Notification Category' contains different notification 'sets'. The Category allows you to customise the different triggers and filters depending on what type of notification you wish to receive. These are as follows:

Item: Creates notifications triggered by Item activity.

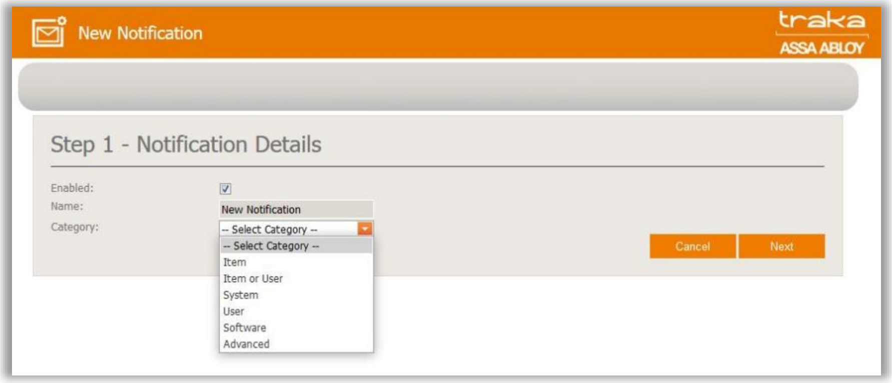
Item or User: Creates notifications triggered by Item or user activity.

System: Creates notifications triggered by System activity.

User: Creates notifications triggered by User activity.

Software: This option will allow notifications to be created by any Software activity.

Advanced: This option is used to create notifications for every type of trigger available.



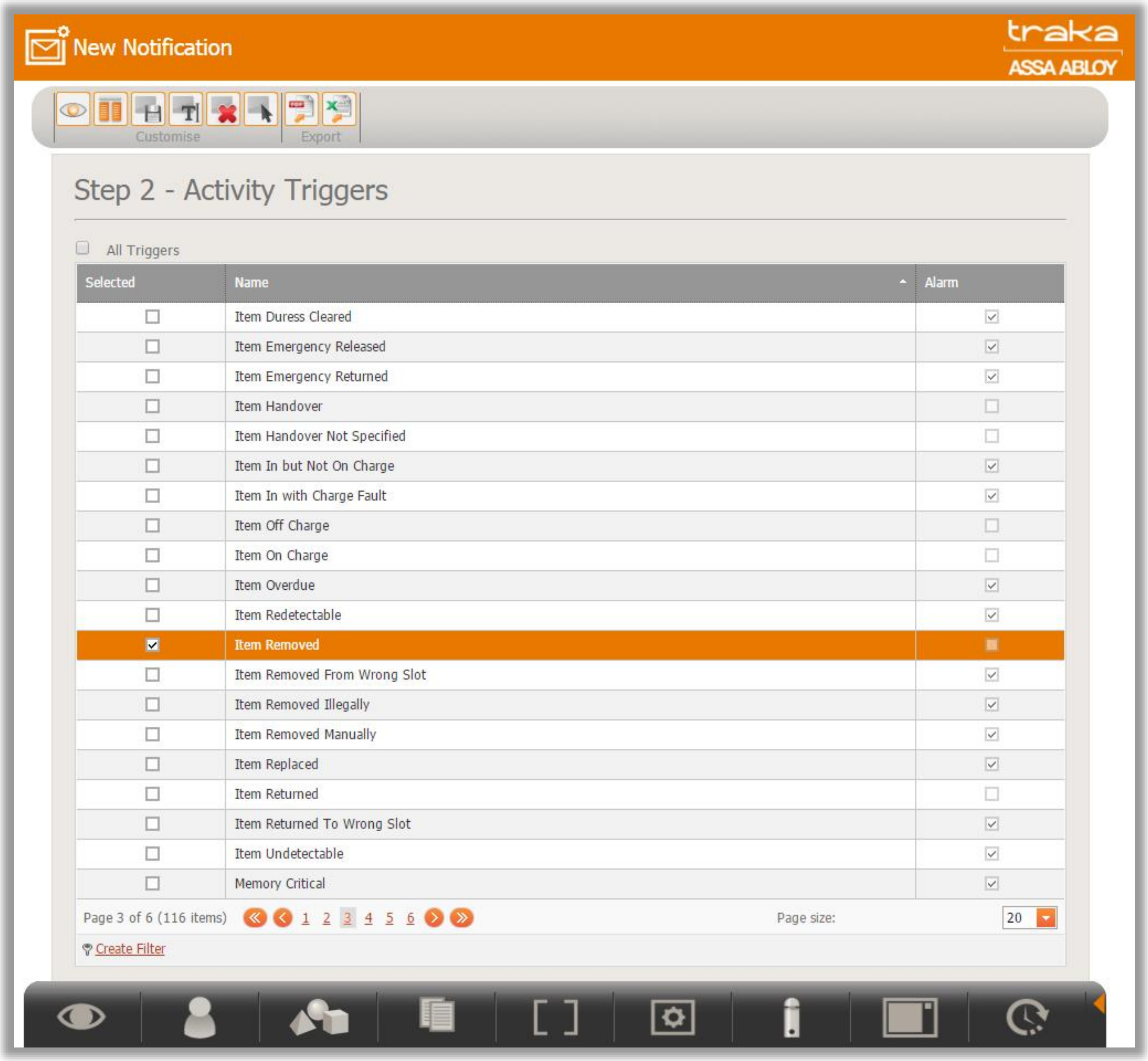
2. Once you have selected an option from the 'Notification Category', click 'Next' to continue.

6.6.3.2 ACTIVITY TRIGGERS

This section explains how to define which activity types can trigger a notification.

Activity Triggers allow the selection of one or more activity types that may trigger a notification. The activity trigger is used in conjunction with filters to allow selection of activity and target object(s) where the target object is a system **OR** item **OR** a user.

From the 'Notification Details' page, you will be directed to the 'Activity Triggers' page. Here you can select one or more activities that will trigger the email notification. Clicking on the Check Box next to 'All Triggers' will automatically select all the Activity Triggers.



In the example above, 'Item Removed' has been selected. This means that when any item is removed from any system by any user, the email notification will be triggered.

If you wish to limit this notification to activities on a particular system, item, or user, you can use the respective filters.

Clicking on the Check Box next to 'All Triggers' will automatically select all the Triggers listed.

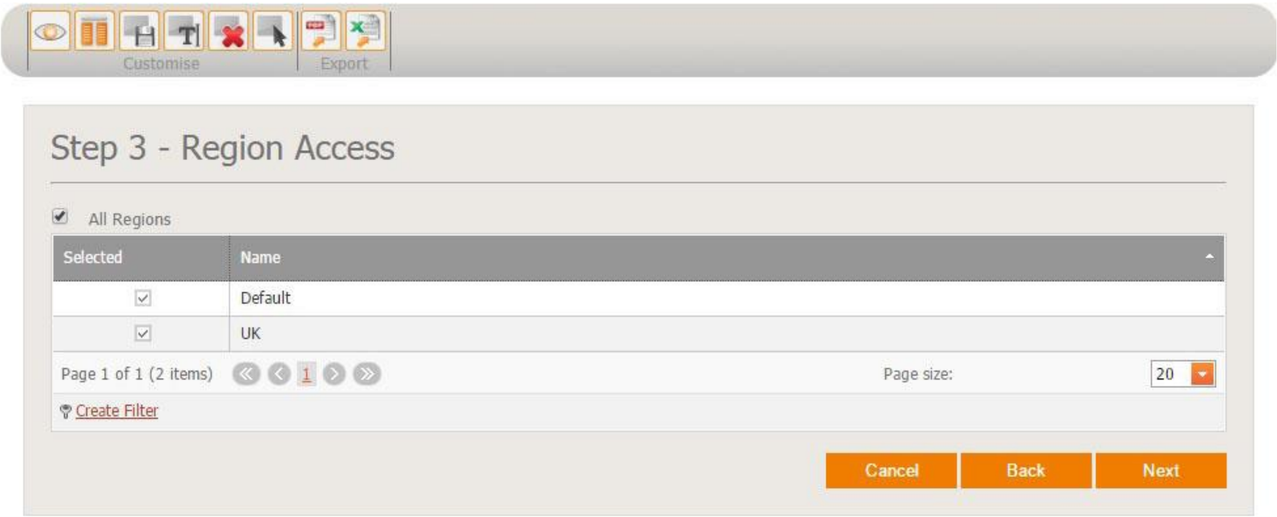
1. When you have completed selecting 'Activity Triggers', click **Next** to continue.

NOTE: If no activity type is selected, then no notification will be triggered for any activity.

6.6.3.3 REGION ACCESS

'Region Access' controls the visibility of the notification role allowing separate roles to be defined per region if required. Region access also adjusts the filters in the filtering section to only show filters relevant to the selected region.

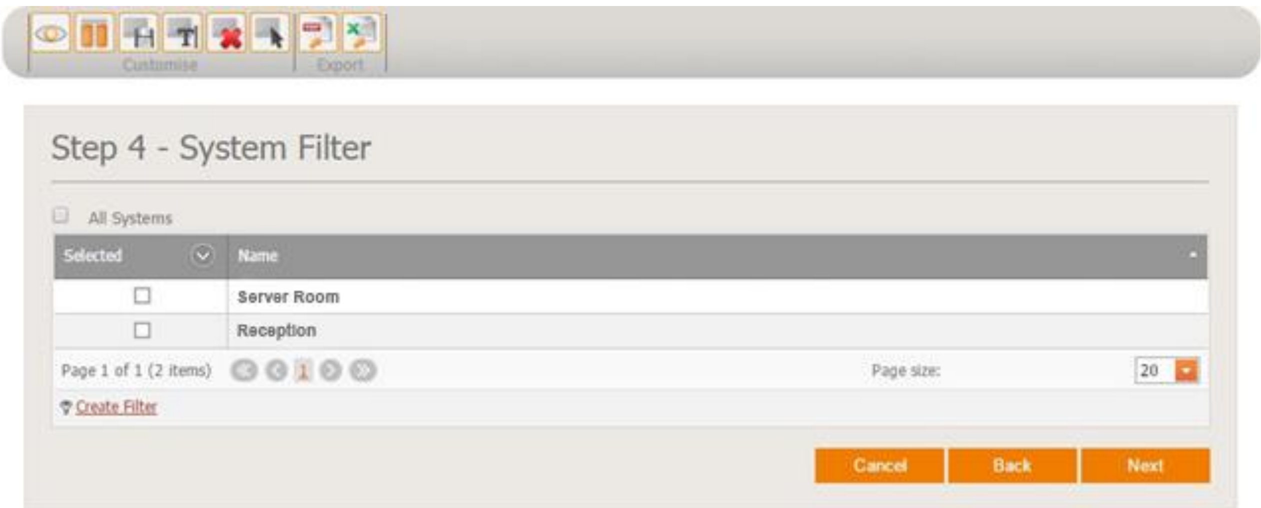
If the logged in user is an 'All Regions' user, the 'All Regions' checkbox will be ticked by default. If the user is not an 'All Regions' user the checkbox will be unchecked and greyed out. The user will then have to select the individual regions they are interested in. Clicking on the Check Box next to 'All Regions' will automatically select all the Regions listed.



6.6.3.4 SYSTEM FILTER

The 'System Filter' allows for the selection of specific cabinet or locker systems. Notifications will be triggered only on the selected system(s).

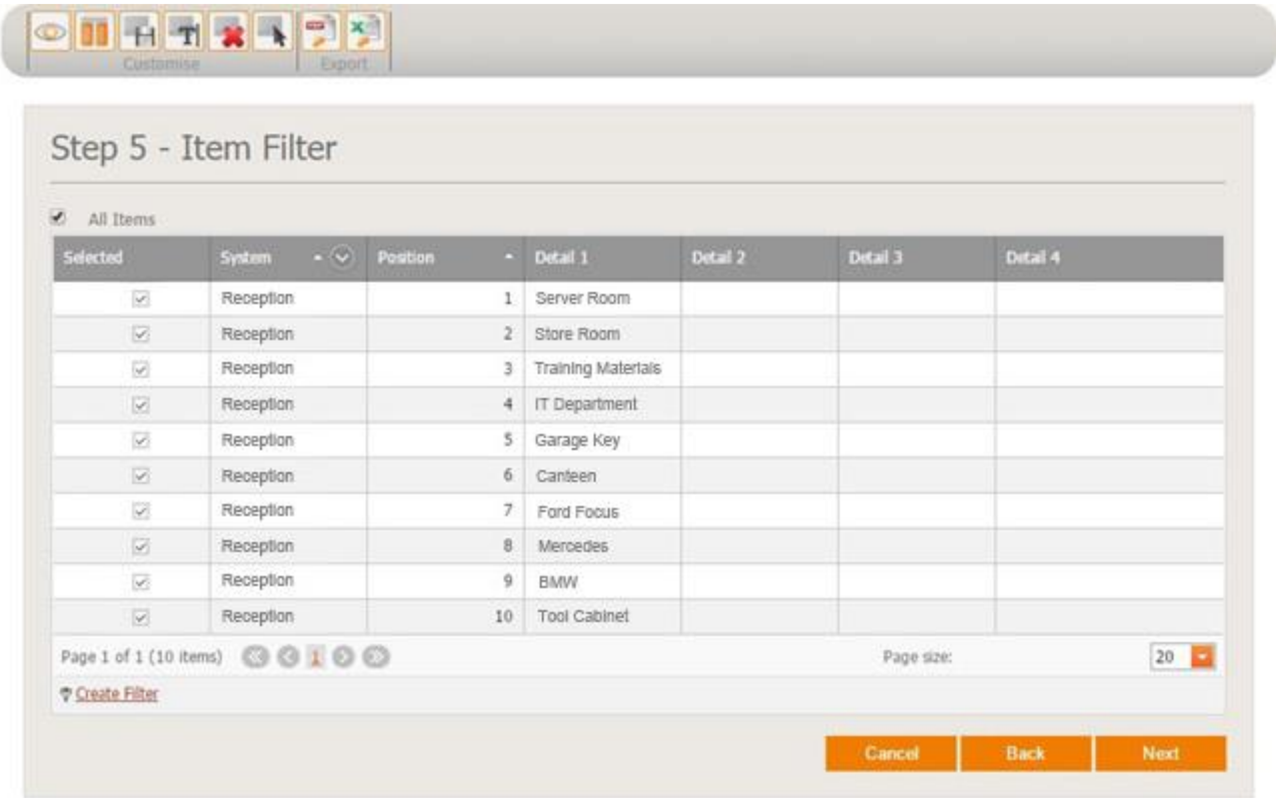
You can specify that only activities generated on a particular system will trigger a notification. Simply tick the box of the system(s) you wish to include. Notifications will only be triggered on the selected systems. Clicking on the Check Box next to 'All Systems' will automatically select all the Systems listed. Once you have finished your selection, click **Next** to continue.



6.6.3.5 ITEM FILTER

The 'Item Filter' allows for selection of specific items. Selecting no item will cause a notification to be triggered when an activity event occurs that references any item, otherwise only the selected item(s). Items will show in this tab depending on what systems are checked in the previous tab.

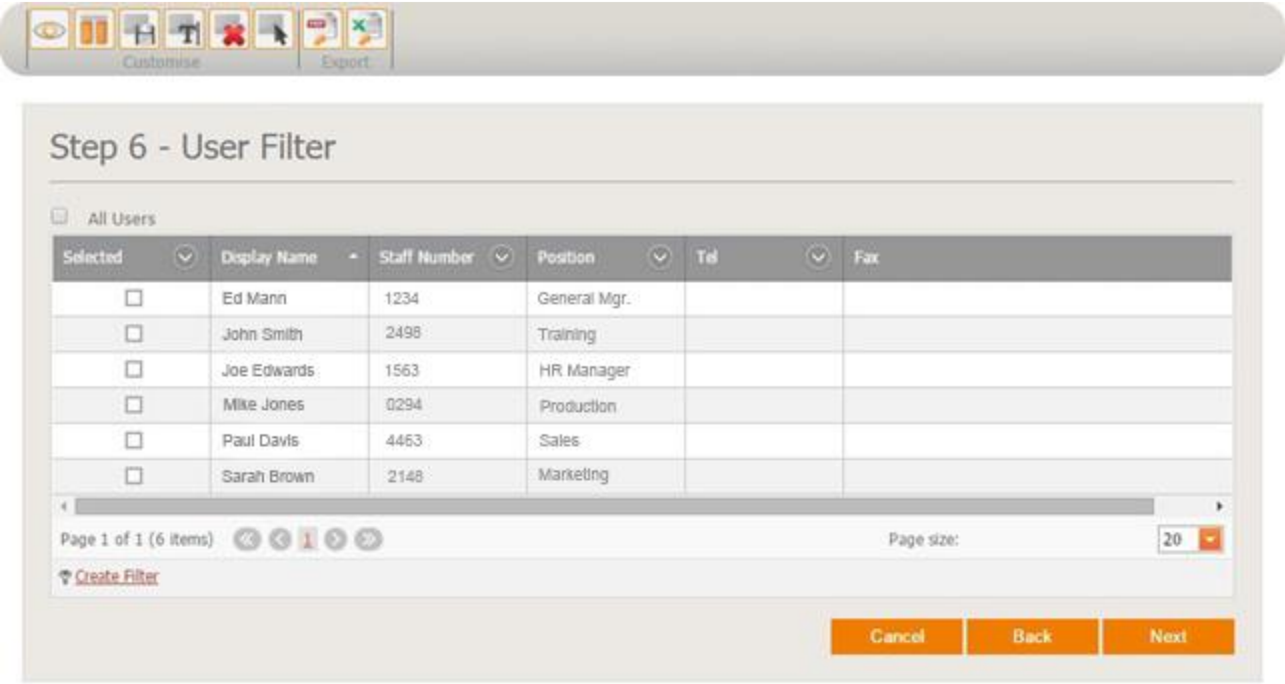
You can specify that only activities generated by a particular item will trigger a notification. Tick the box of the item(s) you wish to include. If no items are selected, then a notification will be triggered for an activity that occurs that references any item. Clicking on the Check Box next to 'All Items' will automatically select all the Items listed. Click 'Next' to continue.



6.6.3.6 USER FILTER

The User Filter allows for selection of specific users. Selecting no user will cause a notification to be triggered when an activity event occurs that references any user otherwise only the selected user(s).

You can specify that only activities generated by a particular user will trigger a notification. Tick the box of the user(s) you wish to include. If no users are selected, then a notification will be triggered for an activity that occurs which references any user. Clicking on the check box next to 'All Users' will automatically select all the Users listed.



Once you have finished selecting Users, click **Next** to continue.

6.6.3.7 EMAIL TEMPLATE

You will now be taken to the 'Email Template' page where you will be required to enter specific details.

To: Enter the email address of the person(s) who will receive this email. When sending to multiple users, separate each address with either a comma or a semi-colon followed by a space. A 'Token' for the users email address may also be used here. By default, the email address is {User.Detail06} but can be customised if required. This is done within 'User Fields' under 'Settings'.

CC: Enter the email address of the person(s) who will be carbon copied with this email.

BCC: Enter the email address of the person(s) who will be blind carbon copied with this email.

Subject: Enter the subject of the notification.

Body: Here you can enter the body of the Email Template. You can also select 'tokens' from the drop down boxes that define certain content of the notification i.e. forename, event, description, timestamp etc. Once selected, they will then populate the body of the email. This indicates what you will see in the email once the notification is sent.

NOTE: The CC and BCC fields are optional.

Below is a list of tokens that are selectable from the drop-down boxes on the Email Template page.

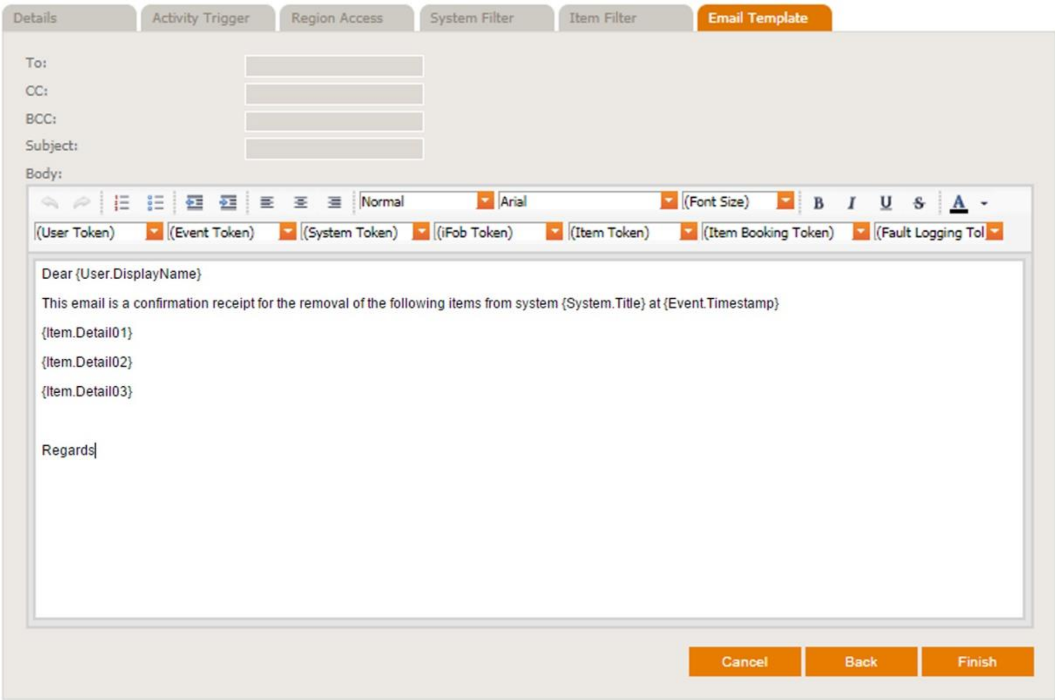
- {User.Forename}
- {User.Surname}
- {User.CardNumber}
- {User.Detail01}
- {User.Detail02}
- {User.Detail03}
- {User.Detail04}
- {User.Detail05}
- {User.Detail06}
- {User.Detail07}
- {User.Detail08}
- {User.Detail09}
- {User.Detail10}
- {User.Detail11}
- {Event.Timestamp}
- {Event.EventCode}
- {Event.Description}
- {System.Title}
- {iFob.Serial}
- {iFob.Positon}
- {iFob.Description}
- {iFob.LastTimeTaken}
- {iFob.LastTimeReturned}
- {Item.Detail01}
- {Item.Detail02}
- {Item.Detail03}
- {Item.Detail04}
- {Item.Detail05}
- {Item.Detail06}
- {Item.Detail07}
- {Item.Detail08}
- {Item.Detail09}
- {Item.Detail10}
- {Item.Detail11}

NOTE: The User Detail tokens refer to the eleven definable fields that you edit in the User Fields.

NOTE: The Item Detail tokens refer to the eleven definable information fields that are saved against a particular Item Type.

NOTE: Item tokens only relate to the first item defined for a position.

NOTE: If you wish to manually place these tokens in the body of the email, please ensure that you start and end each token with the following brackets {}. For example, {User.Forename}.



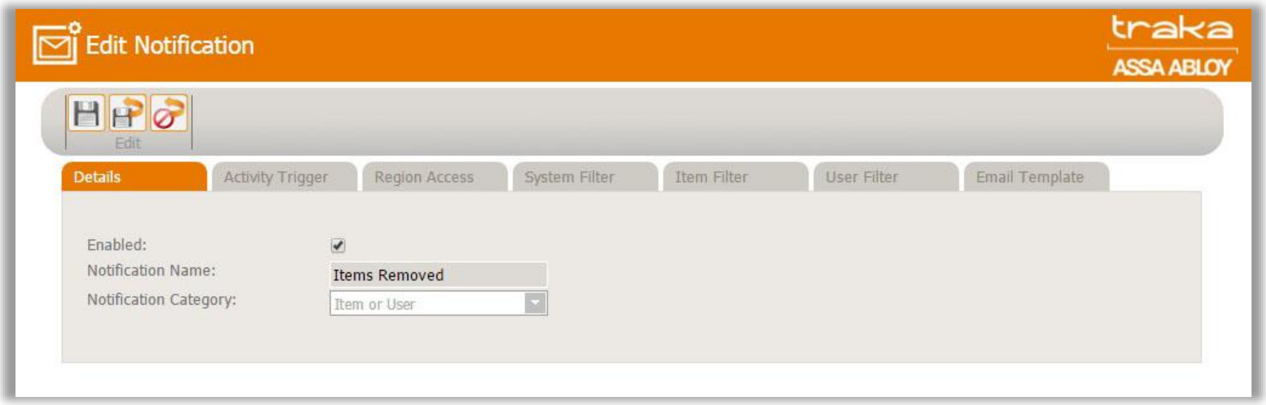
NOTE: It is important to enter information into the Subject field otherwise, the email will not be sent.

Once you have finished creating the Email Template, click the 'Finish' button.

6.6.4 EDITING NOTIFICATIONS

Should you wish to edit any 'Notifications' in the list, you can either double click on a Notification or select the Notification and click 'Edit' as shown below. Depending on which 'Notification Category' was chosen at the start of the process, you will be directed to a new page showing all the specific options as tabs.

Selecting an individual tab will take you to its specific page for editing. When you have finished making your changes, click 'Save and Return'.

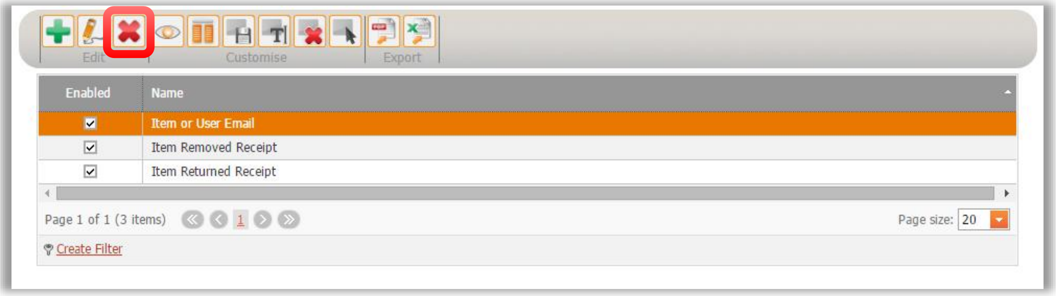


NOTE: It is not possible to change the 'Notification Category' whilst editing. Should you wish to do this, you will have to delete the Notification and create a new one.

Please now refer to the Using Email Notifications section.

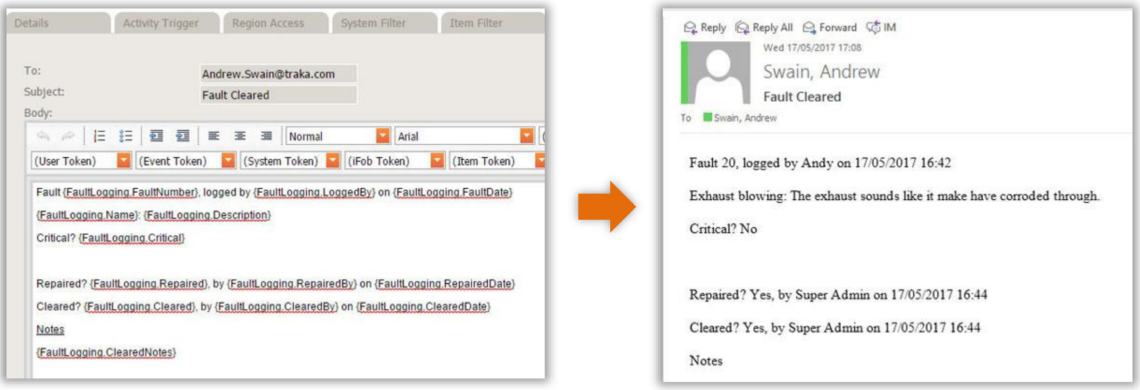
6.6.5 DELETING AN EMAIL NOTIFICATION

To delete an existing email notification, select the notification and then click on delete.



6.6.6 USING EMAIL NOTIFICATIONS

Once you have [set up your Email Notification]() and it is enabled, you will begin to see notifications come through to the specified email addresses. For this example, the following details have been saved as an email notification.



NOTE: This is just an example of how the email notification system works. You can set up many different notifications with very different activity triggers.

1. The user who has been identified with this particular notification accesses the corresponding system.
2. They then remove the appropriate item from the system.
3. This will now trigger the notification to be sent to the email address entered against the notification.

6.7 ITEM BOOKING

Item Booking is a cost option feature, which allows items to be reserved for a specific set of users over a specified time period.

Typical examples of its functionality may include reserving a meeting room, a company pool vehicle, or access to restricted areas and items. Item Booking can also be enhanced with the utilisation of Exception Alerts incorporating Email Notifications. Booking Confirmation Emails are created within TrakaWEB Admin. Furthermore, sub-configuration options are available which can:

- Automatically cancel a booking if associated items have not been taken within a set time from the start of the booking
- Automatically end a booking once all associated items have been returned as opposed to waiting for the end of a booking period
- Configure a limit as to how far in the future a booking can be made for all users

Item Bookings can only be created and edited through TrakaWEB and are not editable at Traka Touch.

6.7.1 ITEM BOOKING-FIXED RETURN OVERVIEW

Item Booking is currently only available on Fixed Return Key Control and Locker Systems, which are not configured to operate as 'First in First Out' or 'Temporary Deposit Locker' modes.

Item Booking allows an item to either; be allocated to an end-user by an Administrator or, for users to login to TrakaWEB and create bookings for themselves when they have been given a special software permission. This permission can be given to users in isolation, therefore allowing them to be able to login and create a booking for themselves but not access any other areas of TrakaWEB.

The Booking Wizard ensures that the Booking process is simple and straight forward. It prompts the user for information such as where the item is being taken from, when the booking will be active and what is being booked. It guides the user step-by-step through all the stages of the booking process. The Wizard also ensures that duplicate bookings cannot be made and that region visibility rules are fully taken into account.

A summary page displays all bookings made by a particular user with a Gantt chart. The chart offers zoom functionality to allow bookings to be viewed over a time period between 1 hour and 1 year.

An individual Traka Touch system will store up to 1,000 current/future bookings at any one time. TrakaWEB can store an unlimited number of bookings across all systems.

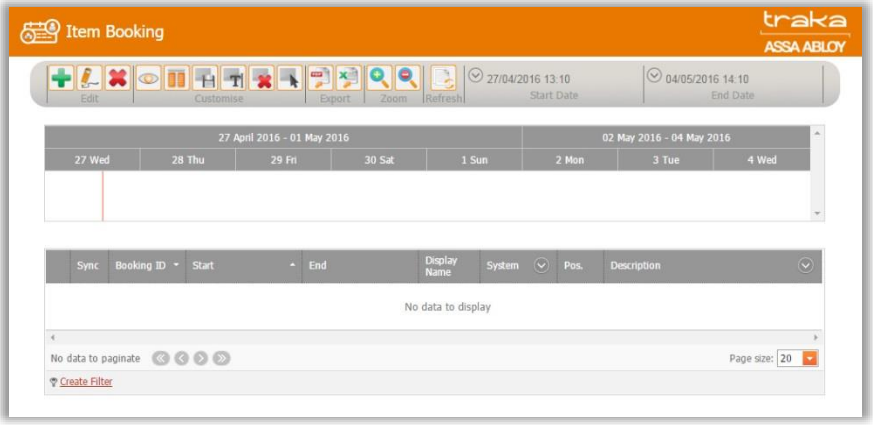
6.7.2 THE ITEM BOOKING LANDING PAGE

The option to navigate to the Item Booking Landing page in TrakaWEB is located in the Navigation Toolbar.

1. Click on the 'Items' icon.

2. From the tab, click on the 'Item Booking' icon.

You will now be taken to the Item Booking Landing Page as shown below.



Many of the icons on the Ribbon Toolbar will appear familiar. You will however notice the addition of 2 magnifying glasses.

NOTE: The zoom features can be used to view details on the Gantt chart once a booking has been created. Because the timescale used within Item Booking can vary between 1 hour and 1 year, you can zoom in to view Bookings set to smaller increments of time or zoom out to view bookings set to larger increments of time.

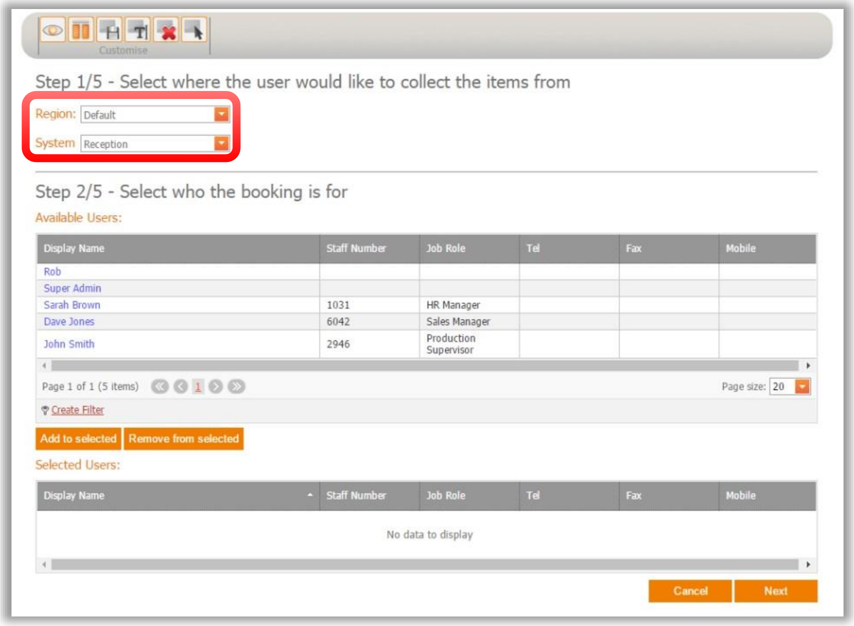
6.7.3 THE BOOKING WIZARD

1. From the main Landing page, click on the 'Create' icon.

Only a user with Administrator access will be able to set up a Booking. This is a 5-step process, divided up over a number of pages. The first page displays the first 2 steps.

Step 1/5 – Select where the user would like to collect the items from

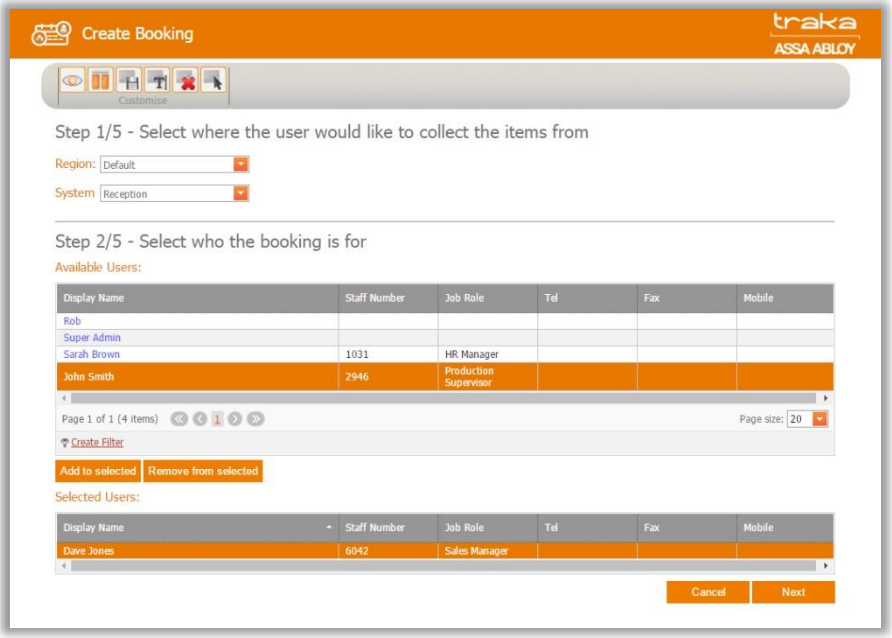
1. From the drop-down menus, select the specific Region and System.



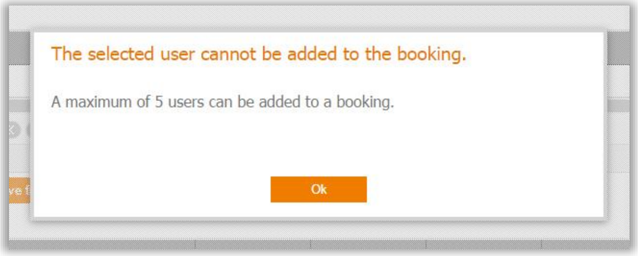
Step 2/5 – Select who the booking is for

2. Select the user you wish to create the booking for. You can either double click next to the name or click on ‘Add to Selected’. The selected name will be added to the ‘Selected Users’ field.

NOTE: If you click on the actual username, you will be redirected to the Edit User page and will have to navigate back to the Item Booking page and start over.



A maximum of 5 users may be added. Should you attempt to exceed this amount; a message will appear. Clicking 'OK' will close the message.

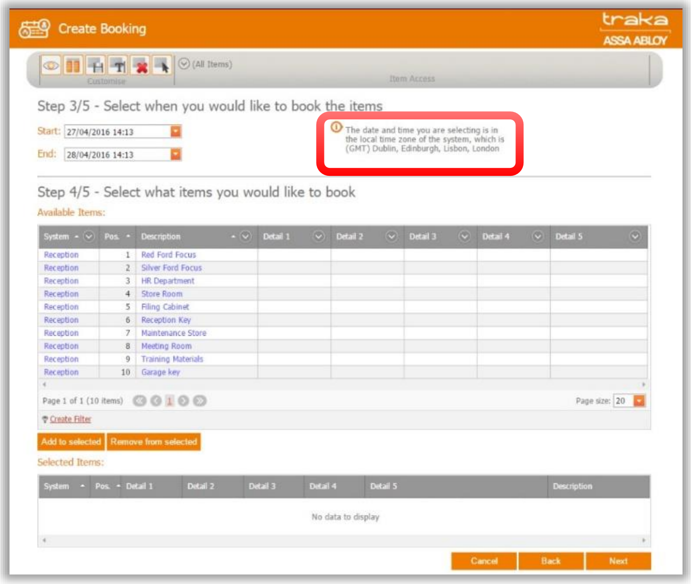


Step 3/5 – Select when you would like to book the items

The next page will continue with the next 2 steps of the process.

NOTE: If at any time, you wish to make a change, click on the 'Back' button to return to the previous page.

NOTE: The date and time chosen for the booking is in the local zone of that system. The time zone of the system is displayed within the booking wizard, as seen in the screenshot below.

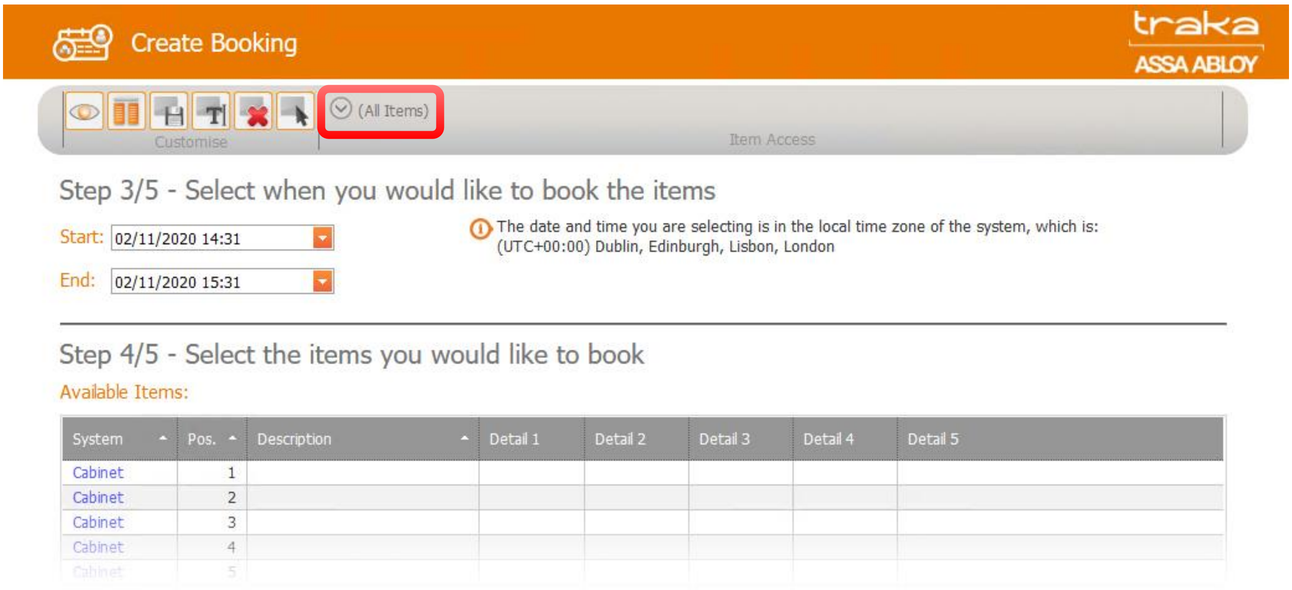


At the top of the page, there is a drop-down filter option which may be set as **All Items** or **Authorised Items.**

NOTE: The filter options are dependent on whether the 'Unrestricted Software Item Access' option is ticked in Software Permissions Groups.

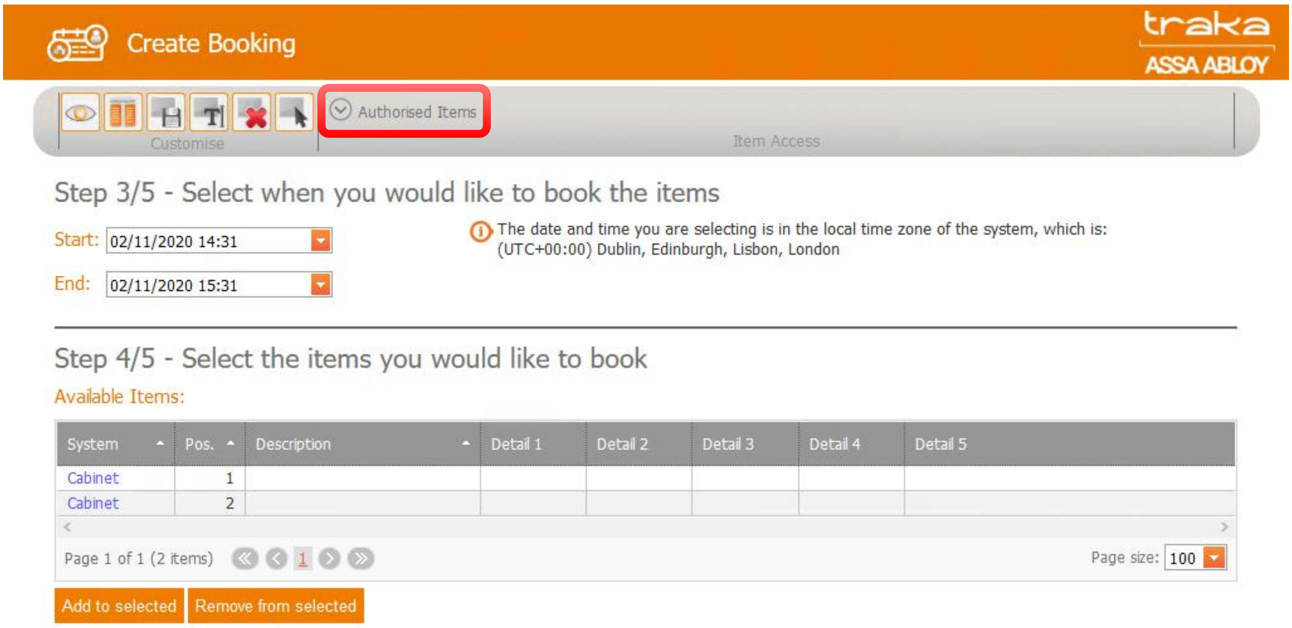
With the **All Items** filter enabled, any Item may be booked for a user regardless of whether or not they have access to it.

NOTE: This option will only be available if the 'Unrestricted Software Item Access' option is ticked in the Software Permissions Groups.



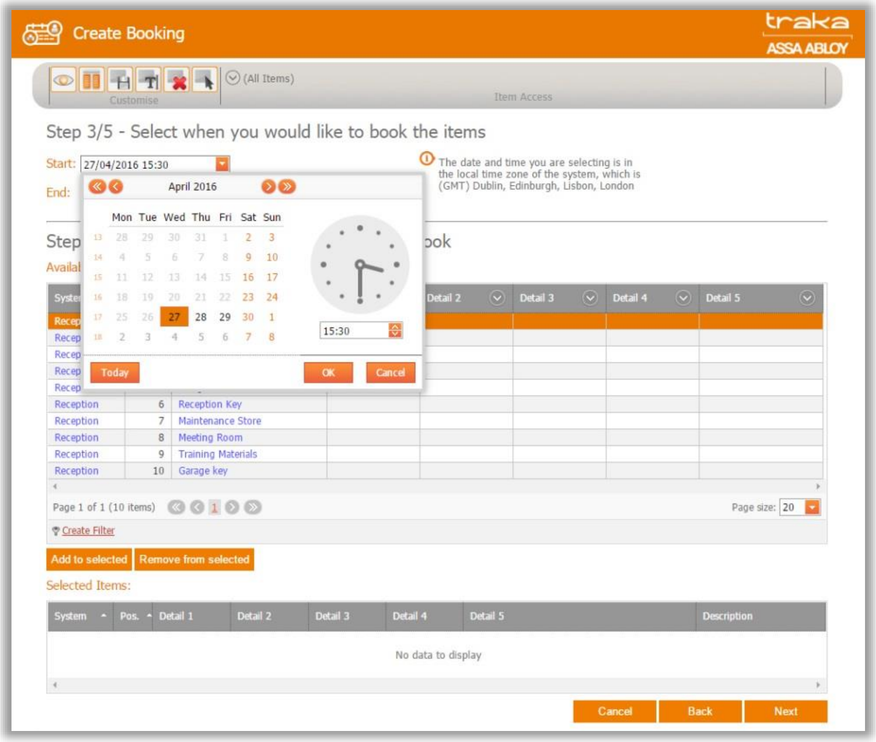
From the dropdown menu, the filter may be changed to **Authorised Items.** With this enabled, a user may only book items that they have been assigned access to.

NOTE: With the 'Unrestricted Software Item Access' option unticked in the Software Permissions Groups, this will be the only available option.

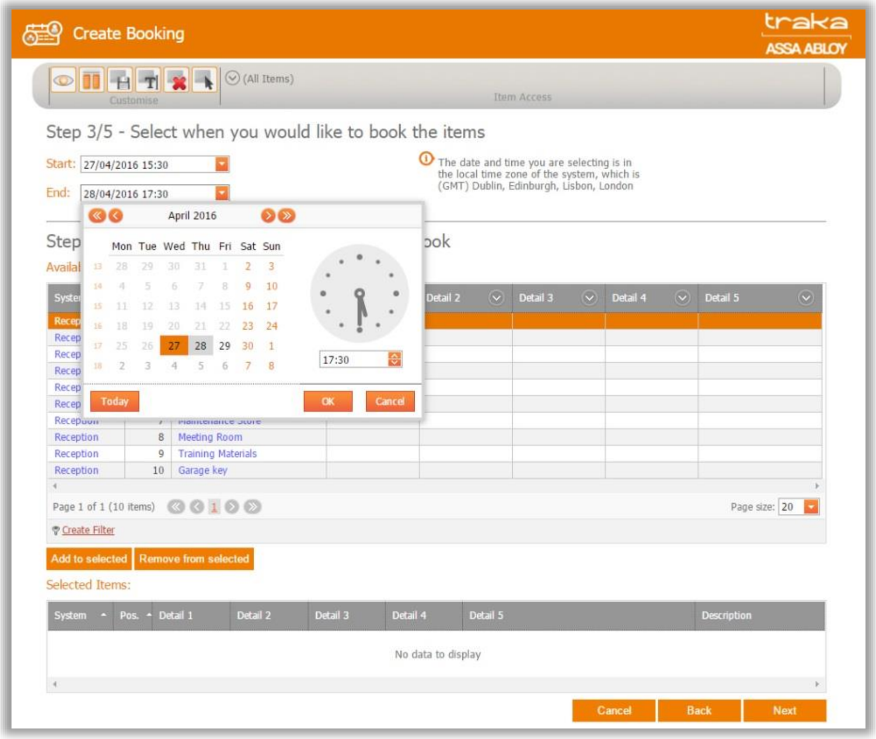


Once you have made a selection, you can progress with setting a start and end duration for the booking.

3. Click on the **Start** drop-down and select when the booking will start. Then click **OK**.



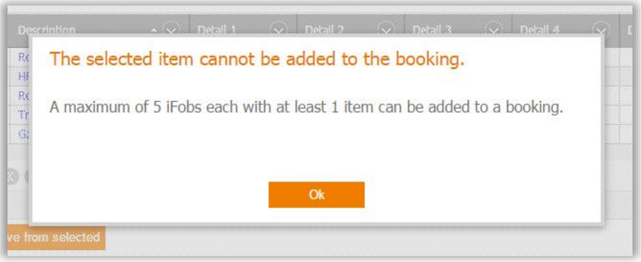
4. Click on the drop-down menu for **End** and select when the booking will end then click **OK**.



Step 4/5 – Select the items you would like to book

5. Select which items you would like to book. Either double click next to the item or click on 'Add to Selection' to add them to the Selected Items field.

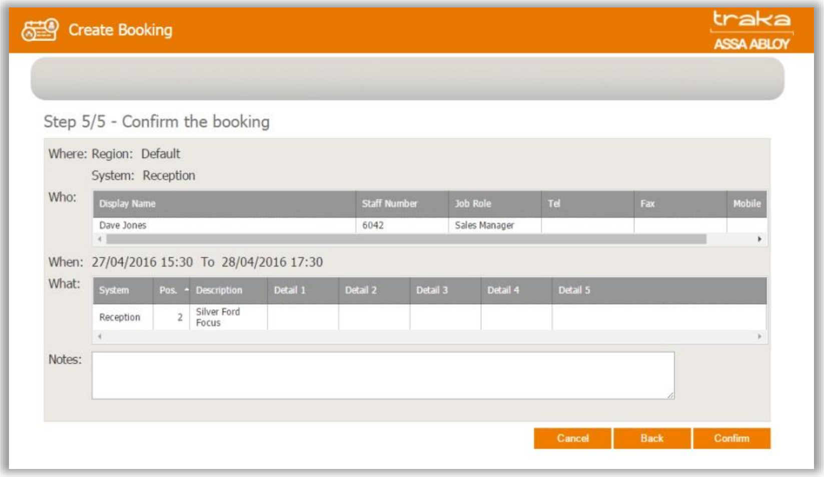
A maximum of 5 items may be added. Should you attempt to exceed this amount; a message will appear. Clicking 'OK' will close the message.



6. Once you have finished selecting items. Click 'OK' to continue.

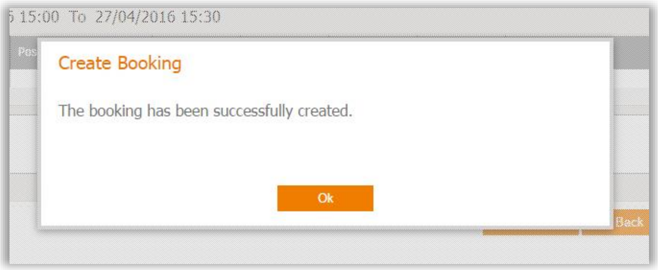
Step 5/5 – Confirm the booking

Step 5 will summarise the information entered from the previous 4 steps. If required, you can add notes in the space provided.

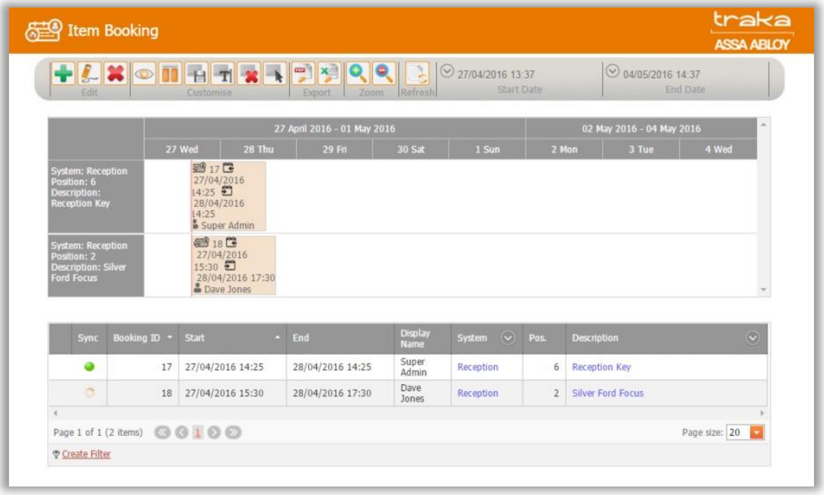


7. If you are satisfied that the details are correct, click 'Confirm' to continue.

8. A message will appear to inform you that the booking has successfully been created. Click 'OK' to close the message.



The Item Booking Landing page will display a Gantt chart showing a timeline for the booked items. The timeline in the example below is divided into 2 horizontal columns: days and months.



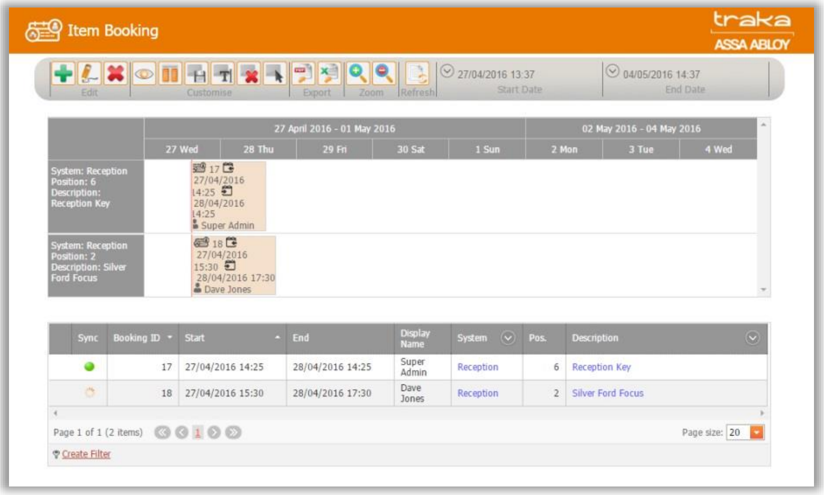
6.7.4 ADDING EXTRA USERS TO AN EXISTING BOOKING

If required, additional users maybe included to an existing booking. This will however still apply to a maximum of 5 users per booking.

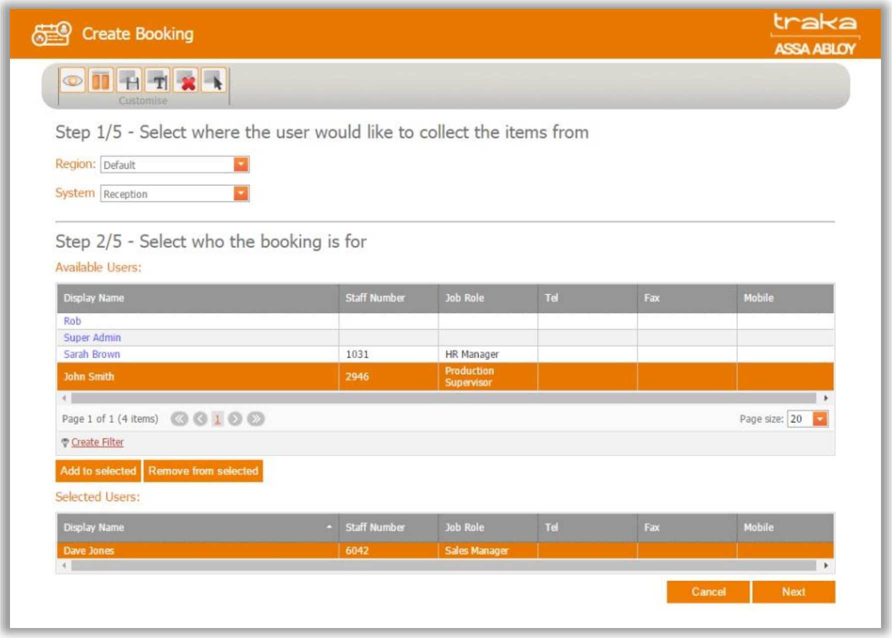
1. Select the Item Booking from the Navigation Toolbar.

The existing Item Booking chart will be displayed.

2. Select the booking that you wish to include additional users and then select the 'Edit' button. This will then take you through the 5-step process.



3. From the available list of users, select the new user to be added to the selected booking.



NOTE: When adding extra users, any items that the editing user has not been granted access to, will be removed from the booking.

Once completed, click on Next and make any further changes as required.

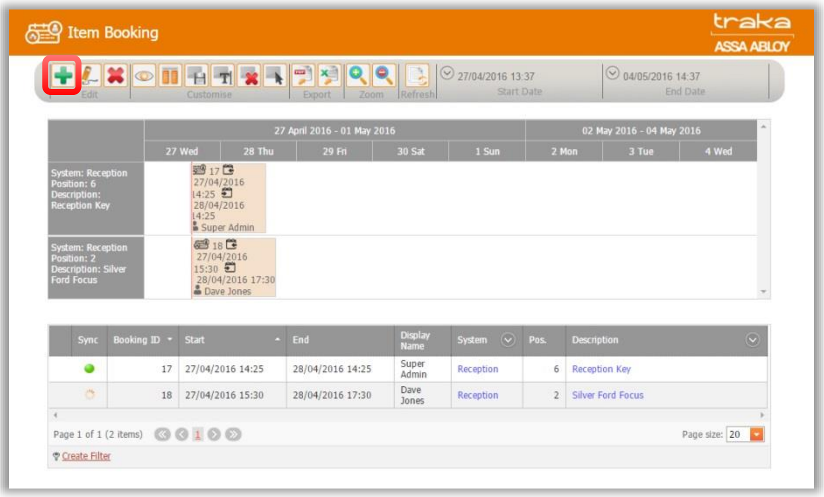
6.7.5 ADDING EXTRA ITEM BOOKINGS

If required, you may add extra bookings to the one already created.

1. Click on the 'Item Booking' icon in the Navigation Toolbar.

The existing Item Booking chart will be displayed.

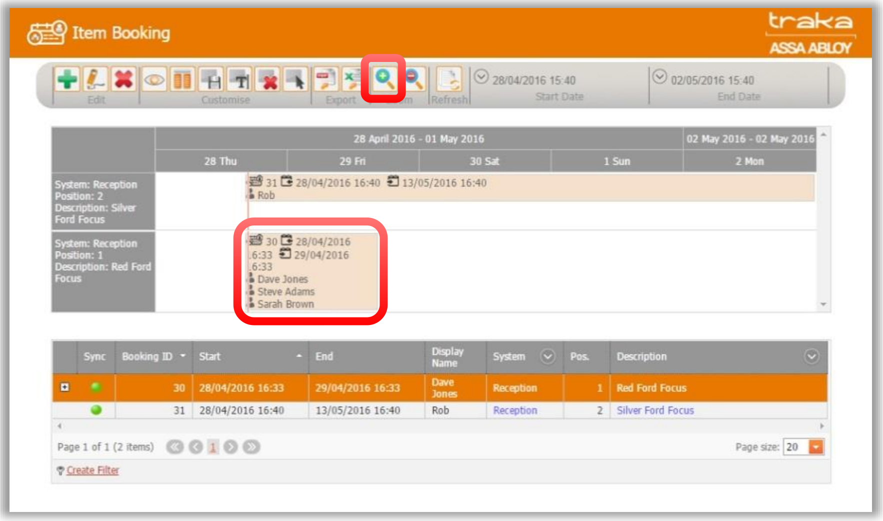
2. Click on the 'Create' icon. This will take you back through the 5-step process to create another booking.



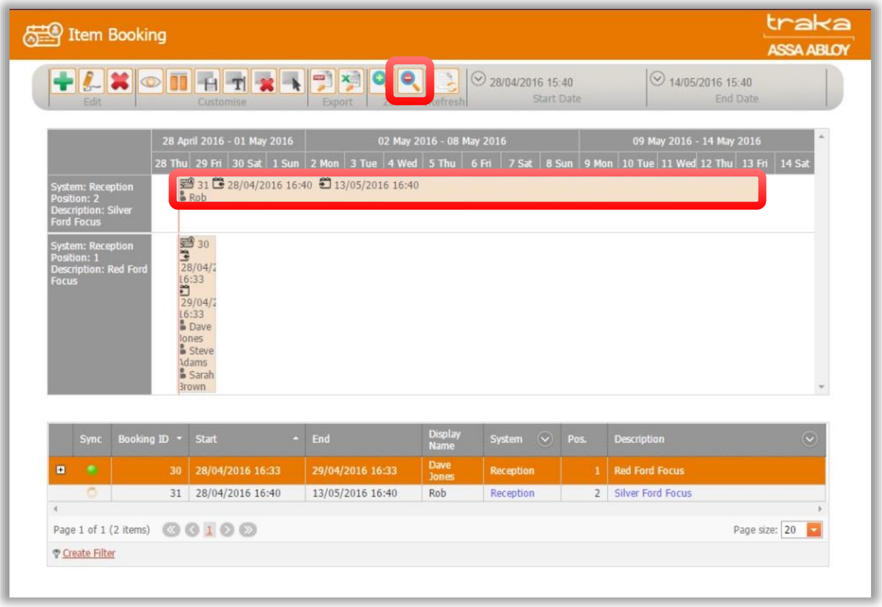
6.7.6 USING THE ZOOM FEATURE

The Zoom feature will allow the user to zoom in and out of the Gantt chart. This allows for easier viewing between bookings made for an hour and bookings made for up to a year.

The example below demonstrates 2 bookings made for 2 different periods of time. The zoom-in button has been used in this case to better view the booking details for an item over a period of 1 day.



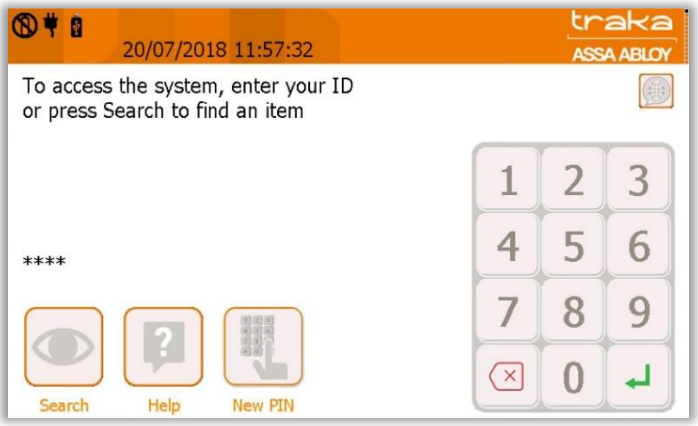
The example below shows the same booking, but the zoom-out feature has been used to view a booking made over a significantly longer period of time.



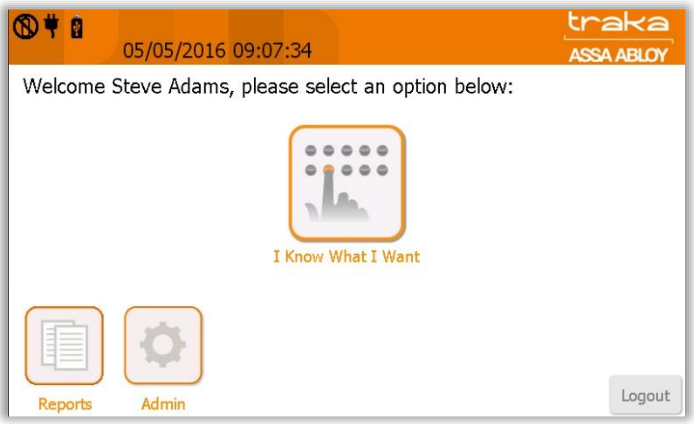
6.7.7 COLLECTING BOOKED ITEMS

Once a user has booked an item, it will be accessible to them at the system.

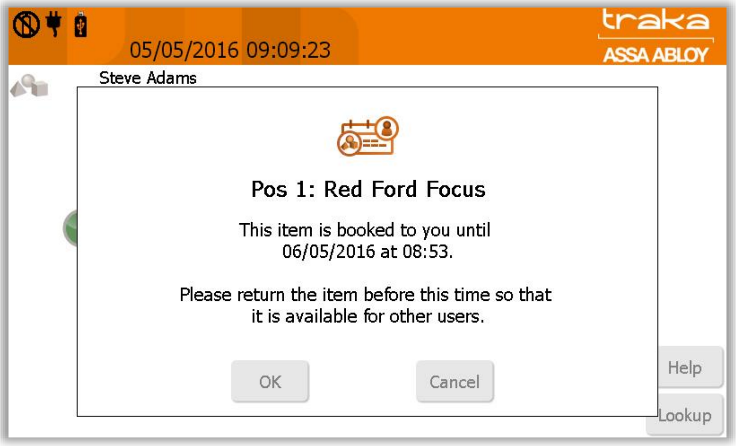
1. Click on the screen to access the keypad.
2. Access the system by using your ID. This may include Keypad ID, swipe card or fingerprint.



3. Click on 'I Know What I Want'.



The door will open and if the item is available to you, it will now be accessible. A message will appear on the screen providing you with the Booking information.



6.7.8 ITEMS NOT TAKEN

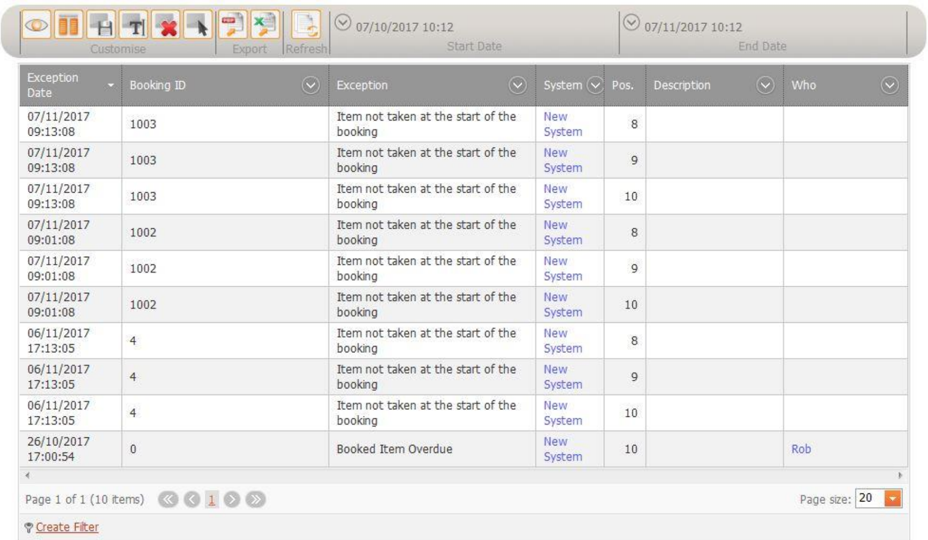
A sub-configuration option is available which can be used to cancel a booking if the items have not been taken within a configurable timeframe from the start of the booking. For example, an Item Booking has been set to begin at 09:00 and the cancellation timeframe is set to 30 minutes. If the user attempts to remove the item at 09:35, it will already have been cancelled. The timeframe can be set as follows:

- 5-60 minutes
- 1-24 hours
- 1-365 days

If there are multiple items associated with a booking and some but not all of the items have been taken, then the booking in this case will not be cancelled.

If a user only has access to items through Item Booking and the booking has been cancelled, they will no longer be able to gain access to the item unless they have been given Item Access to do so.

An exception report will be created in TrakaWEB showing a list of 'Items not taken at the start of a booking' as shown.



Exception Date	Booking ID	Exception	System	Pos.	Description	Who
07/11/2017 09:13:08	1003	Item not taken at the start of the booking	New System	8		
07/11/2017 09:13:08	1003	Item not taken at the start of the booking	New System	9		
07/11/2017 09:13:08	1003	Item not taken at the start of the booking	New System	10		
07/11/2017 09:01:08	1002	Item not taken at the start of the booking	New System	8		
07/11/2017 09:01:08	1002	Item not taken at the start of the booking	New System	9		
07/11/2017 09:01:08	1002	Item not taken at the start of the booking	New System	10		
06/11/2017 17:13:05	4	Item not taken at the start of the booking	New System	8		
06/11/2017 17:13:05	4	Item not taken at the start of the booking	New System	9		
06/11/2017 17:13:05	4	Item not taken at the start of the booking	New System	10		
26/10/2017 17:00:54	0	Booked Item Overdue	New System	10		Rob

Page 1 of 1 (10 items) Page size: 20
Create Filter

6.7.9 END BOOKING UPON ITEM RETURN

A simple sub-configuration option is available when Item Booking is enabled that will end a booking once one or all of the associated items have been returned to the system. This sub-configuration can also be used with the 'Items not Taken' option.

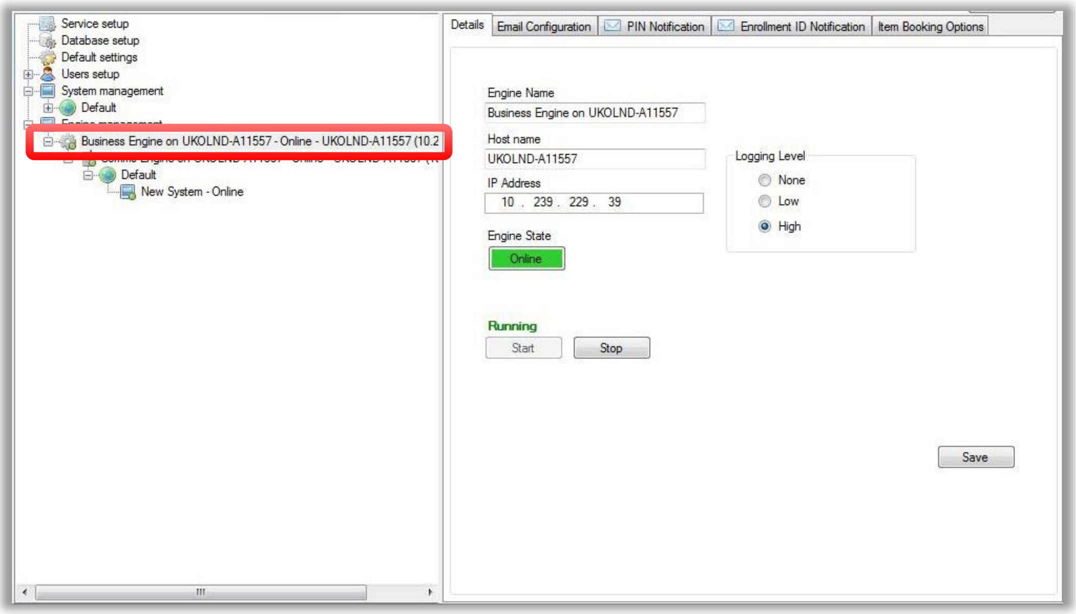
It is not a requirement that all the associated items have to be taken and returned before this mode of operation is terminated. For example, if 3 items have been booked and only one has been taken, upon its return to the system, the booking will end. If users want to book multiple items, they should consider removing all the items at once or create an individual booking for each item.

Traka Touch will monitor the return of items to the system, checking against active bookings and generate a 'Booking Ended' system event. This event will be shown in the System reports along with the booking reference number and the end date and time that the items were returned.

6.7.10 RESTRICT FUTURE BOOKINGS

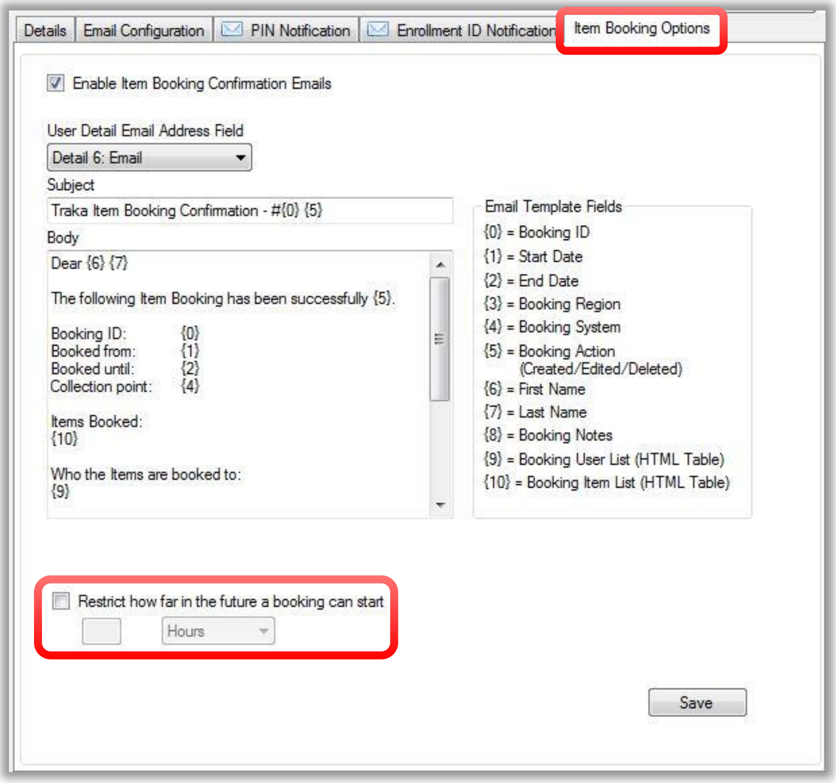
An option is available to configure how far in the future an Item Booking can be made for all users through TrakaWEB. This option is configured within the Admin App and will affect TrakaWEB only.

2. Within the TrakaWEB Admin App, select the **Business Engine.**

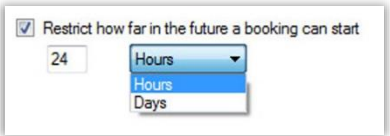


3. Next, select the **Item Booking Options** tab.

The option for the future booking restrictions is located at the bottom of the window as shown below.

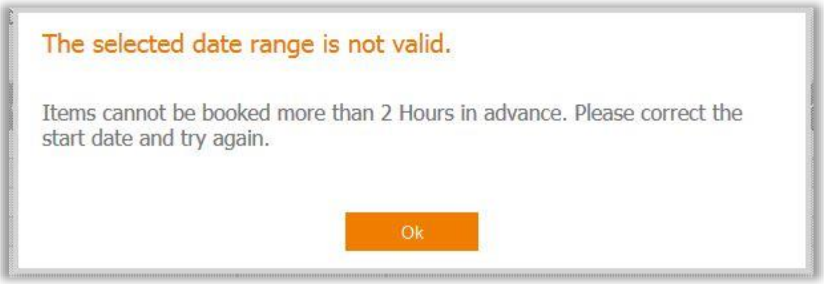


Once the checkbox has been enabled, the text box will default to 24 and the units will be in hours. The drop-down box will enable you to switch between Hours and Days and the number in the text box can be changed manually.



Once enabled, the Booking Wizard will enforce the booking restriction on creating or editing bookings for both Booking Users and Booking Administrators.

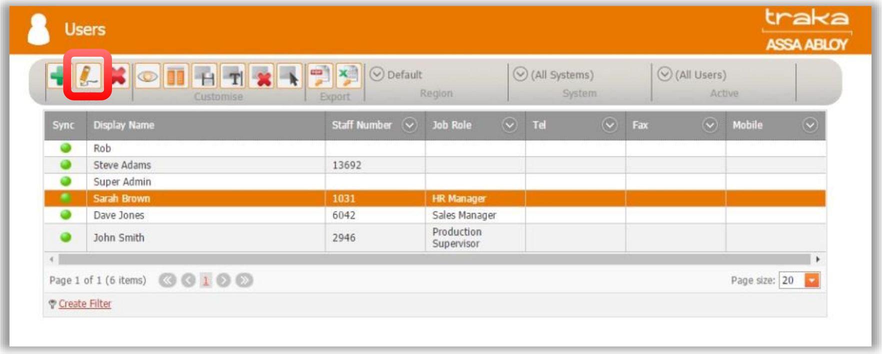
The start date restriction will be calculated against the current time of the selected system based upon its time zone. For example. If a 2-hour restriction time has been set in place and a user attempts to make a booking that falls outside of the 2 hour restriction, a warning will be displayed as shown.



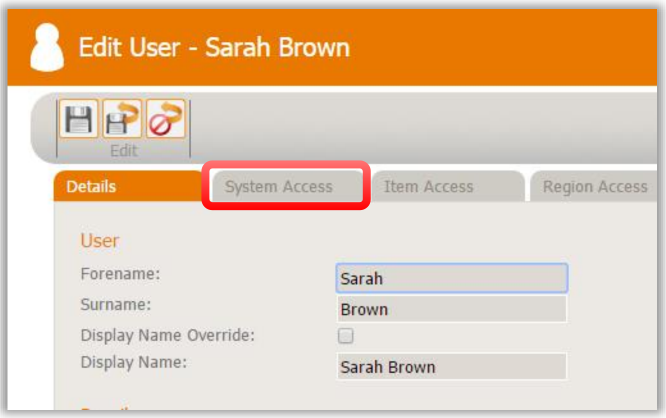
6.7.11 ITEM BOOKING OVERRIDE

The Item Booking Override feature allows a user with special permissions to book an item that already has a booking allocated against it.

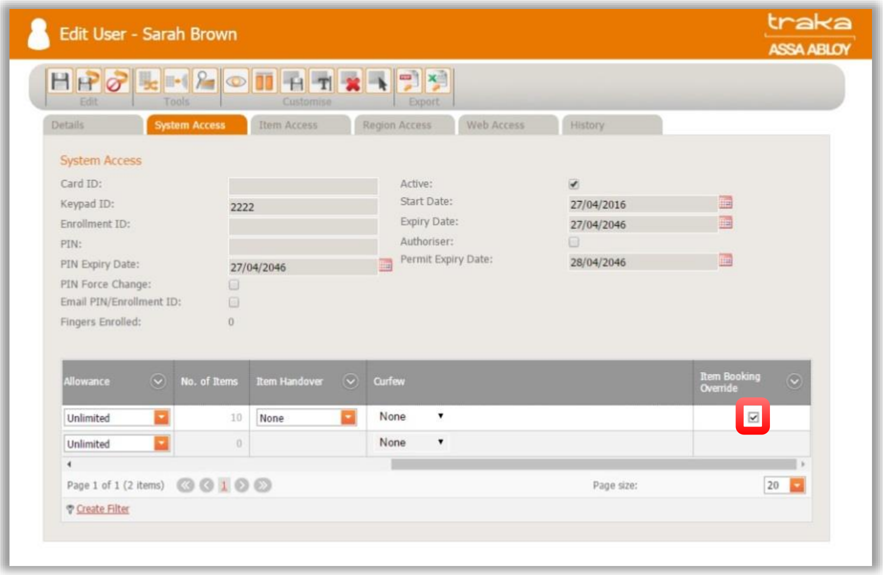
1. Select the user you wish to allocate the Booking Override permission to and then click the 'Edit' button.



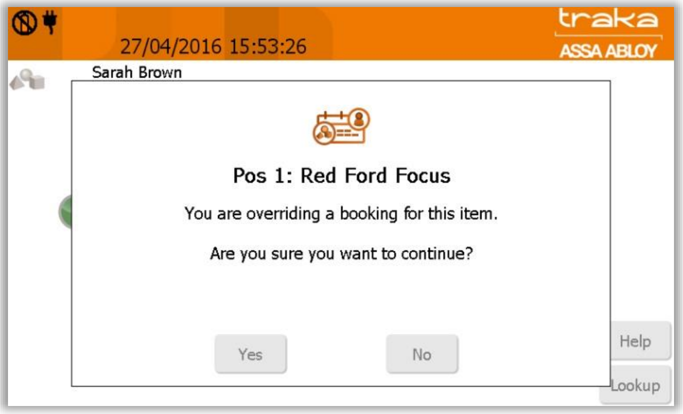
2. At the next page, click on the 'System Access' tab.



3. At the bottom of the 'System Access' page, scroll to the right and click on the check box under 'Item Booking Override' as shown below.



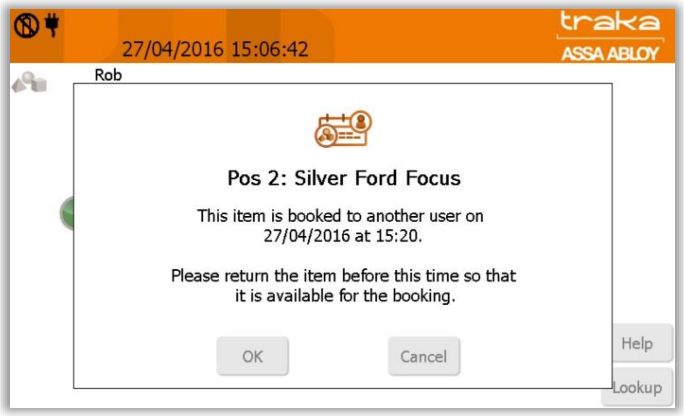
With the 'Item Booking Override' permission given to the user, they now have the ability to override an already booked item.



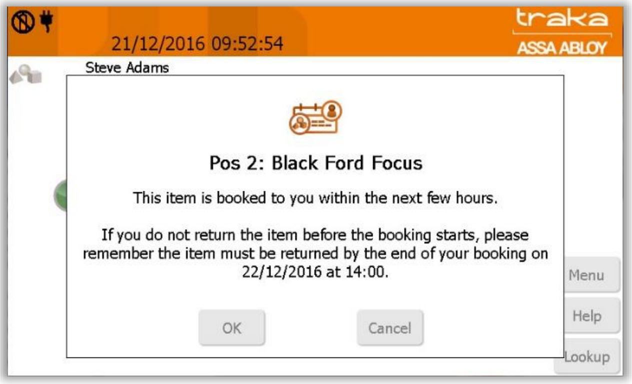
6.7.12 ITEMS BOOKED TO OTHER USERS

When a user has made a booking, the Traka Touch screen will display which items are already held by other users.

It is possible to access an item that is already booked to another user up to 12 hours before its next booking, so long it is still within the system. In this situation, the user will be advised of the booking details and when the item should be returned.



A user may also remove an item that is already booked to them up to 12 hours prior to when the booking period is due to commence. In this instance, the system will remind the user to return the item before the booking begins.



NOTE: If a user takes an item before the next booking begins and fails to return it before that time, the system will record an 'Item not returned prior to booking' event.

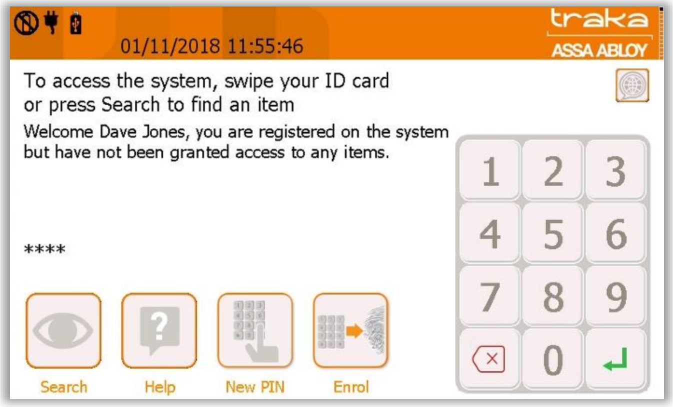
NOTE: If a user takes an item before or during a booking and fails to return it before the booking ends, the system will record an 'Item not returned at the end of the booking' event.

NOTE: Exception Alerts can be created in the form of Email Notifications to inform users when items need to be returned or when items have not been returned to the system. This is particularly useful for back-to-back bookings.

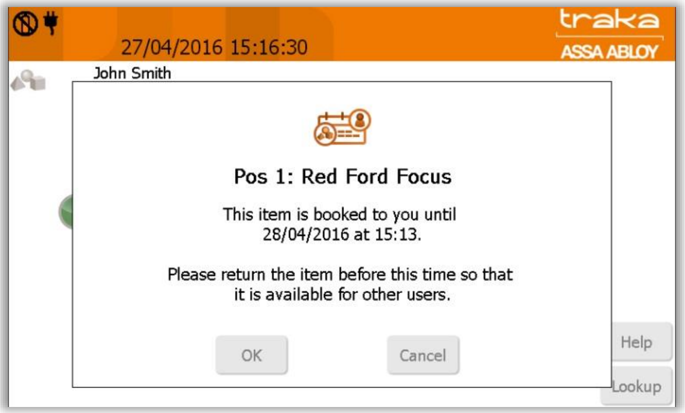
6.7.13 ACCESS RESTRICTIONS

A situation may arise whereby an administrator would only want certain users to only have access to items via an Item Booking. Therefore, when the user has no active bookings, they are unable to access the system. This can be done whereby the user is given login credentials and is set as active on the system but not granted access to any items. A typical example of this may be where the user requires access to cleaning materials during a specific work shift, but not at any other time.

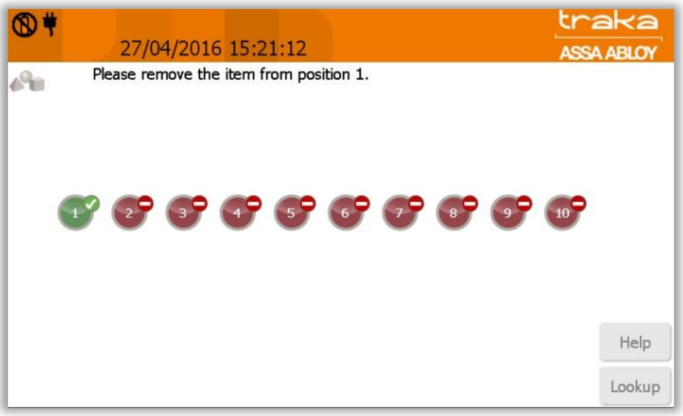
When the user enters their ID at the Traka Touch Screen and they have no active bookings, they will see the following screen.



However, when a single item is granted to the user via a booking, the Traka Touch screen will display a message stating which item they have access to, and the time restrictions applied.



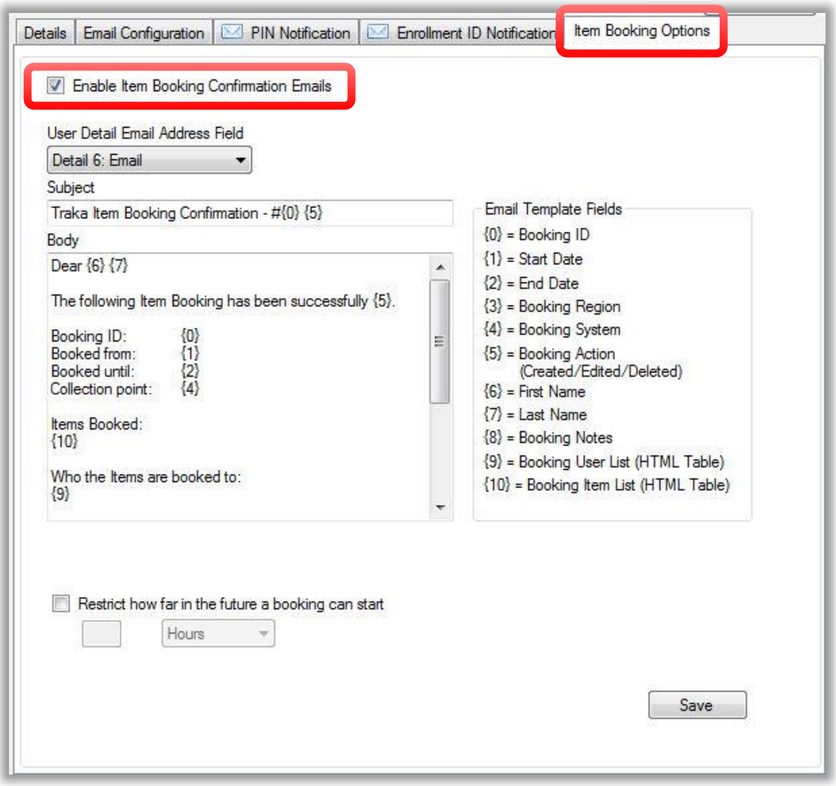
The user can then remove and return the item at the system in the usual way.



6.7.14 ITEM BOOKING CONFIRMATION

The ability to enable the Item Booking feature to send confirmation Emails is set up within TrakaWEB Admin.

1. Within TrakaWEB Admin, click on the 'Item Booking Options' tab.
2. Select the 'Enable Item Booking Confirmation Emails' checkbox.



You will be able to use placeholders to populate each individual field with information relating to the Email confirmation you wish TrakaWEB to send to users, including email address, subject and the main body of text for the notification.

3. Once you have created the notification, click on the 'Save' button.

6.7.15 SOFTWARE PERMISSIONS GROUPS

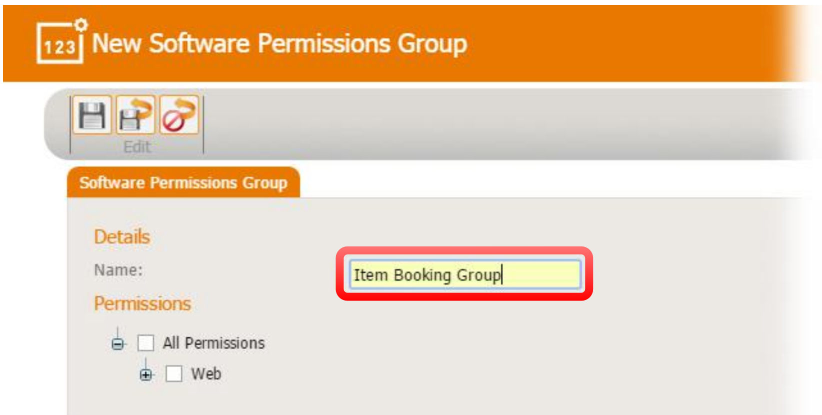
Special software permissions can be given to users to allow them to create or amend their own bookings. Likewise, permissions can also be given to create bookings for other users which could be granted to a booking administrator.

The software permissions can be restricted down so that only the booking summary page and Booking Wizard are accessible to the end-user, making an effective self-booking portal environment. Alternatively, users can be granted access to the other areas of TrakaWEB as well.

1. From the Navigation Toolbar, click on the 'Software Permissions Group' button.

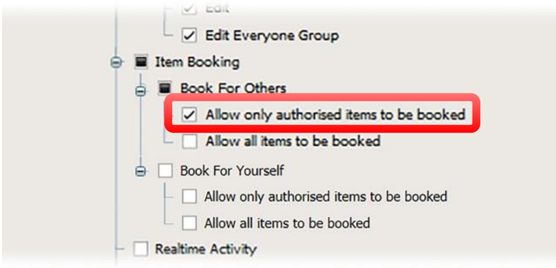
2. You will now be taken to the 'Software Permissions Groups' page. Click on the 'Create' button to continue.

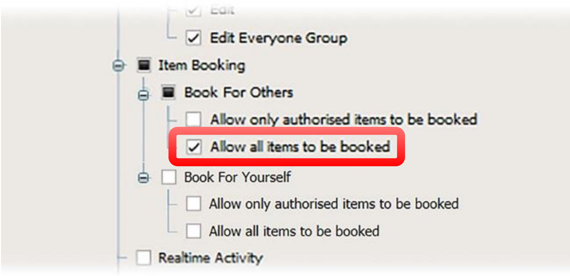
3. At the next page, you can insert the name of your 'Software Permissions Group'.



4. Expand the Permissions tree and select the check boxes for the specific Permissions as shown in the examples below.

Book for Others



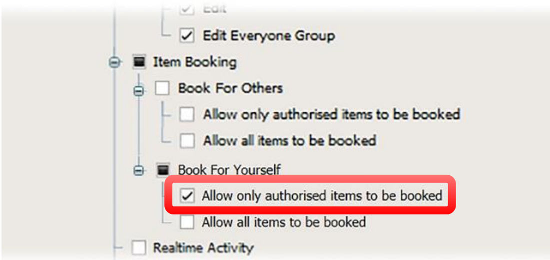


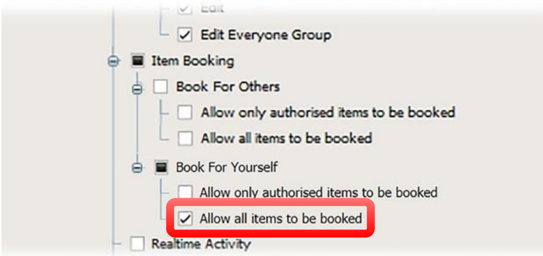
The check box for **Allow only authorised items to be booked** will allow users who have been granted access to those items to be able to take them during a booking.

The check box for **Allow all items to be booked** will allow users to take booked items even if they have not been granted access to them.

If both check boxes are selected, then the option 'Allow all items to be booked' will apply. If both boxes are left unchecked, then you will be unable to book items for others.

Book For Yourself





The check box for **Allow only authorised items to be booked** will allow users who have been granted access to those items to be able to take them during a booking.

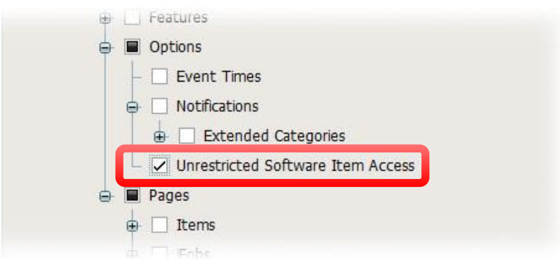
The check box for **Allow all items to be booked** will allow users to take booked items even if they have not been granted access to them.

If both check boxes are selected, then the option 'Allow all items to be booked' will apply. If both boxes are left unchecked, then you will be unable to book items for yourself.

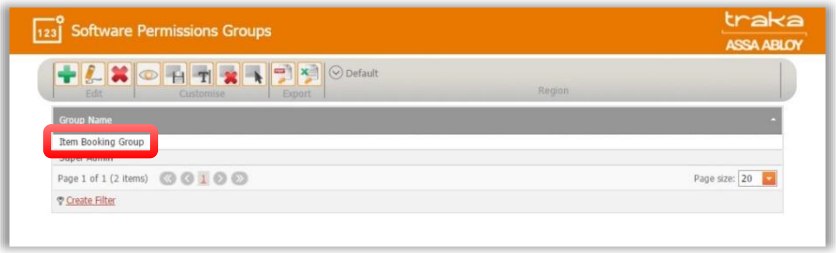
Restricted & Unrestricted Item Access

If unrestricted Item Access is unticked, the user will only be able to grant other users, items that the booking user also has access to.

This may be overridden by ticking the Unrestricted Software Item Access box in Software Permissions Groups.

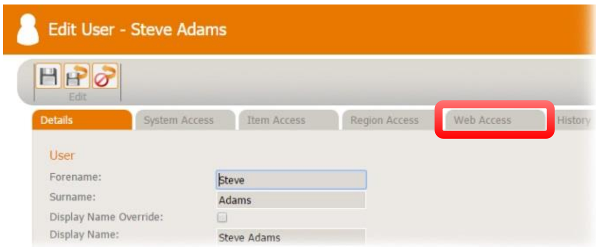


5. Once you have finished making your selection, click **Save and Return**. The newly created Permissions group will be shown.

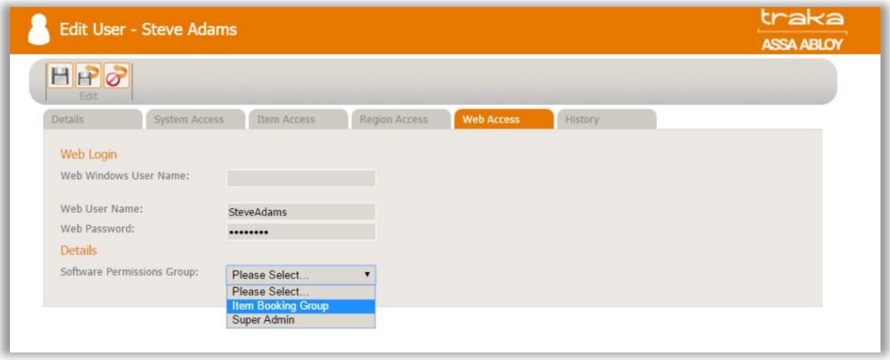


You will now be able to allocate the Permissions Group to specific users.

6. Navigate to the **Edit User** page and then click on the **Web Access** tab.



7. At the next page, create the Web Login details for the user and select the Software Permissions Group from the drop-down menu.



When the user logs into TrakaWEB, they will then be able to create and amend their own Item Booking but will not have access or the ability to edit any other features.

NOTE: If you wish to delete a Software Permissions Group, then you will need to deallocate it from any users first.

6.7.16 ITEM BOOKING REPORTS

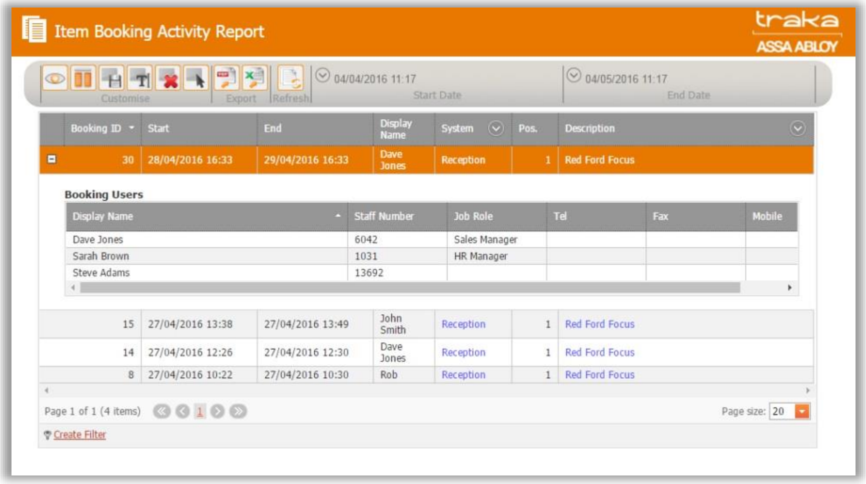
Whilst the Booking Summary page will show all active and future bookings, a separate audit trail will be made available in the reports section of TrakaWEB. There are two types of Booking report available: Item Booking Activity Report and Item Booking Exception Report.

6.7.16.1 ITEM BOOKING ACTIVITY REPORT

1. Click on 'Reports' on the Navigation Toolbar, then locate the 'Item Booking Activity Report' under the 'Utilisation' drop-down menu.

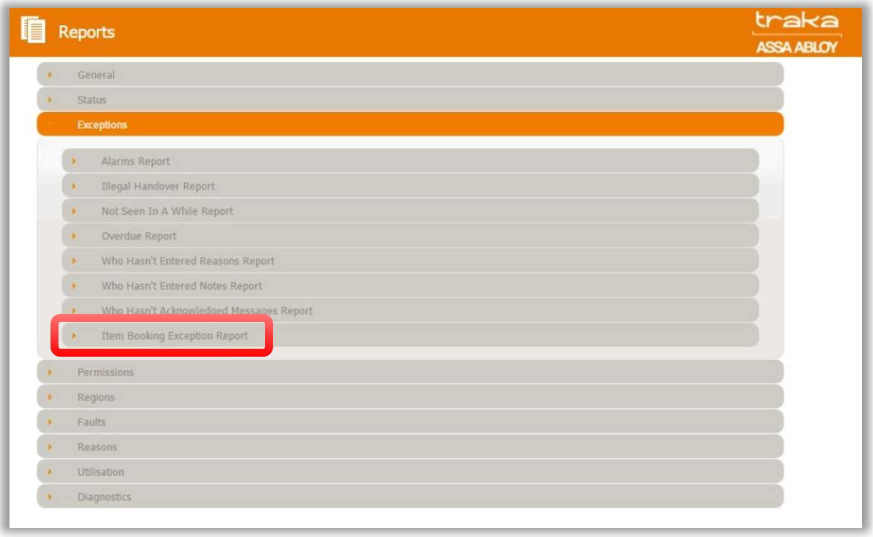
2. Click on 'View This Report'

You will now be taken to the 'Item Booking Activity Report'.

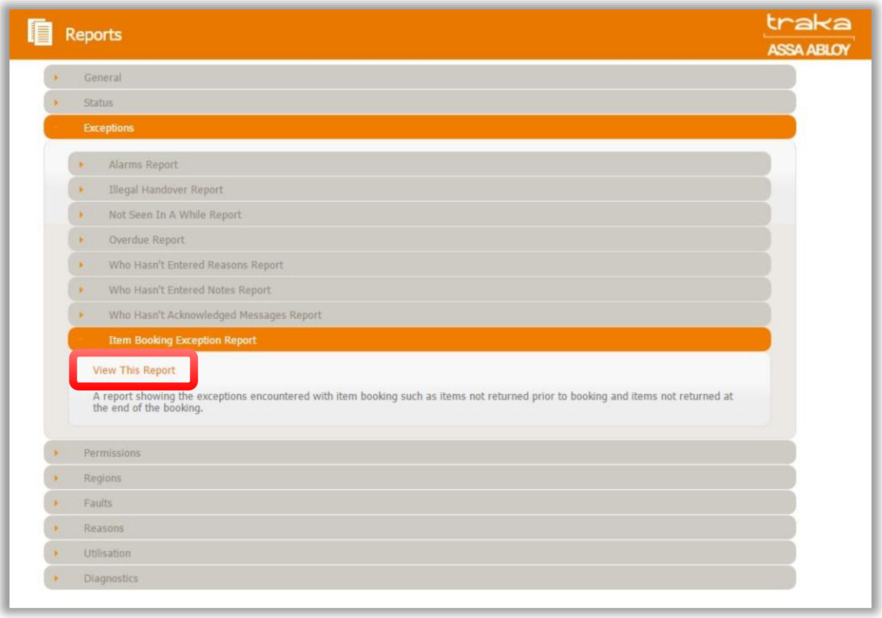


6.7.16.2 ITEM BOOKING EXCEPTION REPORT

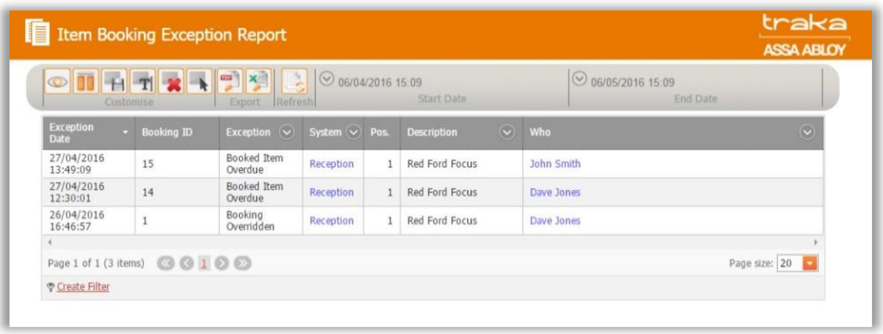
1. Click on ‘Reports’ on the Navigation Toolbar, then locate the ‘Item Booking Exception Report’ under the ‘Exceptions’ drop-down menu.



2. Click on ‘View this Report’.

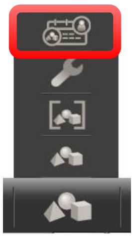


You will now be taken to the ‘Item Booking Exception Report’.

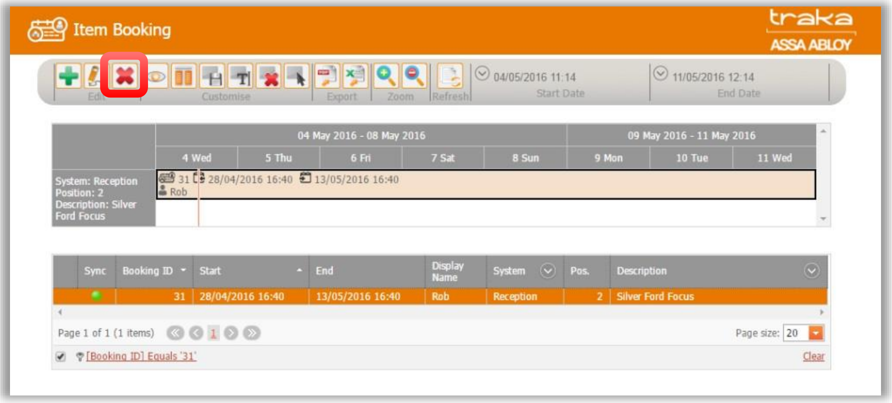


6.7.17 DELETING ITEM BOOKING

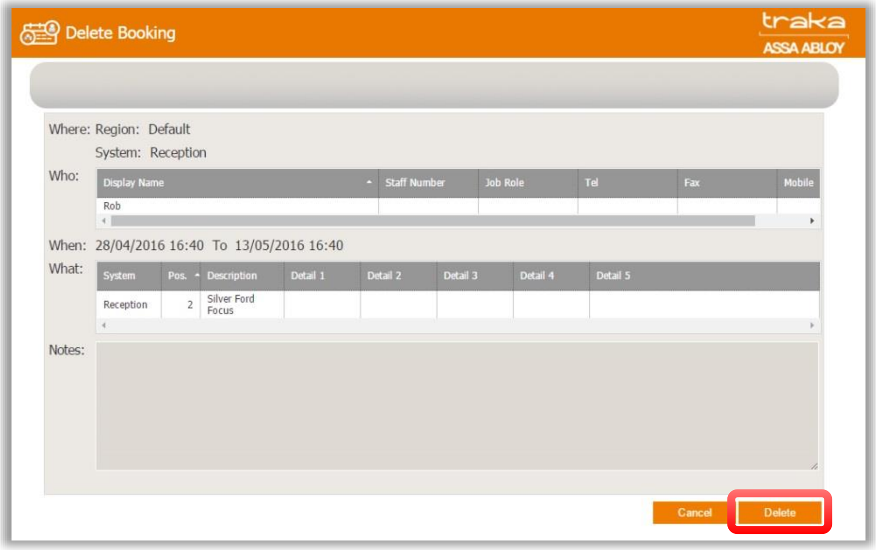
1. Select Item Booking from the Navigation Toolbar.



2. At the Item Booking landing page, select the booking you wish to delete, and then click the 'Delete' button.



3. You will be directed to the 'Delete Booking' page. Click on the Delete button at the bottom of the page.



6.8 FUEL, DISTANCE & LOCATION LOGGING

Fuel, Distance & Location Logging are individual cost options which can be used to assist fleet managers with day-to-day management of their vehicles. Each feature can be used independently or in combination. They can be purchased individually and also be turned on or off as required.

Users with access to the system will be granted a key to a vehicle, then after returning the key to the system, they will be requested to enter information regarding the fuel usage, the distance travelled, or time duration of journey, and the vehicle's current location. The next user to remove that key will be shown information as to the current location of the vehicle.

6.8.1 FUEL, DISTANCE & LOCATION LOGGING OVERVIEW

Fuel Level logging allows the end user to record a fuel level against an item when it is returned. This could be the fuel level of a vehicle or the battery charge level of a device.

Distance logging allows the end user to record a cumulative distance value against an item when it is returned. The distance units will be configurable by item type and will include miles, kilometres and hours.

Location logging allows the end user to record the current location of a vehicle.

When a user returns an item, Traka Touch will prompt the user to enter current information via the on-screen alphanumeric keyboard.

The current fuel, distance and location will be shown in the System Viewer of TrakaWEB and the search screen of Traka Touch.

A current report will be available in TrakaWEB listing for all the items with the feature enabled.

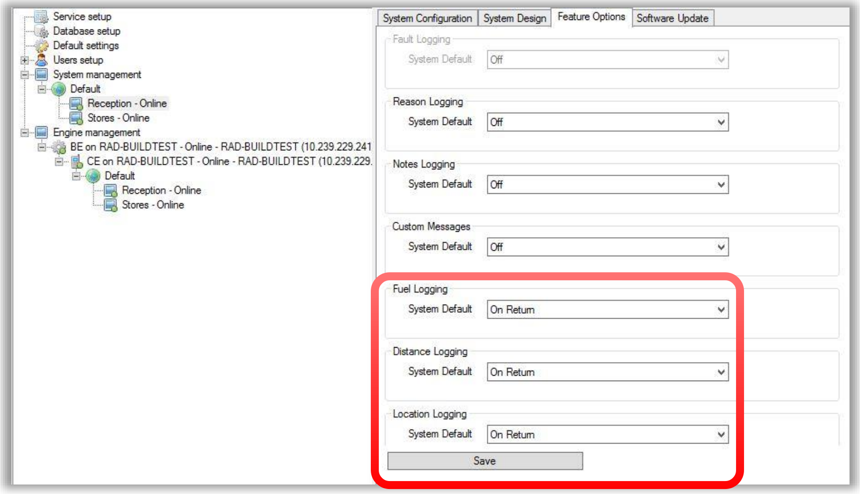
An exception report will be available to list users who have returned items but not provided the requested information at the Traka Touch System.

6.8.1.1 ENABLING THE OPTION

The Fuel, Distance & Location Logging features require a system configuration before they can be enabled. Contact Traka or your Distributor for further details.

The features can be enabled through two different methods before they are usable in TrakaWEB.

1. To enable the options within the Admin Application, a user will need to set them to 'On Return'. An administrator who has the appropriate access to the Admin Application will need to select the desired system and navigate to the Feature Options tab. Once selection has been completed, Click 'Save'.

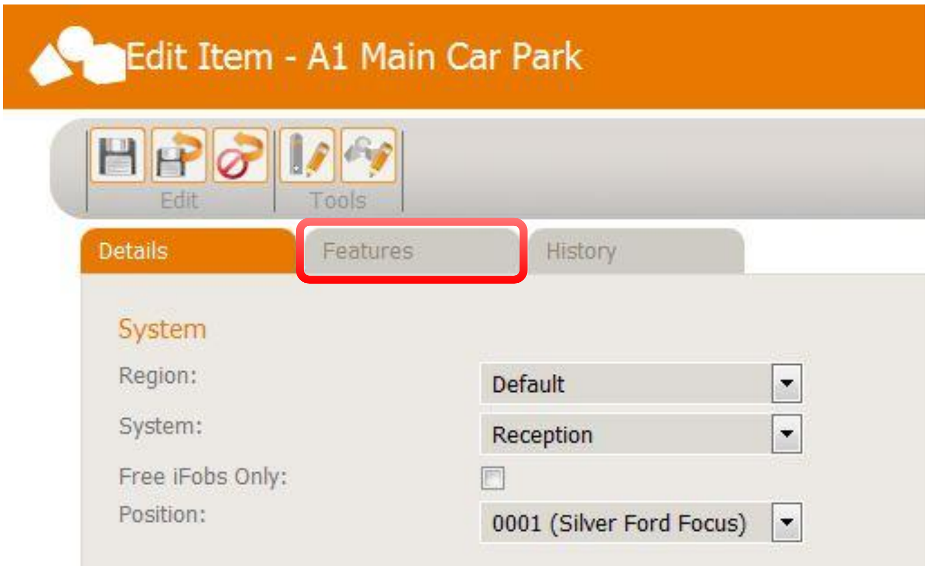


NOTE: Enabling the features in TrakaWEB Admin will set all items in the system to have the feature active.

Alternatively, each feature can be activated within TrakaWEB through the 'Features' tab.

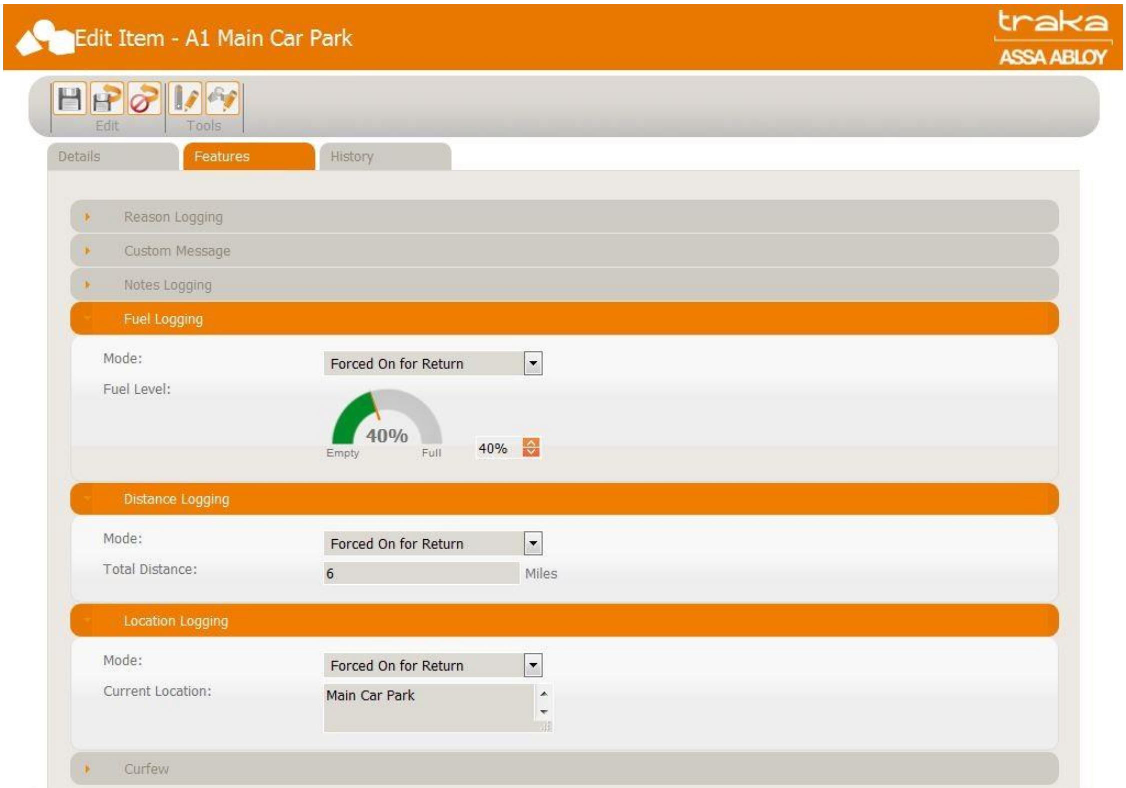
2. From the 'System Viewer', select 'Edit Item'.

3. At the next window, select the 'Features' tab.



Within the 'Features' tab you will see a list of all the Feature Options that are available.

4. Selecting the 'Fuel Logging', 'Distance Logging' and 'Location Logging' panels will enable you to change the 3 features to 'Forced On for Return'. Once the required features have been selected, click 'Save and Return'.



Note: If you choose to enable the features through TrakaWEB, they will only be available on the current selected item. Depending on how many items you wish to have the particular features enabled upon, it may be more time efficient to enable them in TrakaWEB Admin and then disable them on any items you don't want them enabled upon in TrakaWEB. If however, you have many items and only wish the features to be enabled on a few, it will be more time efficient to enable them on those items in TrakaWEB.

6.8.1.2 CONFIGURING DISTANCE LOGGING

Fuel Logging and Location Logging do not require any further configuration once they are made active. A user with administration access can however select different options, which will affect the Distance Logging functionality.

1. Within Software Settings, click on the 'Item Types' icon.

2. The user will now be taken to the 'Item Types' page. After the required item has been selected, click on 'Edit'.

3. At the 'Edit Item Type' page, click on the 'Features' tab as shown.

4. Clicking on the 'Logging Mode' drop down menu will provide two options; 'Total Distance' and 'Trip Distance'.

5. Clicking on the 'Units' drop down menu will provide three options: 'Miles', 'Kilometres' and 'Hours'.

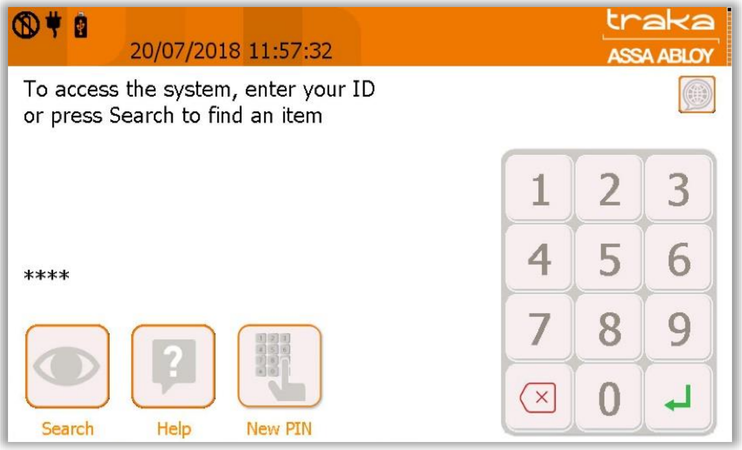
6. Once a selection has been made, click on 'Save and Return'.

NOTE: If a user changes the units at any time, the previous numeric value in the system will remain the same but will display the current set unit. For example, 8 hours will become 8 miles if the unit was changed from hours to miles.

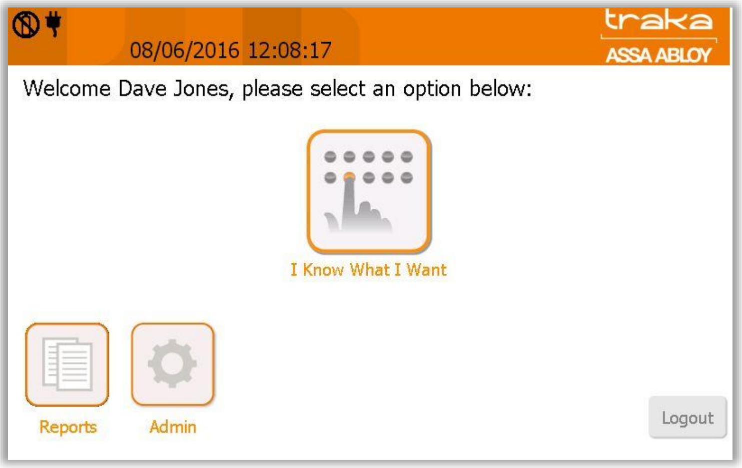
6.8.1.3 REMOVING AN ITEM

1. Click on the Traka Touch screen to activate the system.

2. Access the system using a keypad ID, Swipe Card or Finger Print.

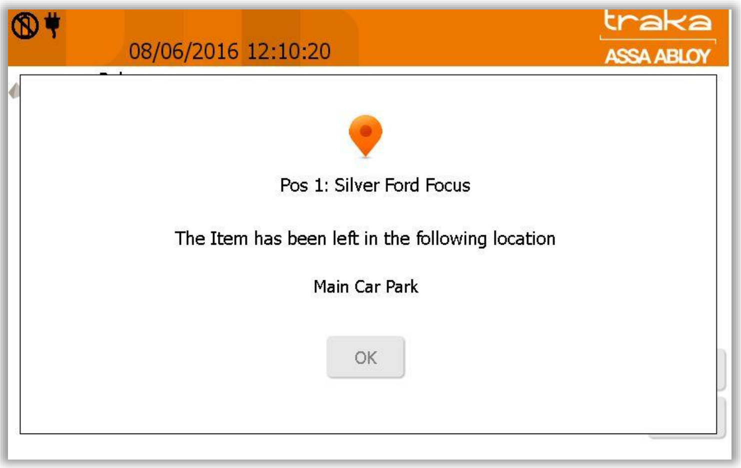


3. Depending on what level of access a user has been granted, click on 'I Know What I Want'.



Once the door has opened, a user will be able to select an item. A screen will then be shown displaying the details of the item's last known location.

4. Click on 'OK' and the item will be released.

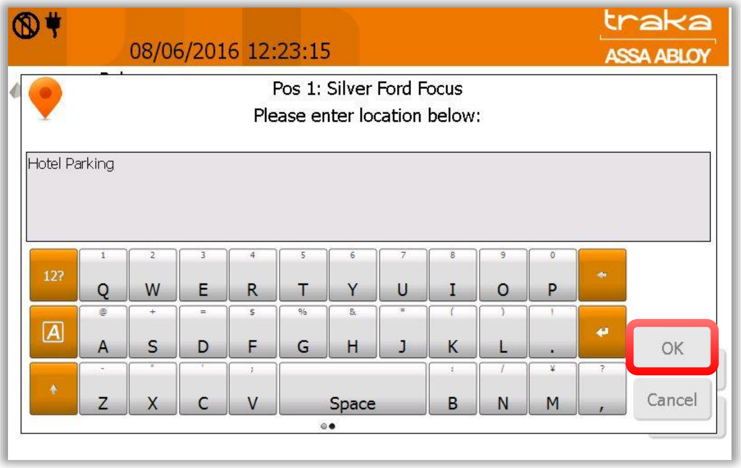


6.8.1.4 RETURNING AN ITEM

When users return items to the system, they will be prompted to enter specific details including its location, fuel or charge status and distance or time duration of travel.

NOTE: Closing the door will prevent a user from entering the requested information. This will generate an 'Exceptions' report in TrakaWEB.

1. If the Location feature has been enabled, after logging into the system and returning the item, the user will be presented with the following screen requesting the items current location. Once the location has been entered, click 'OK'.



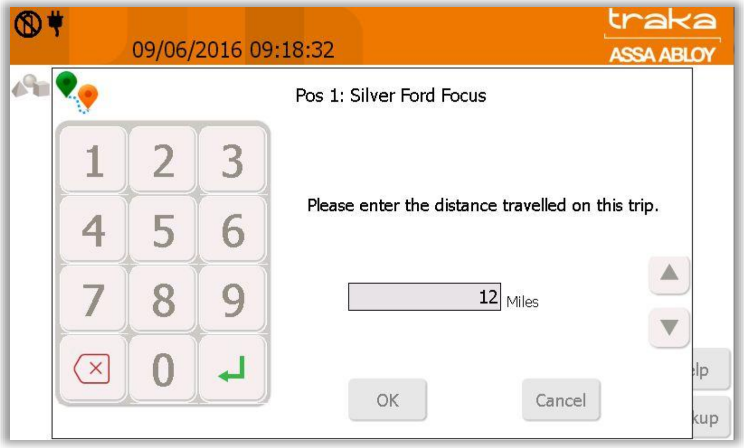
2. If the Fuel feature has been enabled, then at the next screen the user will be required to enter the current fuel/charge level. This is shown as a dial on the screen which can be simply rotated clockwise or anticlockwise using a finger or by using the up and down arrows.

NOTE: For locker based systems, this screen will be used to log the current charge remaining in an item such as a laptop or an iPad.

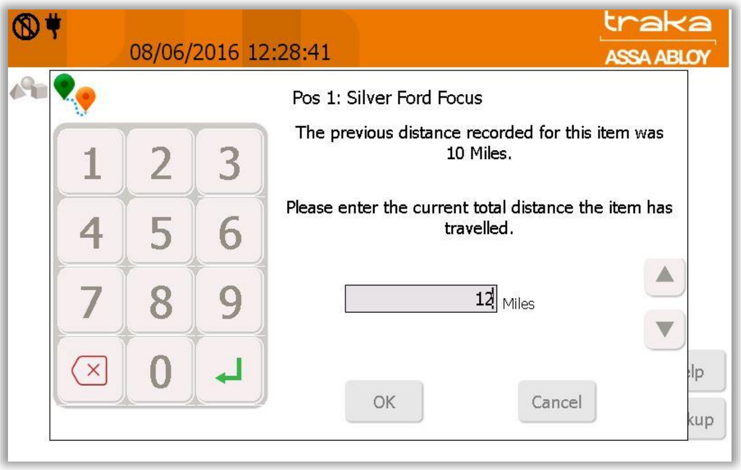
3. Once the fuel/charge level has been set, click 'OK' to continue.

If the Distance feature has been enabled, the next screen will request a user to enter either the 'Trip Distance' or the 'Total Distance'.

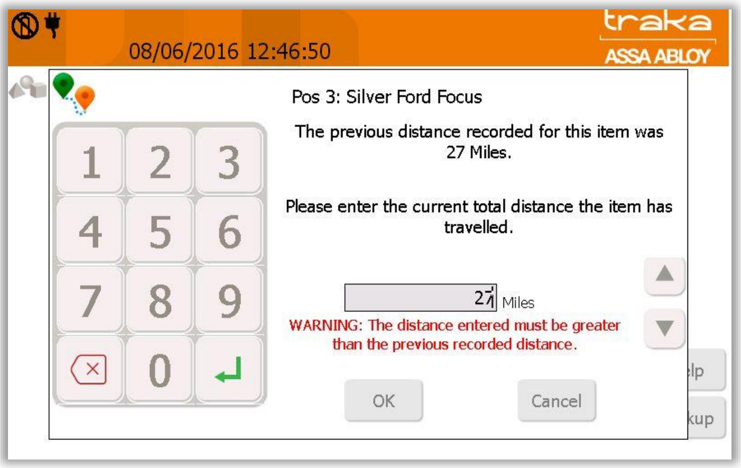
If the logging mode selected was for 'Trip Distance', the user will be required to enter the distance travelled on that trip.



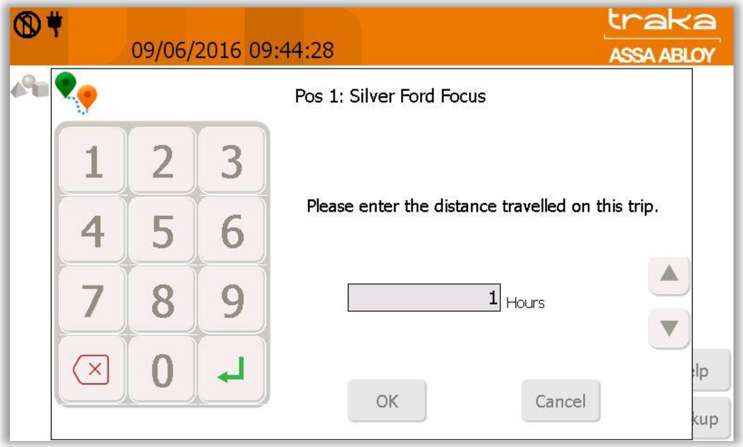
If the logging mode selected was for 'Total Distance', the user will enter the total current distance travelled against the previous distance.



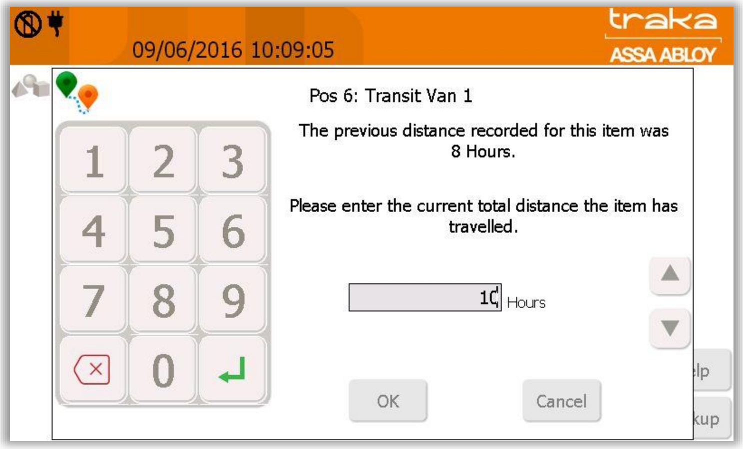
NOTE: If the user enters a current total distance that is less than the previous distance, the system will display a warning. The distance will automatically be set to the same value as the previous logged distance unless a correct value is entered.



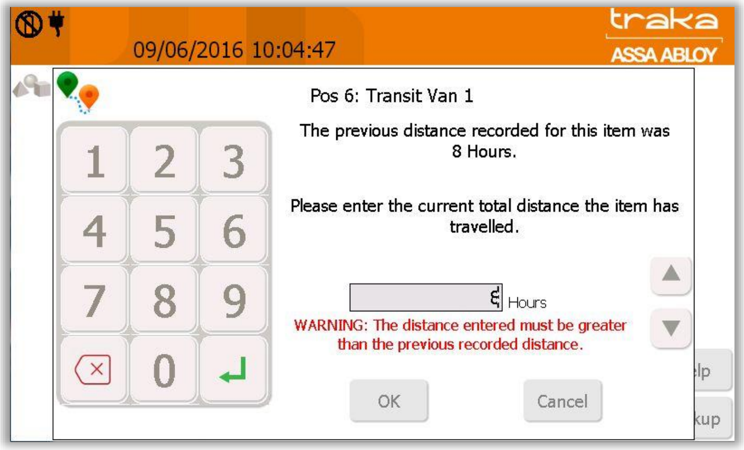
If the units were set to hours, and the logging mode was set to 'Trip Distance' the user will enter the distance travelled in hours.



If the units were set to hours and the logging mode was set to 'Total Distance', the user will enter the total distance travelled in hours against the previous time duration.



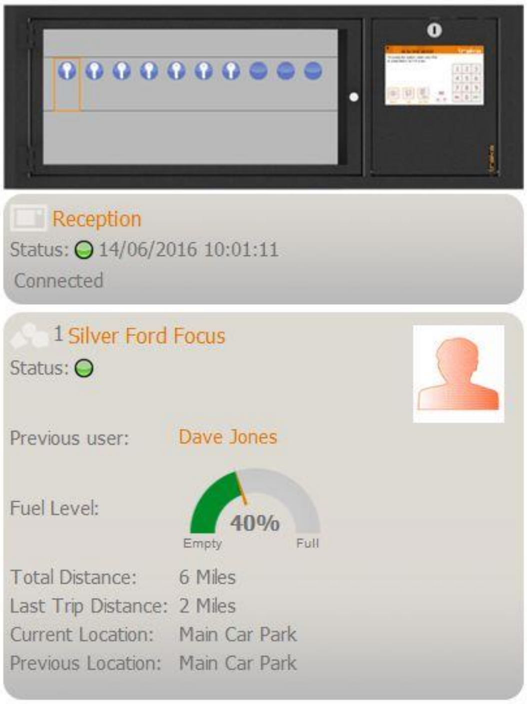
NOTE: If the user enters a current total time duration that is less than the previous time duration, the system will display a warning. The hours will automatically be set to the same value as the previous hours unless the correct value is entered.



6.8.1.5 VIEWING CURRENT FUEL, DISTANCE & LOCATION LOGGING

The system viewer screen will display the basic details of the current selected item in the system.

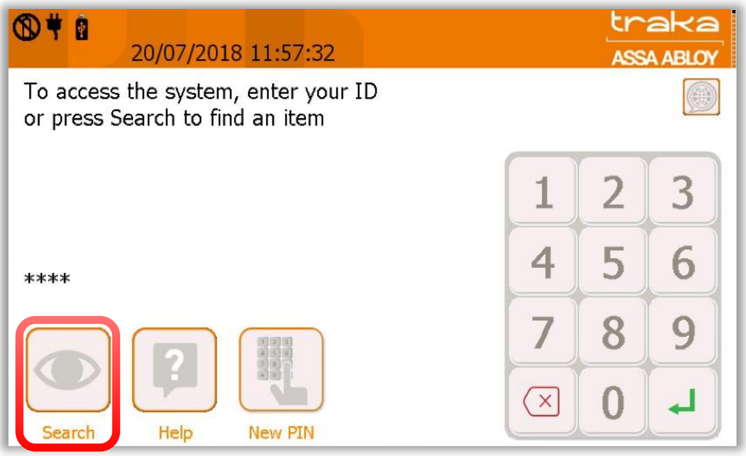
Depending on what features have been enabled, a user can see the current fuel level, the total distance and last trip distance, depending on which features were enabled. The user can also see both the current and previous location of the item as well as the previous user who took the item.



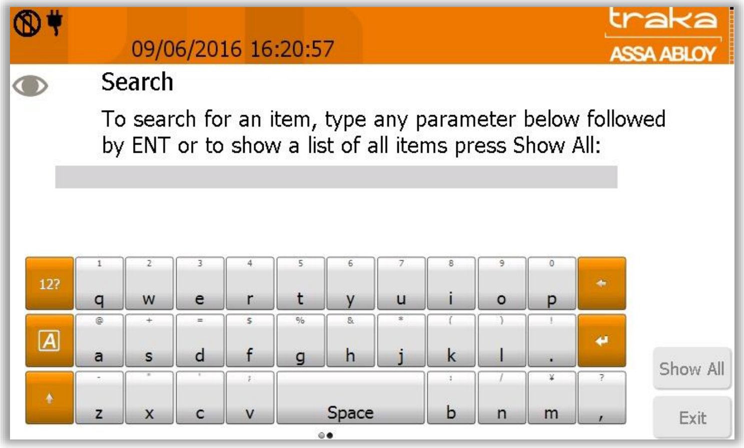
Users can also view the current Fuel, Distance and Location through the search screen on Traka Touch.

NOTE: Depending on how the Traka Touch system has been configured, the Search option maybe located under 'Reports'. See UD0011 – Traka Touch User Guide for further details.

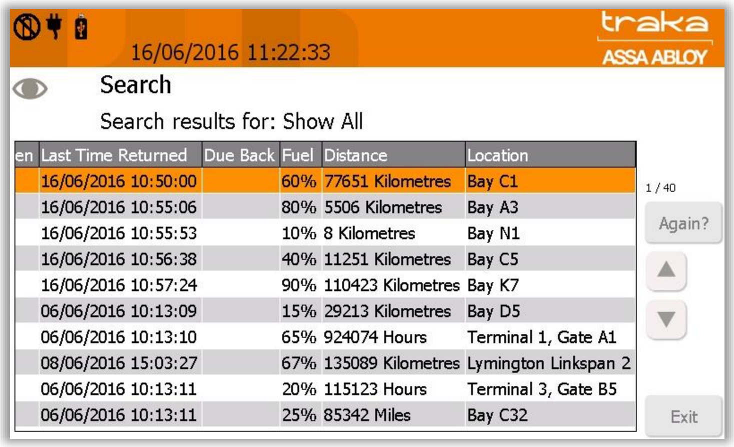
1. Click the 'Search' button on the Traka Touch screen.



At the Search screen a user can use the alphanumeric keypad to input the name of a specific item followed by the  Enter key, or simply click on Show All.



Depending on what features have been enabled, the next screen will display the search results. Scroll to the right to see the current Fuel, Distance and Location for the particular item/s.



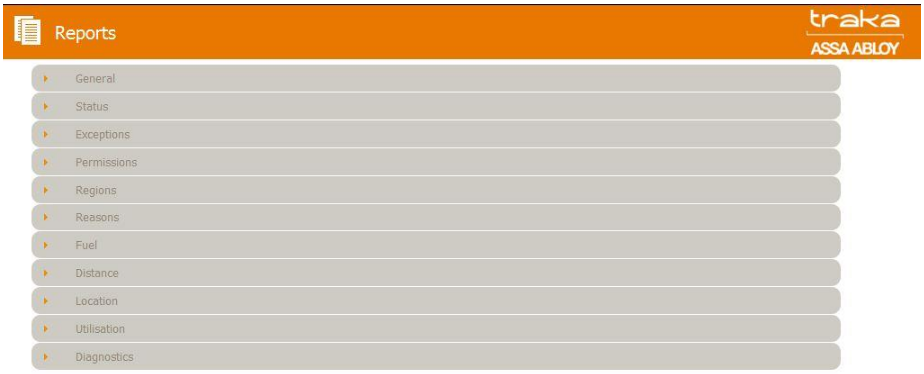
6.8.2 REPORTS

For any Fuel, Distance and Location logging activities, an audit trail will be made available in the reports section of TrakaWEB. Separate reports can be viewed for Fuel, Distance and Location. There also exists an ‘Exceptions’ report.

Each report can be exported as a PDF or Microsoft Excel file.

1. Click on the ‘Reports’ icon on the Navigation Toolbar.

The Reports screen will now be displayed as shown below.

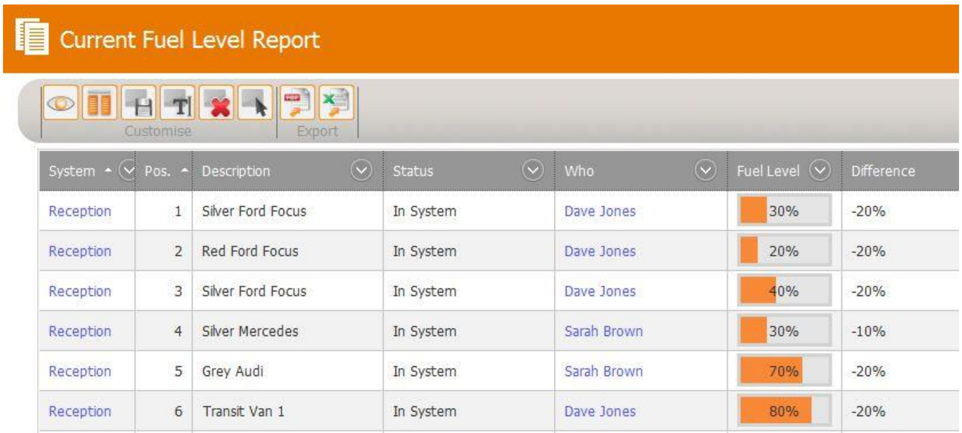


NOTE: Only the features that have been enabled will be displayed in the reports screen.

6.8.2.1 FUEL REPORT

1. To view the Fuel report, click on the Fuel panel and then click on **View This Report**.

The Fuel Level Report will now be displayed as shown below.

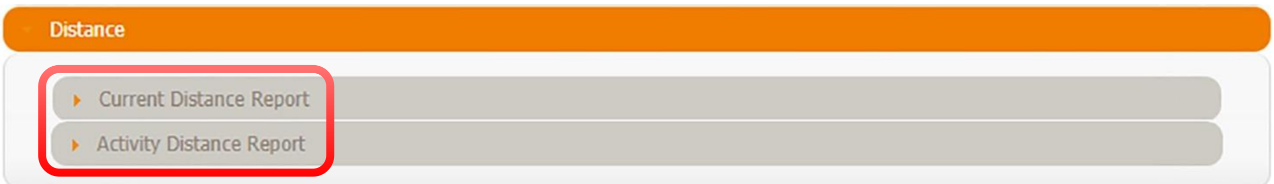


System	Pos.	Description	Status	Who	Fuel Level	Difference
Reception	1	Silver Ford Focus	In System	Dave Jones	30%	-20%
Reception	2	Red Ford Focus	In System	Dave Jones	20%	-20%
Reception	3	Silver Ford Focus	In System	Dave Jones	40%	-20%
Reception	4	Silver Mercedes	In System	Sarah Brown	30%	-10%
Reception	5	Grey Audi	In System	Sarah Brown	70%	-20%
Reception	6	Transit Van 1	In System	Dave Jones	80%	-20%

6.8.2.2 DISTANCE REPORTS

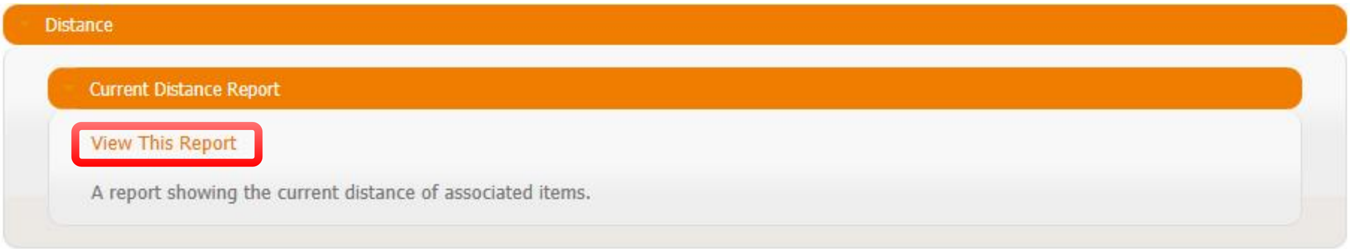
1. To view the Distance reports, click on the Distance panel.

You will notice that there are two reports to choose from; **Current Distance Report** and **Activity Distance Report.**

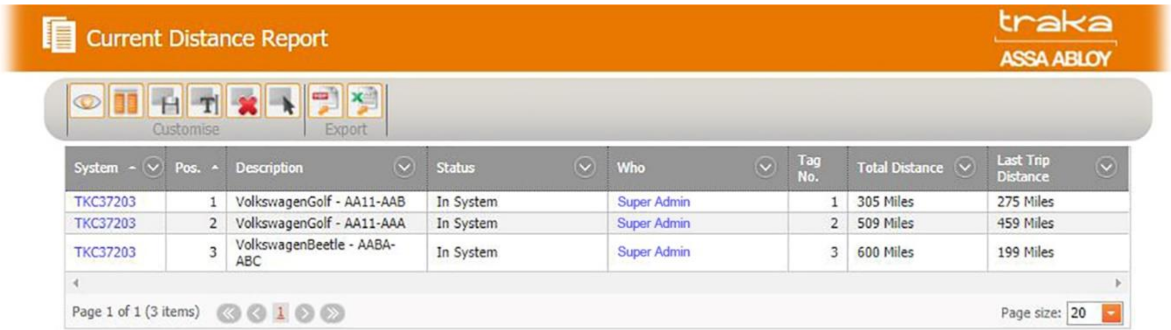


Current Distance Report

1. To view the **Current Distance Report**, click on the panel and select **View This Report.**

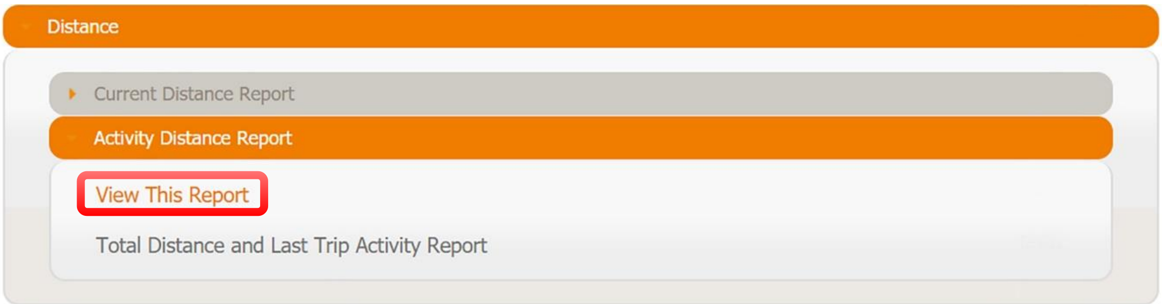


The Current Distance Report will now be displayed as shown below.

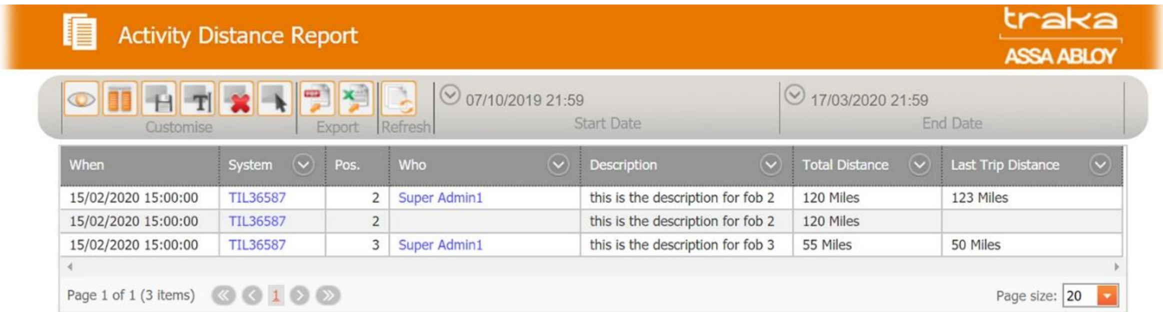


Activity Distance Report

1. To view the **Activity Distance Report**, click on the panel and select **View This Report.**



The current Activity Distance Report will now be displayed as shown below.



6.8.2.3 LOCATION REPORT

1. To view the Location report, click on the 'Location' panel and then click on 'View This Report'.

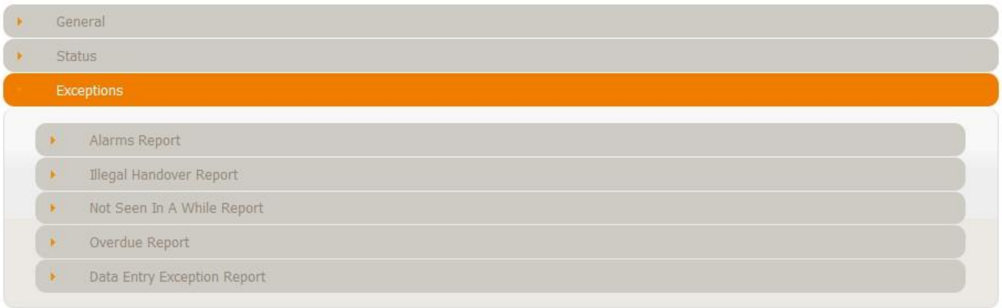
The Current Location Report will be displayed as shown below.

System	Pos.	Description	Status	Who	Current Location	Previous Location
Reception	1	Silver Ford Focus	In System	Dave Jones	Hotel Parking	Main Parking
Reception	2	Red Ford Focus	In System	Dave Jones	Main Car Park	Airport Parking
Reception	3	Silver Ford Focus	In System	Dave Jones	Main Car Park	Hotel Parking
Reception	4	Silver Mercedes	In System	Sarah Brown	Main Car Park	Train Station
Reception	5	Grey Audi	In System	Sarah Brown	Main Car Park	Main Site
Reception	6	Transit Van 1	In System	Dave Jones	Main site	Main Site

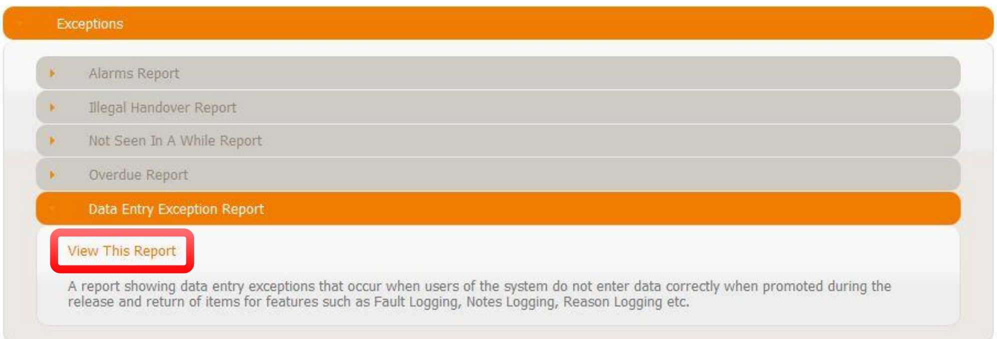
6.8.2.4 EXCEPTIONS REPORT

If a user closes the door upon returning an item and fails to log any details into the system, an 'Exceptions' report will be created. This, like the other reports, can be viewed in TrakaWEB.

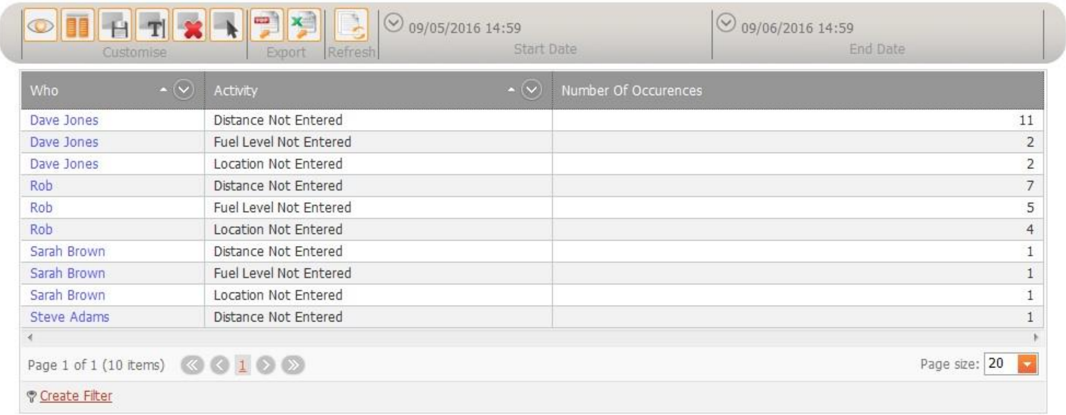
1. To view the Exceptions Report, click on the 'Exceptions' panel.



2. Now click on the Data Entry Exception Report and then click on 'View This Report'.



The Exceptions report will now be displayed as shown below.



Who	Activity	Number Of Occurences
Dave Jones	Distance Not Entered	11
Dave Jones	Fuel Level Not Entered	2
Dave Jones	Location Not Entered	2
Rob	Distance Not Entered	7
Rob	Fuel Level Not Entered	5
Rob	Location Not Entered	4
Sarah Brown	Distance Not Entered	1
Sarah Brown	Fuel Level Not Entered	1
Sarah Brown	Location Not Entered	1
Steve Adams	Distance Not Entered	1

Page 1 of 1 (10 items) Page size: 20

Create Filter

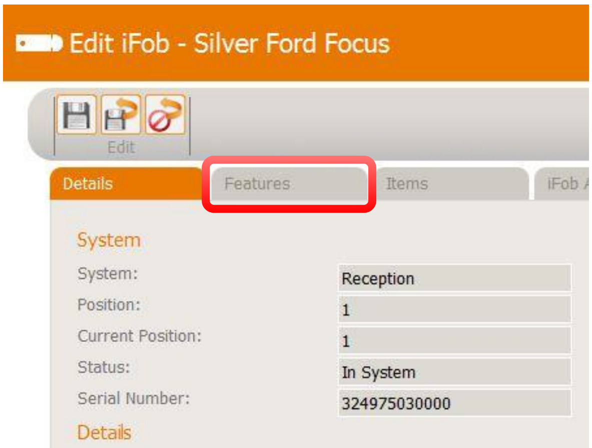
6.8.3 OVERRIDING LOGGING IN TRAKAWEB

Occasionally, it may be necessary for an administrator to override an incorrect logging or change the current values of a logging if, for example, a vehicle has been replaced.

NOTE: It is possible to combine the keys of a new vehicle with the same iFob as the vehicle that is being replaced. The logging history will however remain with the iFob, but the current details can be reset to suit the Fuel, Distance and Location of the new vehicle.

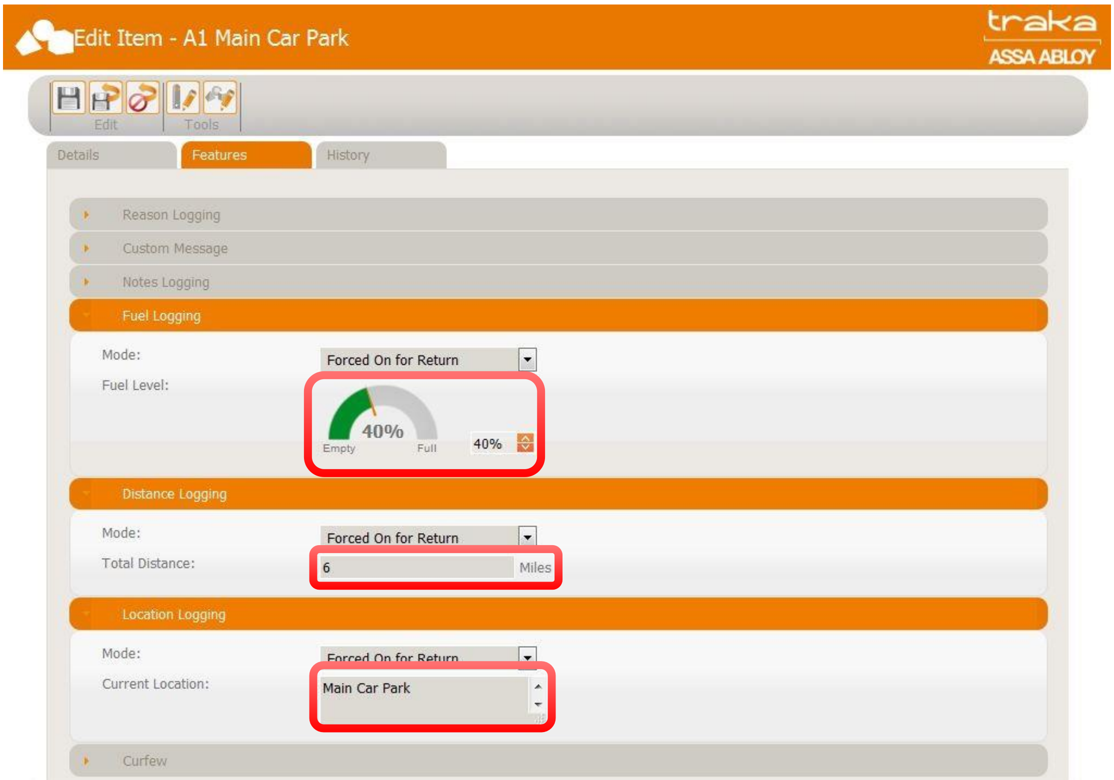
1. In the System Viewer, select the item that requires editing then click on 'Edit iFob'.

2. At the 'Edit iFob' screen, click on the Features tab.



3. Depending on which features have been enabled, at the 'Features' screen, a user can edit the values for the Fuel, Distance and Location to suit the new vehicle.

NOTE: The Fuel Level can only be adjusted using the up and down arrows.



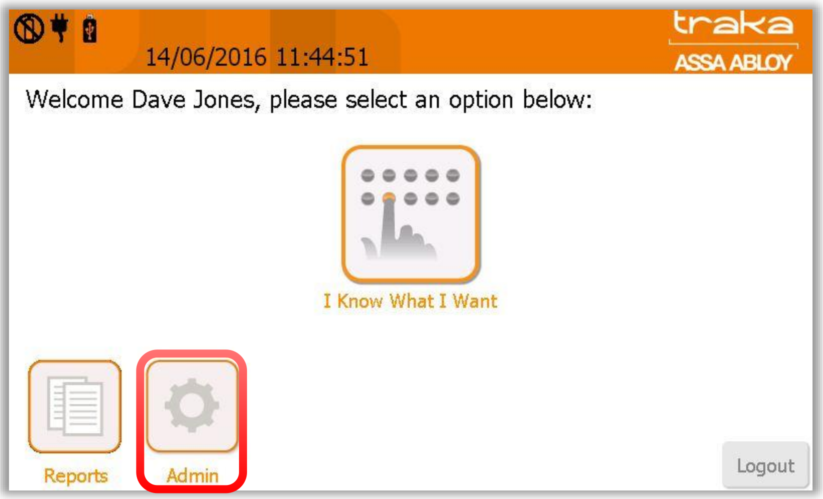
4. Once completed, click 'Save and Return'.

NOTE: When an override change is made in this way through TrakaWEB, the name of the user who made the change will not be visible in the System Viewer report. This is because it is not currently possible for TrakaWEB to know which user made the edit. Whereas Traka Touch can determine users by their login details.

6.8.4 OVERRIDING LOGGING AT TRAKA TOUCH

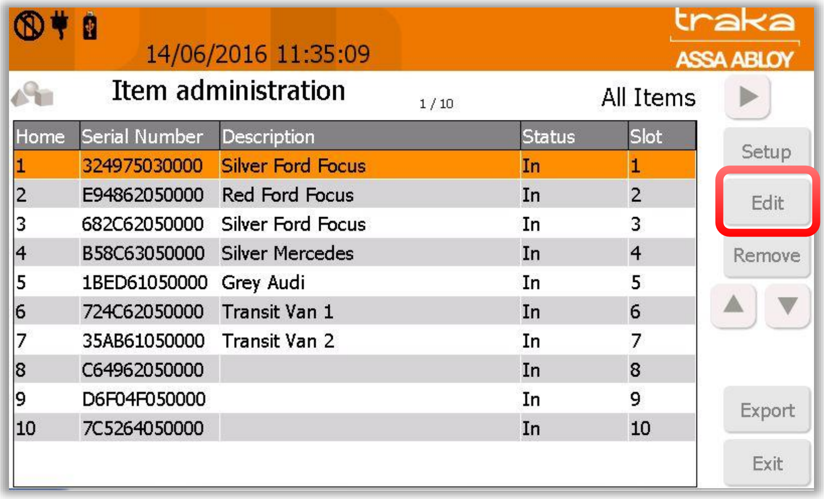
It is possible to override the fuel, distance and location values within the 'Item Administration' screen in Traka Touch.

1. After logging in to the Traka Touch system, click on 'Admin'.

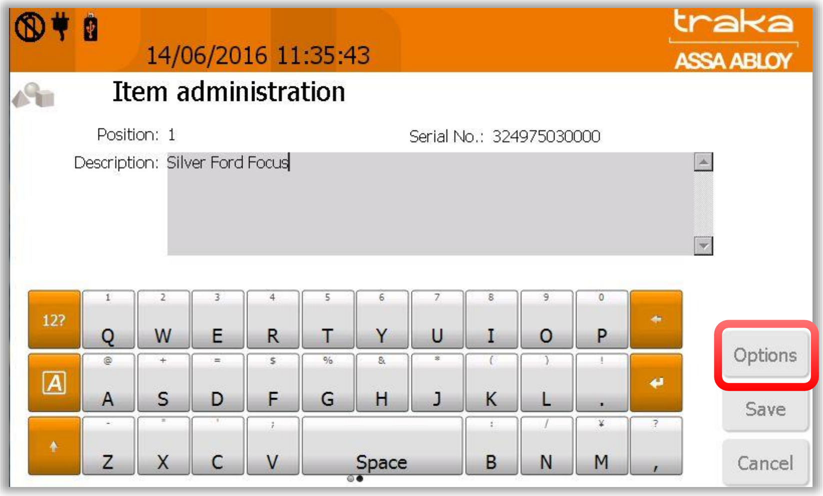


2. Now click on the 'Items' button.

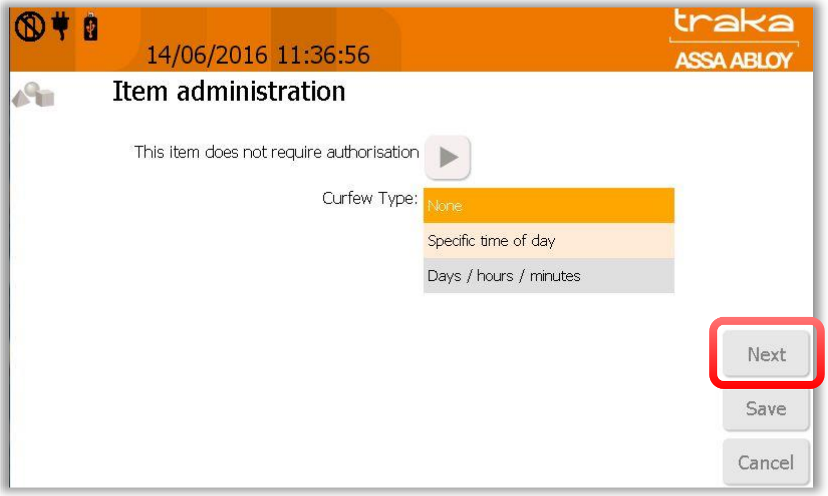
3. At the next screen, select the item for editing and then click on the 'Edit' button.



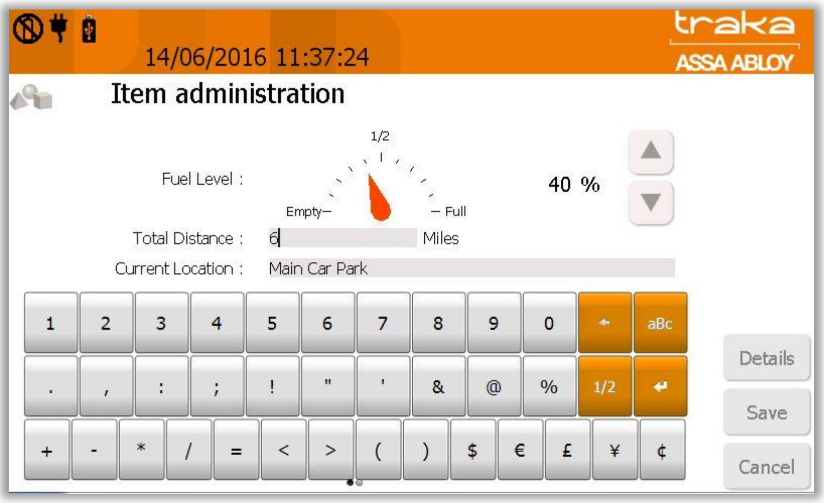
4. At the 'Item Administration' screen, click on 'Options'.



5. At the next screen, click on the 'Next' button.



6. Depending on which features have been enabled, the next screen will allow a user with administration access to change the fuel, distance and location values by rotating the fuel level dial and manually entering values using the alphanumeric keypad.



6.9 ITEM HANDOVER

6.9.1.1 ITEM HANDOVER

Item Handover is a cost option that allows a user who has access to the system to 'handover' an item to a user who is in the database but does not have access to the system. This feature is beneficial for customers who may want certain higher ranking members of staff to issue keys or assets to others staff members throughout the business, but don't want the secondary staff member to have access to the system.

Enabling the Option

Item Handover will need to be enabled in the system configuration file before it is usable in TrakaWEB and at the Traka Touch. To have it enabled within the configuration you will need to contact Traka or your distributor for further details.

Types of Users

To be an Authoriser, Recipient or both, an option will need to be enabled in the users' details.

Handover Authoriser - A user with authorisation to hand an item over to another user is known as a 'handover authoriser'. This is a user that has access to the system and the item they wish to 'handover'.

Handover Recipient - A user who does not have access to the system but exists in the TrakaWEB database. When these users are created they do not need Keypad ID's, Card ID's PIN's etc.

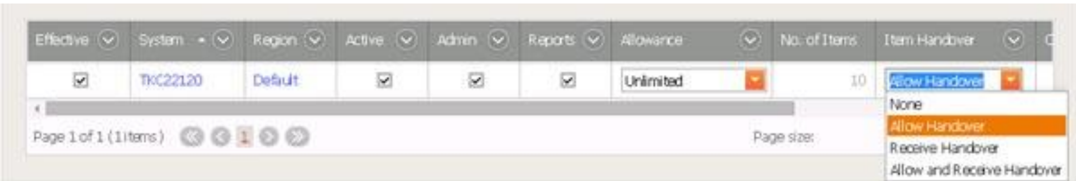
Handover Authoriser & Recipient - A user with authorisation to hand an item over to another user and receive an item handed to them. This is a user that has access to the system and the item they wish to 'handover'.

Setting up the Users

If you need to add new users to your database please refer to the Adding Users section.

1. From the navigation toolbar at the bottom of TrakaWEB, select the Users Button.
2. Highlight the desired User. If you need to add a new user, click the Add button.
3. Select the Edit button or double click the user.
4. Navigate to the System Access tab.

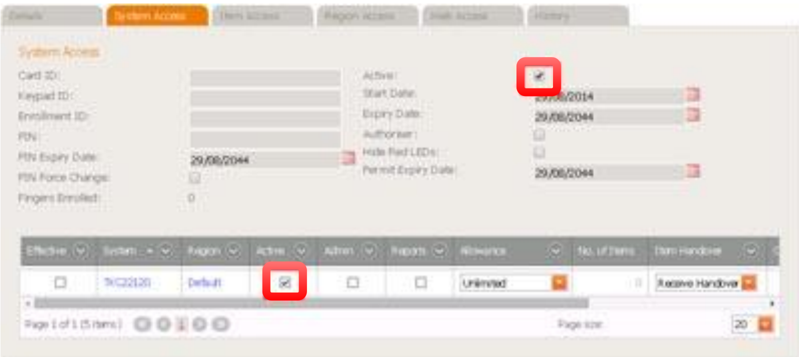
The grid displaying the users' system access will have a column called Item Handover. The drop down selection box consists of the following options.



- Allow Handover - User may legitimately hand items over to a user who is allowed to receive a handover (handover recipient). At the point of item removal, the user will be prompted to define who the item is to be handed over to, if anyone (handover authoriser).
- Receive Handover - User is allowed to receive items which were removed from a system by a user who was authorised to handover those items (handover recipient).
- Allow & Receive Handover - Allows a user to both handover items to a recipient and receive items from an authoriser.

NOTE: Only when Item Handover is enabled in the configuration file will the column be visible in the user grid.

5. For handover recipients, you will need to tick the active tick box at the top of the system access page and in the system line as well.



6. After making your selection, click the Save & Return button.

7. You will need to repeat this process for any users that need to be handover authorisers/recipients.

Traka Touch

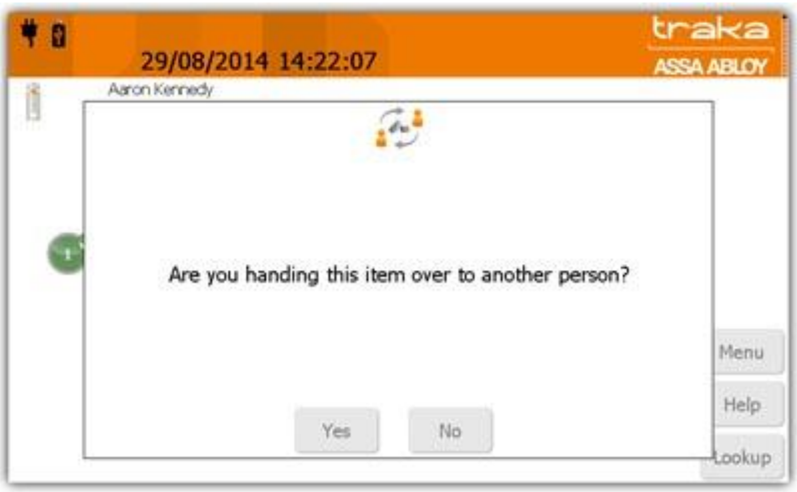
NOTE: It is not possible to assign user authoriser/recipient roles at the Traka Touch system. This must be done in the user details in TrakaWEB.

1. A user with handover authorisation identifies themselves to the system and accesses the item selection screen.

2. The user will need to select an item to hand over.

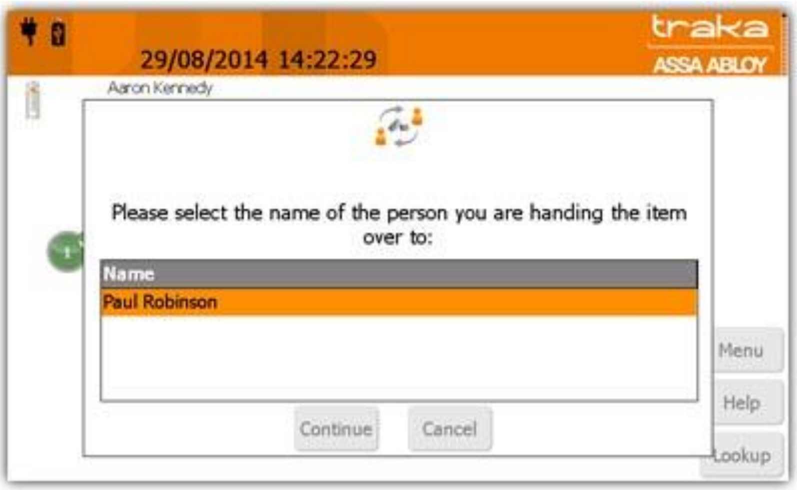
3. The system will ask the user if they are handing the item over to another user.

   a) Yes - If selected, the process will continue, please see step 4.
   b) No - If selected, the message will disappear allowing the item to be removed (providing the user has access).



4. Once they have selected yes, the system will display a list of users that are eligible to have the item handed over to them.

NOTE: This list will be populated by users that have the 'Allow Handover' option enabled in their system access details.

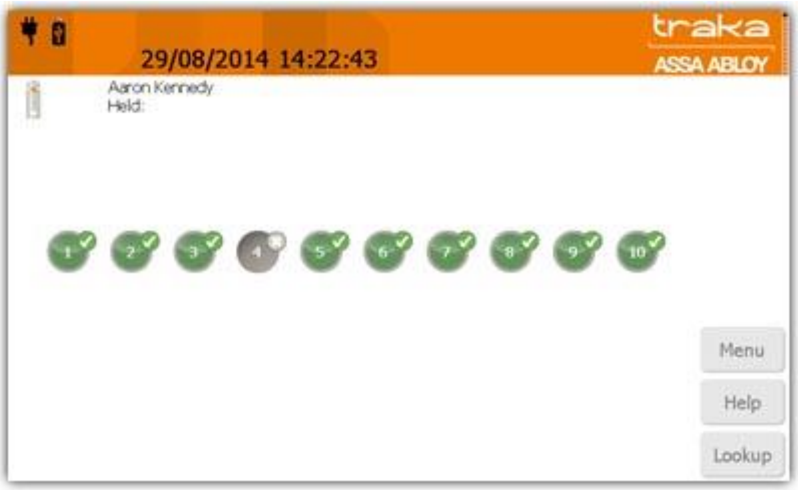


5. Select the desired user and click Continue.

NOTE: Clicking Cancel will take the user back to the item selection screen.

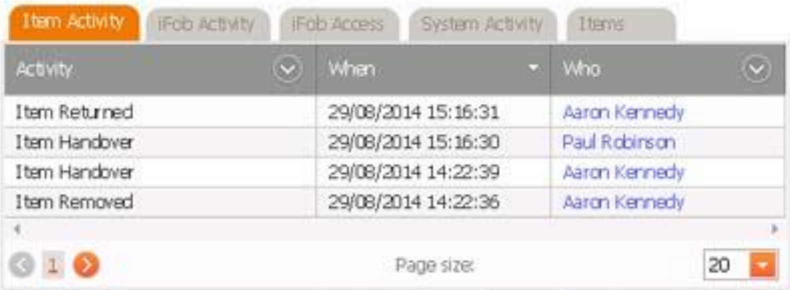
6. The item will then be released from the system.

7. The symbol for the removed item shows that it is out to another user, indicating that the handover was successful.



Activities

The system viewer displays a grid that holds the last 30 days of activities for the selected iFob/item in the system. When a user hands an item to another user an 'Item Handover' activity will be generated in the Item Activity tab. When the user returns the item, another Item Handover activity will be generated with the recipients.



Reports

You can run a report that shows items that were taken from the system and handed to another user through the Item Handover feature. Please refer to the Item Handover Report section.

6.10 RANDOM RETURN TO MULTIPLE SYSTEMS (RRMS)

6.10.1 RRMS & COMMON ITEM ACCESS GROUPS

The regions of ANY type of group affect who can 'see' and be added to that group (or will be automatically added in the case of an Everyone Group).

A normal Item Access Group can only contain items from the systems to which the group applies. So a 'Region A' Item Access Group can only contain items from 'Region A' systems.

For Common Item Access Groups, although the region still controls the visibility of the group in exactly the same way, the items it contains can only ever be RRMS items. RRMS items have no home system and no home position (they are essentially unallocated iFobs). As these items would never be limited to coming from a particular system, you can always add ANY unallocated item to a single Common Item Access Group.

NOTE: That once an item is added to a Common Item Access Group, it cannot be added to any subsequent groups.

Users may expect that items that are physically bound to a department or building would be filtered to the region that the systems are in but that is not the case. The allocation of RRMS items into Common Item Access Groups is essentially inferring the systems which that item can be placed into - hence the 'Common Group' term. If an item is placed into a system outside those regions, it will be unrecognised and only removable by an Administrator.

To summarise:

- An Item Access Group collects together similar iFobs/Items from one or more systems that can be granted to a number of users of those systems. Each item retains its individual access level
- A Common Item Access Group collects iFobs/Items together and gives them all the same access level across all the visible systems/regions in the group. This can then be applied to multiple users of those systems

6.10.2 RRMS OVERVIEW

Random Return to Multiple Systems (RRMS) is a cost option feature that allows Items to be taken from one key control system to another that are connected to the same TrakaWEB instance.

RRMS is available for Traka Touch key cabinets being managed with TrakaWEB Professional Plus. If enabled for a cabinet, RRMS applies to the entire cabinet. Access rights will be based on categories of fobs ("Access Groups") rather than individual fobs. RRMS cannot be used with any other optional Traka Touch or TrakaWEB functionality, or with the User Import Spreadsheet feature. Searches, Status enquiries and some Reports work very differently on systems with RRMS.

NOTE: It is not possible to grant a user direct access to a RRMS Item, this must be done via a Common Item Access Group.

Identifying Items in a RRMS deployment is slightly harder than a fixed return system due to the Item not having a fixed home, which in turn makes it harder to work out which key is which. In fixed return systems, plastic or metal tags would traditionally be used to identify the fixed system and position the Item should be returned to however, with RRMS an Item does not have a specific home and therefore a different approach is required. The Tag Number feature of TrakaWEB allows a unique numeric Tag Number to be recorded against each Item in TrakaWEB which would correspond to a plastic or metal Key Tag attached to the physical keys. This can be any number that makes sense to the end user and does not need to correlate to a system or position.

Reporting in TrakaWEB accounts for the fact that Items can travel from system to system and so extra columns may appear in reports where additional information needs to be presented to provide a complete picture of activity.

Due to the nature of RRMS, some functionality may be limited or not available compared to fixed return or random return to a single system deployment.

6.10.2.1 RRMS CONSIDERATIONS

Once the RRMS configuration has first been setup, only an admin user will be able to remove and return Items. A non-admin user will only be able to remove and return Items once the User and Items have been assigned to a Common Item Access Group.

6.10.2.2 LIMITATIONS

The following limitations currently apply to RRMS:

- RRMS will only function with TrakaWEB and is not available on standalone Traka Touch systems.
- RRMS cannot be used on standard or non-RFID lockers of any kind.

RRMS will not function with any of the following software options:

- User Import/Export Spreadsheet
- 16bit Systems
- 16bit Lockers
- Touch Lockers
- Rack Manager
- DockSafe
- Transfer Ownership
- Curfews
- Abloy Keyholder
- Item Booking
- Item Allowance
- Authorisers
- Item Handover Logging
- Duress Item Position
- Vault Pairing
- Illegal handover alarm event
- Touch Import Spreadsheets

The following Feature Options are not currently compatible with RRMS

- Access Schedules
- Fault Logging
- Reason Logging
- Notes Logging
- Distance Logging
- Fuel/Charge Level Logging
- Location Logging
- Custom Messages

6.10.3 TRAKA TOUCH

Much of the Traka Touch functionality will be reduced for Systems with RRMS Enabled. For more information, please refer to **UD0011 – Traka Touch User Guide.**

6.10.4 ENABLING THE OPTION

A configuration file will be required to enable RRMS, which can be obtained from Traka. To load the configuration file, please refer to **UD0011 – Traka Touch User Guide**.

IMPORTANT: Ensure that the Traka Touch system is not connected to TrakaWEB before enabling the RRMS configuration.

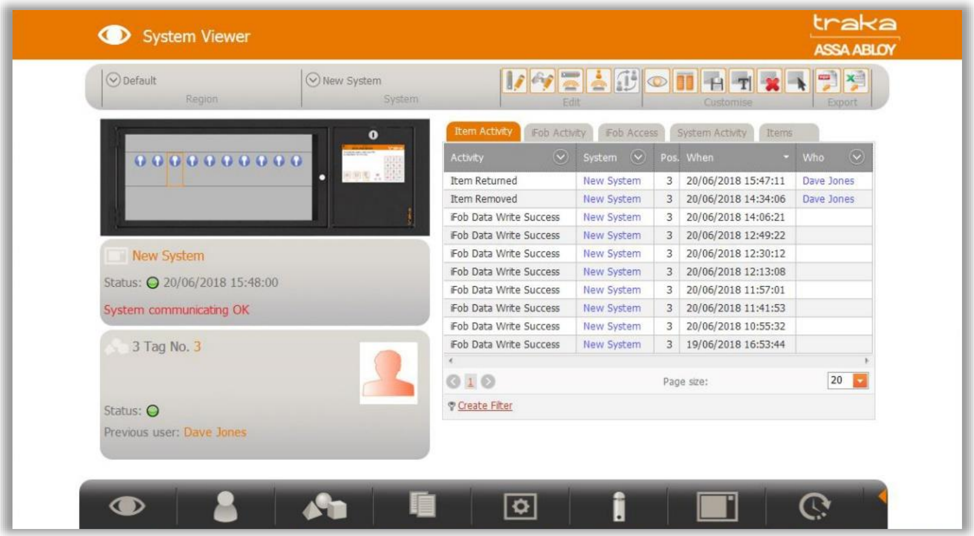
IMPORTANT: It is of critical importance that the installation of RRMS is done on a clean Traka Touch system. The configuration must be loaded when first prompted after the database has been reset. The system will then be converted from FRSS to RRMS. If this is not done, RRMS will not function correctly.

6.10.5 TRAKAWEB SYSTEM VIEWER

With RRMS enabled, the System Viewer will only show information about iFobs/Items that are currently in the systems.

NOTE: For positions that do not have an iFob present, no history will be displayed.

The Item Activity and iFob Activity grids both have a System and Position column added. This is so that a full history can be viewed for an iFob/Item as it travels from System to System over time.



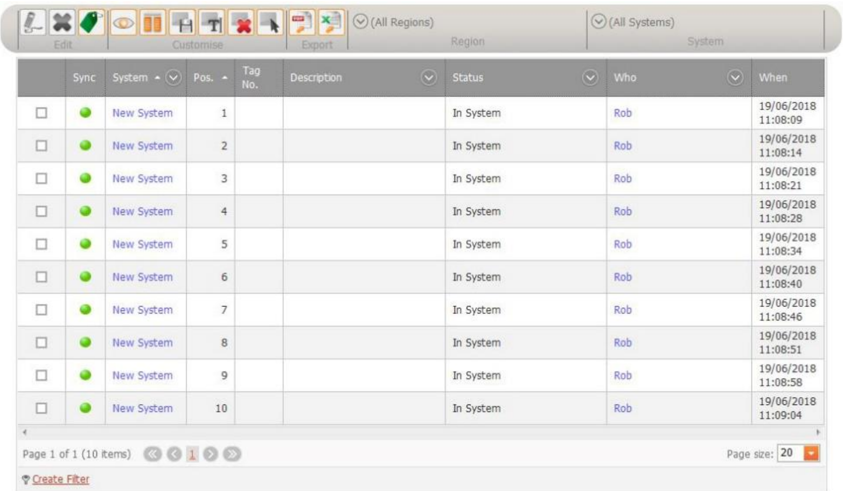
NOTE: The Transfer Ownership toolbar button is currently not available for RRMS systems.

6.10.6 ASSIGNING TAG NUMBERS

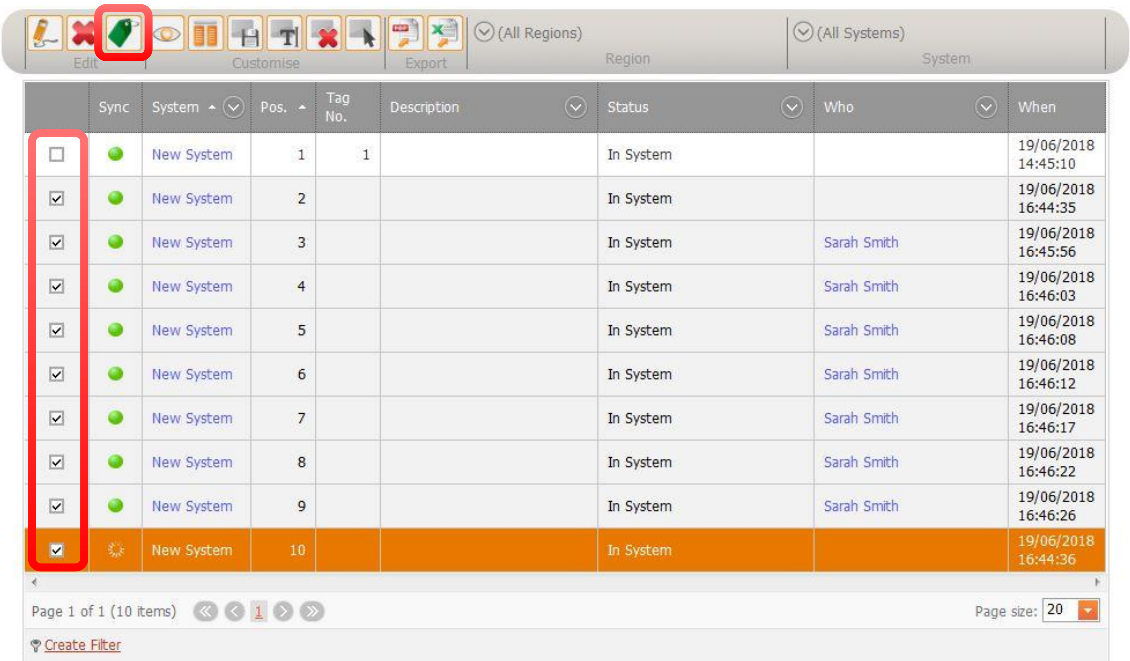
Each key or key bunch will be assigned a physical tag which should correspond with the same tag number within TrakaWEB. Tag numbers in TrakaWEB can only be created or edited by a user with the Edit iFob Software Permission. The Tag Number will be synchronised with the iFob and the Tag Number will be stored in the iFob's memory. The Search function in Traka Touch can be used to locate an iFob by entering the Tag Number into the search.

1. Click on **iFobs** on the Navigation Toolbar.

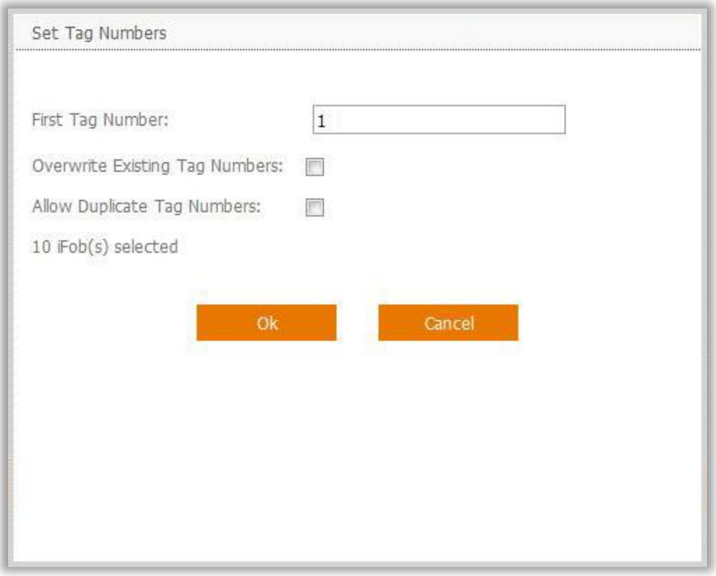
At the iFobs screen, you will see a list of all the current iFobs in the selected system.



Click the checkbox of the corresponding position for the iFob you wish to assign a Tag Number to and then click on the **Set Tag Numbers** icon on the ribbon toolbar. Alternatively, multiple checkboxes can be selected to assign Tag Numbers automatically in sequential order. By clicking outside of a checkbox and then holding the shift key and clicking outside a checkbox further down the list, all the checkboxes in between will be selected as shown below.



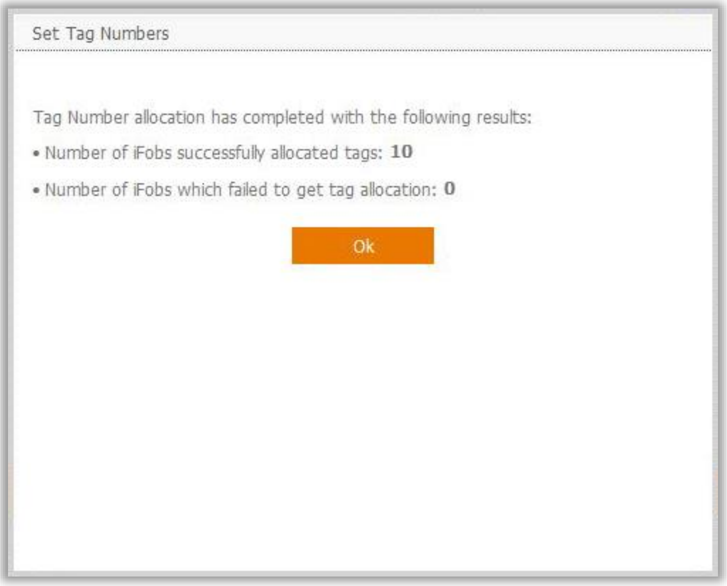
After clicking on **Set Tag Numbers**, a window will appear allowing you to manually insert a Tag Number. There are also 2 optional check boxes that will enable you to overwrite existing tag numbers or allow duplicate numbers.



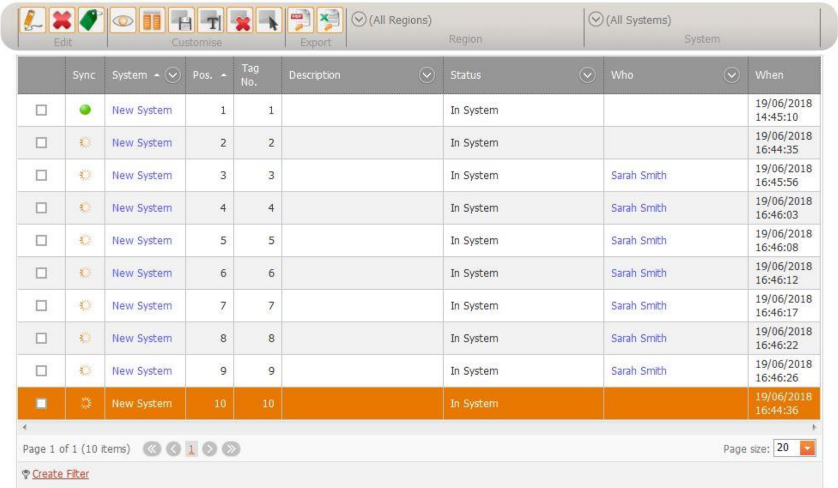
2. After you have inserted the correct Tag Number and selected any of the optional checkboxes, click on **OK**.

A window will appear showing the results of the process.

3. Click on **OK** to continue.



The iFobs screen will now display the newly created Tag Numbers. This process can be repeated to add Tag Numbers to iFobs as required.



The Tag Number will be synchronised with the iFob and the Tag Number will be stored in the iFob's memory.

NOTE: If the administrator chose to overwrite existing tag numbers, any iFobs that already have a Tag Number will be overwritten.

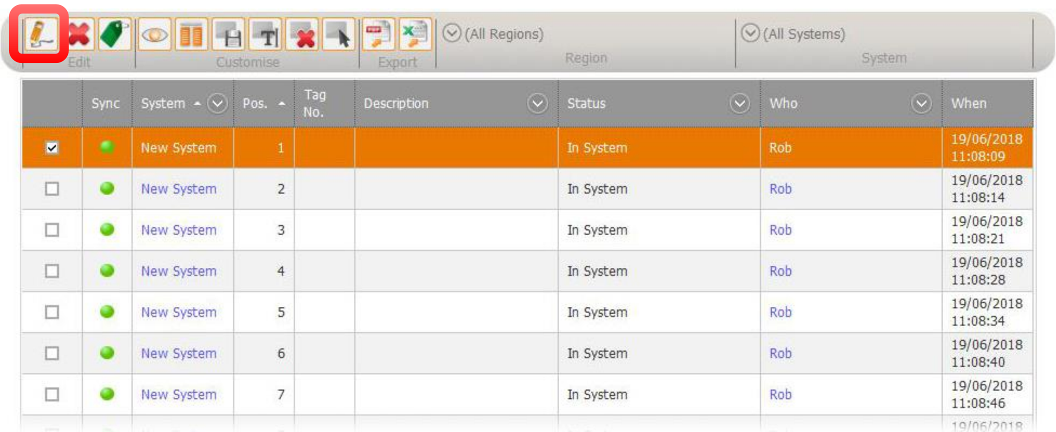
NOTE: If the administrator chose to allow duplicates, no checks will be made during the application of the tag numbers.

NOTE: If the administrator chose not to allow duplicates, any tag numbers that are already in use will be skipped.

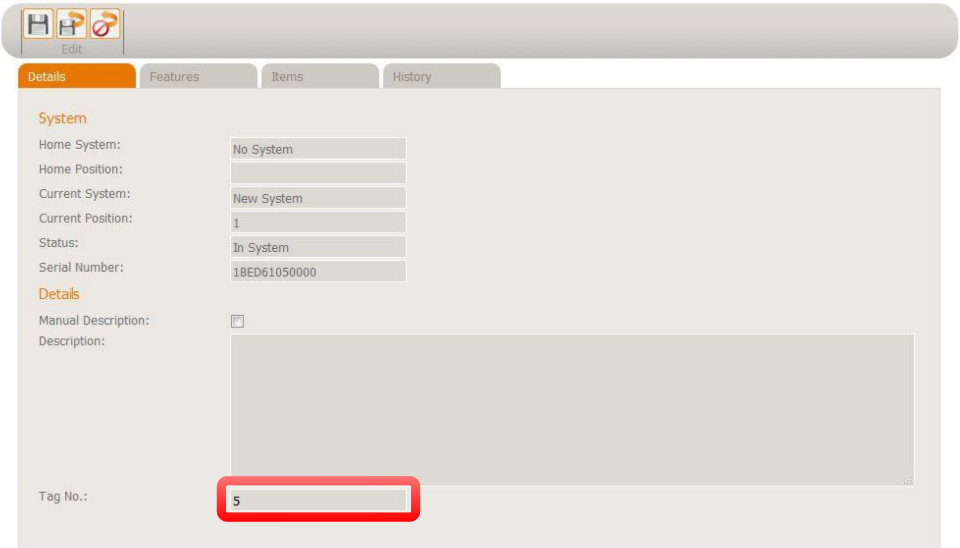
6.10.6.1 EDITING TAG NUMBERS

Should you wish to edit a Tag Number for an iFob, this can be achieved by accessing the iFobs page from the Navigation Toolbar.

1. Click on the checkbox for the iFob or iFobs with the Tag Number you wish to remove and then click on the **Edit** button.



At the Edit iFob page, you can now change the Tag number as shown below:



2. Once completed, click on **Save & Return**.

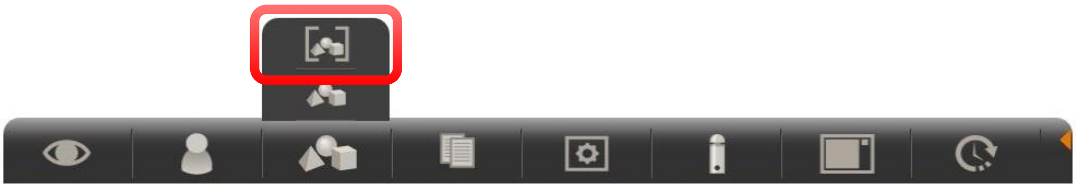
NOTE: To clear a Tag Number, enter '0' as the Tag Number value and then click Save.

6.10.7 COMMON ITEM ACCESS GROUPS

Item Access Groups with the ‘Common Group’ option ticked in TrakaWEB will be known as a ‘Common Item Access Group’. This will be used to apply a common access right to all Items that are a member of the group that can be shared across multiple systems to which the item can be returned. For more information on Item Access Groups, refer to **section 4.4.6**

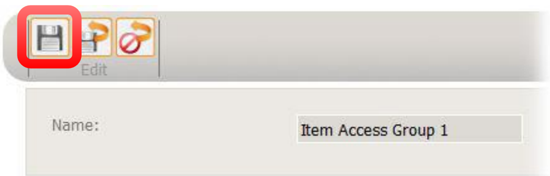
NOTE: The ‘Common Group’ option will only appear if one or more systems are configured with RRMS in the TrakaWEB database.

1. Select **Item Access Groups** from the Items menu on the Navigation Toolbar.



2. At the **Item Access Groups** page, click on the **Create** button. 

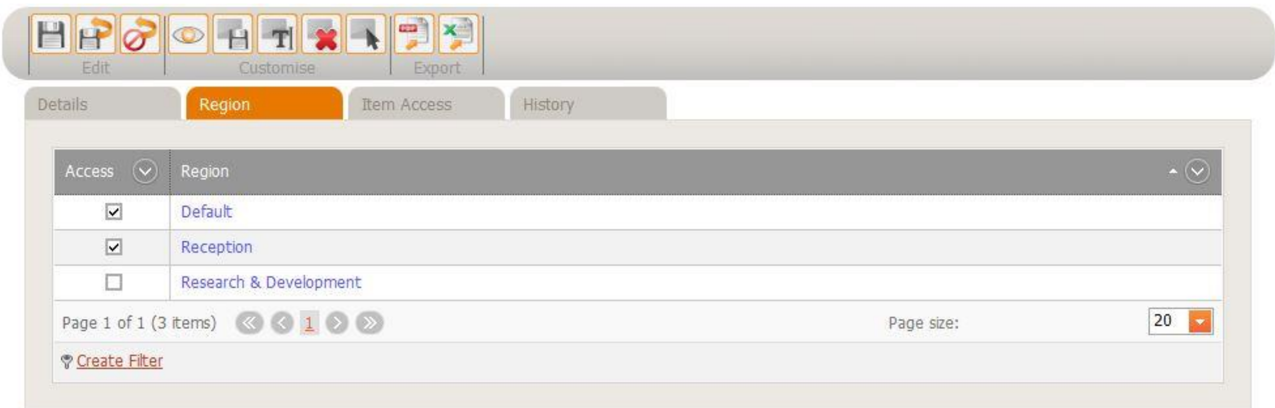
3. At the next screen enter a name for the New Item Access Group and then click on **Save.**



To create a common Item Access Group, place a tick in the Common Group checkbox. If all the systems defined in TrakaWEB have RRMS enabled, the Common Group option will be ticked by default.

4. Next, click on the **Region** tab.

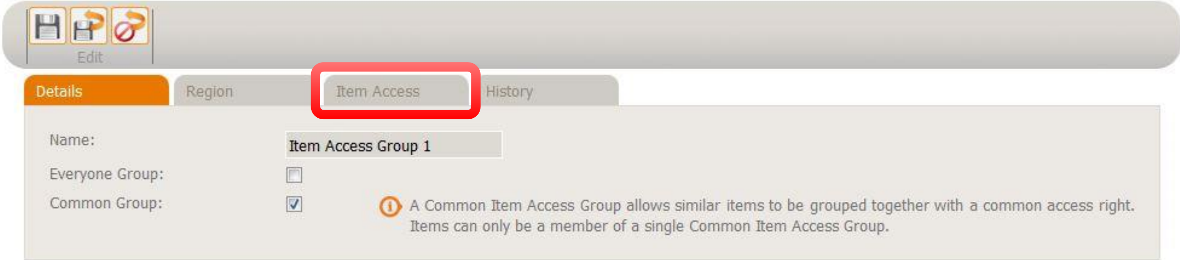
Regions control the visibility of the Common Item Access Group in the same way as a standard Item Access Group.



The Region will also determine which systems the associated Items of the common Item Access Group can be returned to. For more information on Regions, refer to **Section 4.6.1**.

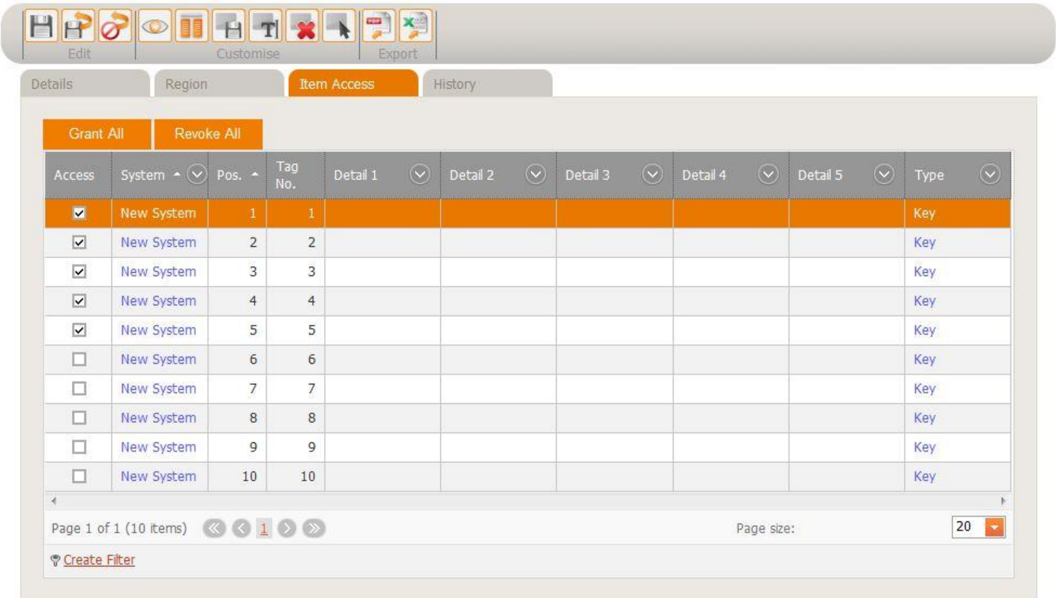
NOTE: If an Item is returned to a RRMS system that is outside the scope of the Common Item Access Group's region, the Item can be returned but will no longer be accessible to standard users. In this case, only an Admin User can remove it.

5. After making a selection, click on the **Item Access** tab.



You will now be taken to the Edit Item Access Group page where you can add iFobs to the selected Item Access Group.

6. Click on the checkboxes to assign the iFobs to the Item Access Group.



NOTE: An iFob/Item can only belong to a single Common Item Access Group.

NOTE: Items that are assigned to a FRSS or RRSS are not able to form part of a Common Item Access Group.

7. Once completed click on **Save & Return** to be redirected back to the Item Access Groups list.

6.10.7.1 ASSIGN USERS TO COMMON GROUPS

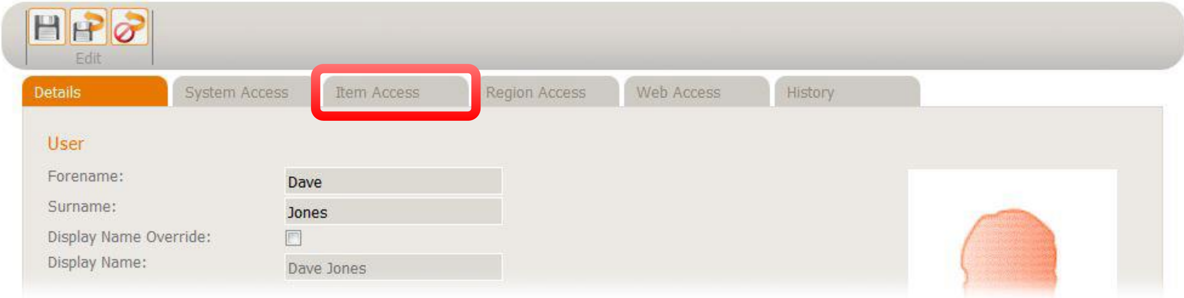
With the iFobs now assigned to a Common Item Access Group, you can now select which users will have access to that Group. This will determine which iFobs they will be allowed access to.

Users are created in the usual method within TrakaWEB.

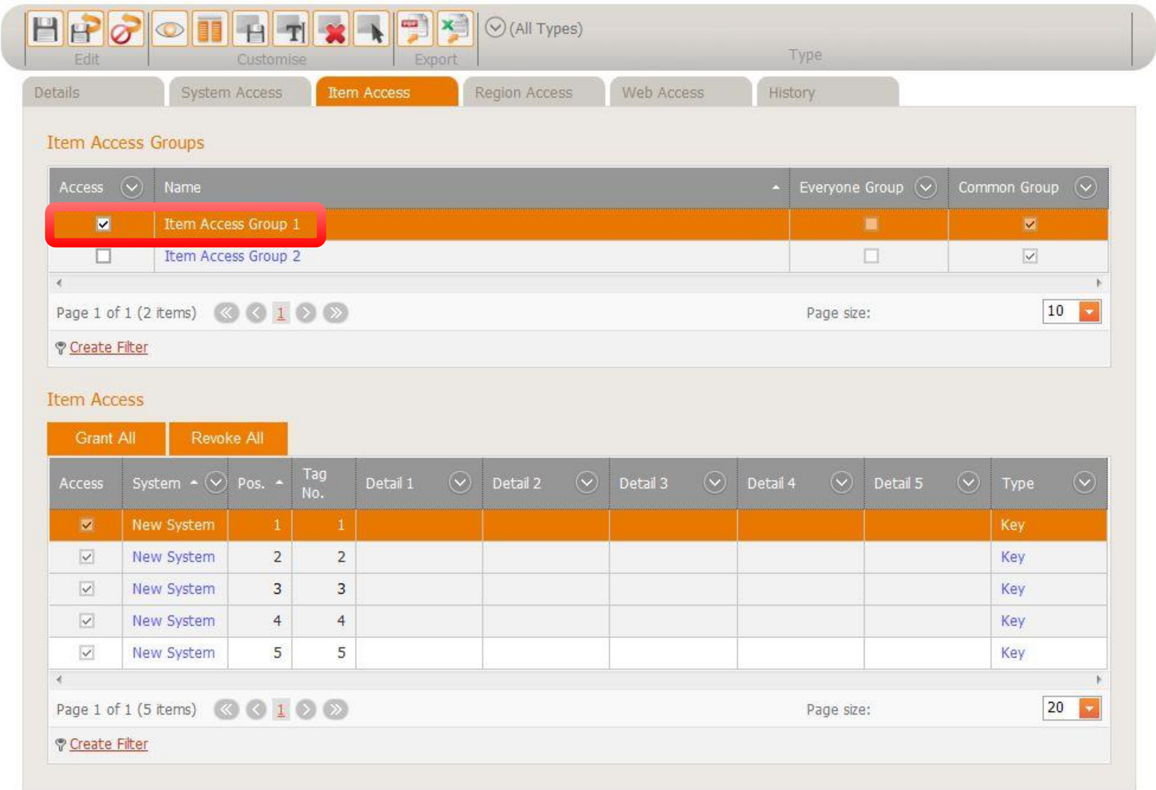
NOTE: Due to RRMS limitations, the System Access page contains fewer details.

1. Select a user from the Users page that you wish to edit.

2. At the Edit User page, click on the **Item Access** tab.



3. At the next page, select which Item Access Group you wish to allocate to the user.



4. Once you have made your selection, click on **Save and Return**.

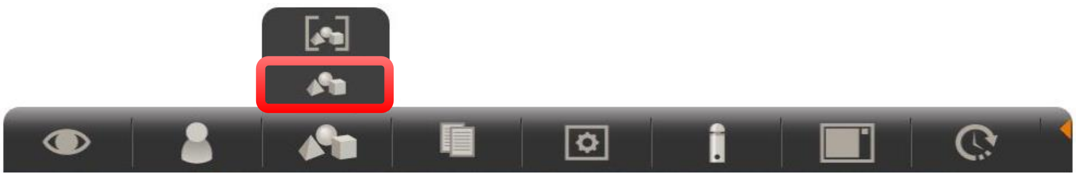
6.10.8 TRAKA TOUCH - SEARCHING FOR IFOBS

A system with RRMS enabled will only retain information about the iFobs/Items that are currently in the system. If an iFob/Item is removed, then the System will only retain the event history and will not store any details of the actual iFobs/Items.

This means that the function of a Traka Touch System can only search for the iFobs/Items that are in the System.

Where a wider scale search is required across multiple systems, it is more practical to search for Items in TrakaWEB.

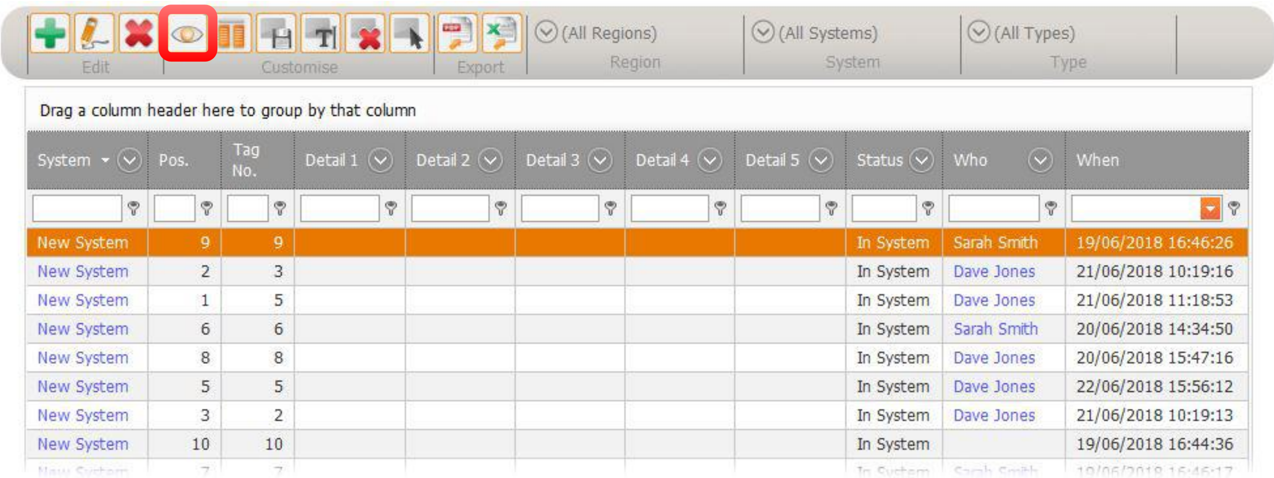
1. Click on the Items icon within Items on the Navigation Toolbar.



The Items page will show a list of details for all iFobs/Items in each available System.

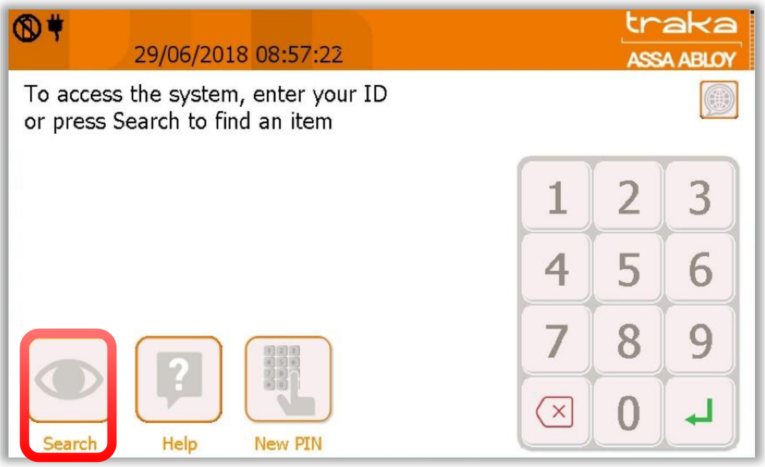
2. Click on the **Search For** icon on the Ribbon Toolbar.

You can now enter search details for each column in the grid. For more information on Searching, refer to section 4.1.1.1.

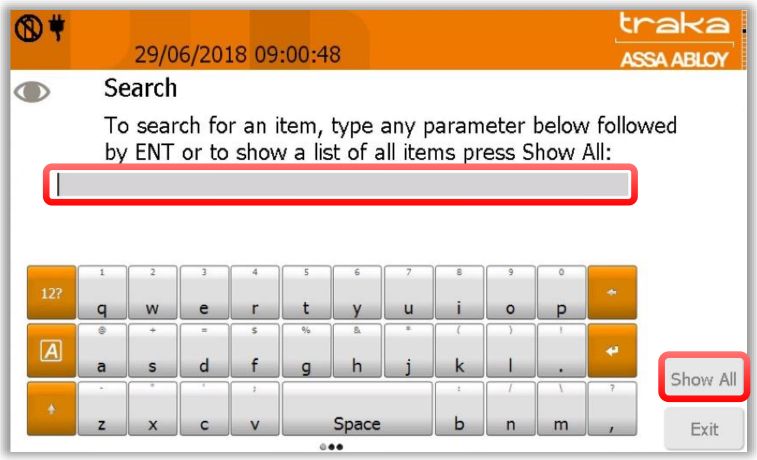


Locating Items in Traka Touch can be done using the Search function.

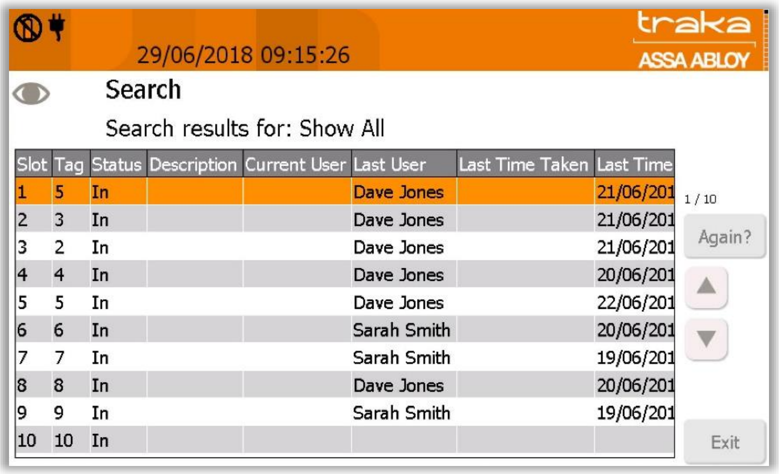
3. Tap **Search** on the Touch screen.



4. At the Search screen, enter the details for the Item you wish to locate or tap on **Show All**.



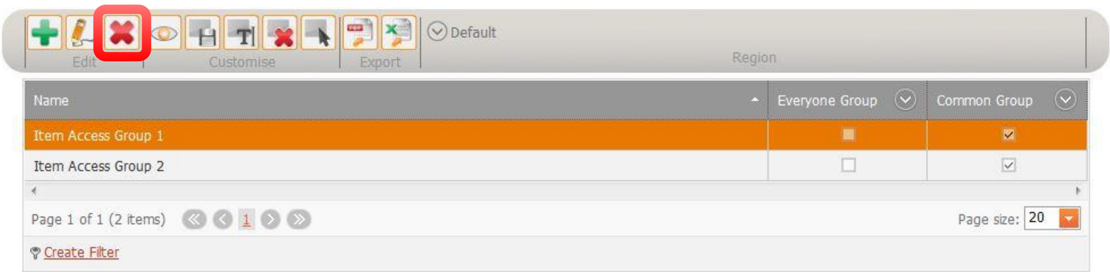
Depending on your choice of search option, the next screen will display a list of results.



6.10.9 DELETING GROUPS

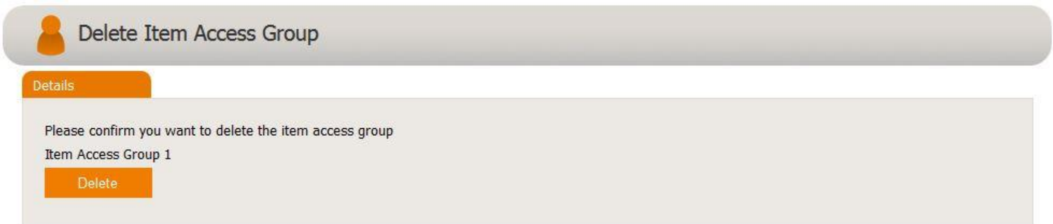
Other than creating and editing Common Item Access Groups, it may also be necessary to delete them if they are not required.

1. Navigate to the Item Access Groups from the Navigation Toolbar.
2. Select the Item Access Group you wish to delete and click on the delete button.



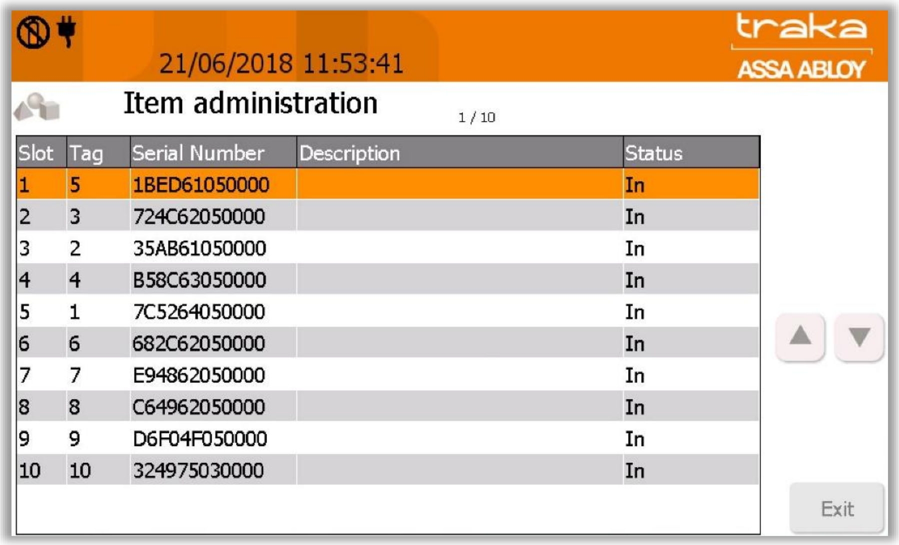
At the next page, you will be asked to confirm that you want to delete the selected Item Access Group.

3. Click on the Delete button to continue.



6.10.10 ITEM SETUP

With RRMS enabled, there is no requirement for Item Setup within Traka Touch. The Item Administration screen will provide a record of all the iFobs currently in the system.



6.11 TEMPORARY KEY STORE (TKS)

Temporary Key Store is a cost option feature that will allow a user to temporarily deposit their keys into a different cabinet to that which the keys were removed from.

The Temporary Key Store cabinet maybe used in a situation where taking keys is against compliance such as outside of work premises or areas considered to be of high-risk. In conditions such as these, the keys maybe placed in the Temporary Key Store cabinet to keep track of their location and retrieved later as required.

An override option can be assigned to a user in TrakaWEB, which will enable them to remove iFobs from the Temporary Key Store regardless of them being granted access. This will generate a 'Temporary Key Store Override' event which will appear in the activity report. However, Real Time Activity will not show any 'Temporary Key Store Override' events unless activated from Activity Types in the Software Settings menu. An 'Activity Trigger' can also be set within TrakaWEB to generate an Email Notification.

Due to the nature of the Temporary Key Store functionality, there is no Search option available on Traka Touch.

6.11.1 LIMITATIONS

The Temporary Key Store feature is compatible with the following:

- Key Control Products
- Random Return Multiple Systems
- Remote Commands (Remote Release and Remote User Login)
- Email Notifications (Temporary Key Store Override event)
- Extension Cabinets

The Temporary Key Store is not compatible with the following (Excluding home-system setup):

- Lockers
- Rack Manager
- Random Return Single System (RRSS)
- Fixed Return to Single System (FRSS)
- Item Booking
- Access Schedules
- Allowance Across Systems
- Reason Logging
- Notes Logging
- Fault Logging
- Fuel, Distance and Location Logging
- Item Handover
- Custom Messages
- Curfews
- Authorisers
- iFob Authorisation
- User & Item Import Spreadsheet on Touch
- Individual Item Allowances
- Integration Engine

6.11.2 PREREQUISITES

A configuration file will be required to enable RRMS and TKS, which can be obtained from Traka. To load the configuration file, please refer to **UD0011 – Traka Touch User Guide**.

Although the iFob home system maybe be a Fixed Return system, the Temporary Key Store is based on Random Return to allow iFobs to be returned and retrieved from any position.

Please refer to the Random Return to Multiple Systems section of this document for more information on setup up and configuration of RRMS.

6.11.3 USING TEMPORARY KEY STORE

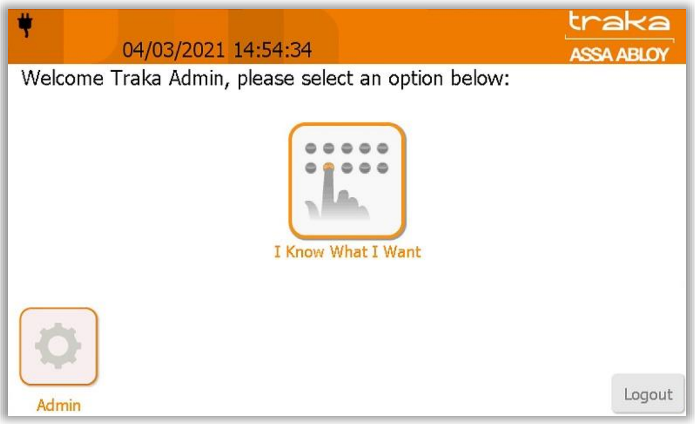
A user will be able to deposit multiple items that they have been granted access into the Temporary Key Store. By using the I Know What I Want functionality on Traka Touch, they will in return be able to remove those items as required.

Only the user who deposited the items to the Temporary Key Store maybe able to remove them unless they have been granted the override permission. In this situation, an override event will be generated.

Due to the nature of The Temporary Key Store/RRMS, there is no Search functionality available.

Items are taken from the home system as required, by a user who has been granted access to them.

If a User with the Admin role accesses the TKS system, they will be presented with the option to either enter the Admin menu or deposit and remove items by selecting the **I Know What I Want** button.



When a non-Admin User logs into the system, the door will automatically open to allow them to deposit or remove items.

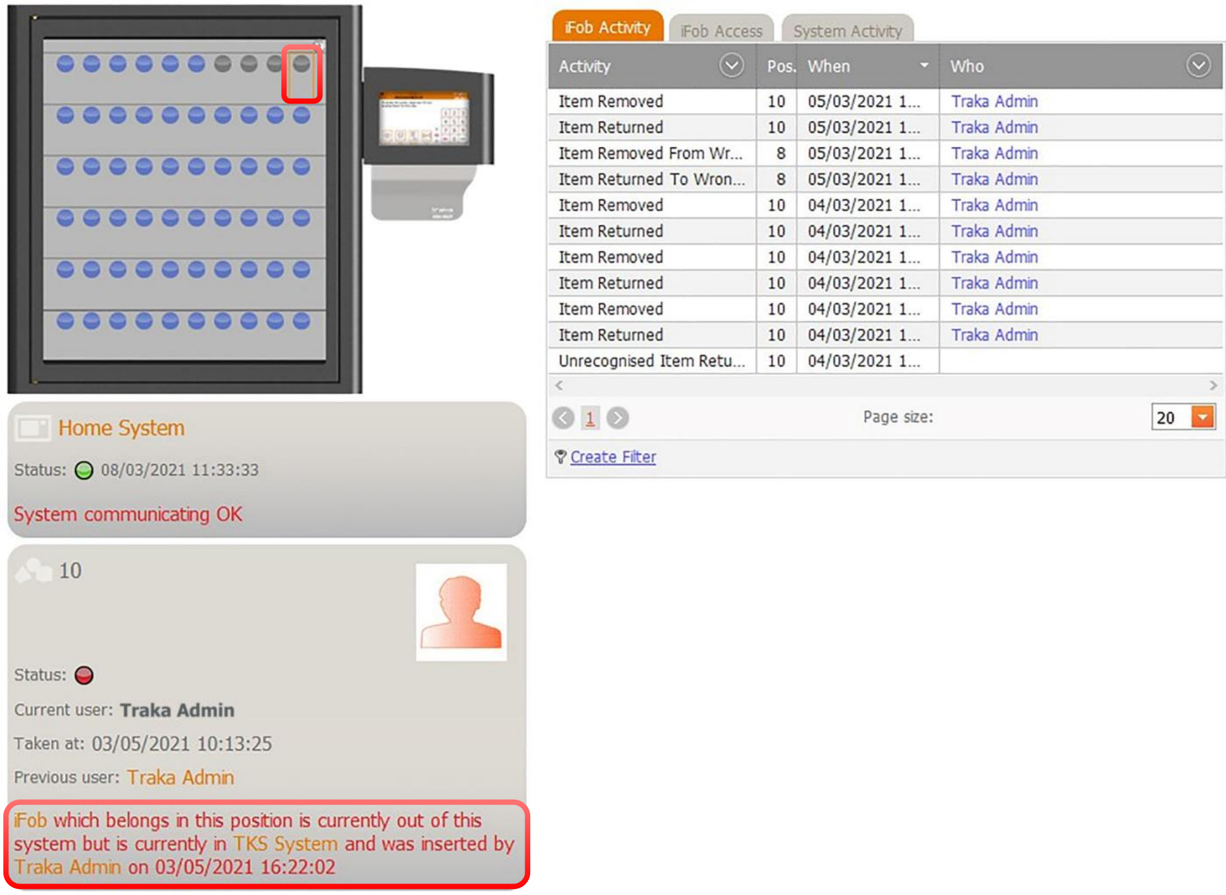
1. After logging in as an Admin User, Access the system by selecting the **I Know What I Want** button.

   The door will now open and you can then place the iFob in the system.

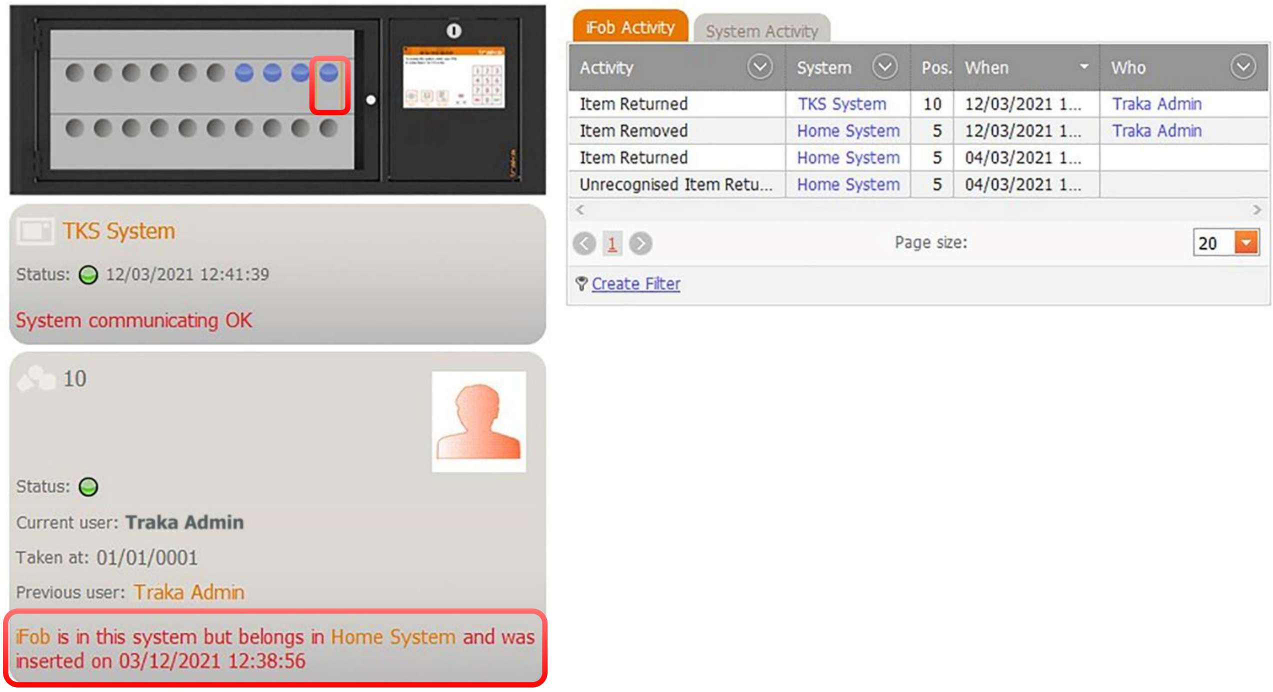
2. Place the iFob in any available slot and then close the door. The system will automatically log out.

When a user returns to the system to remove items, they will only be allowed to take items that they originally deposited. Items in red represent Items that have been deposited by other users. This rule will apply to all users unless they have been given the override permission.

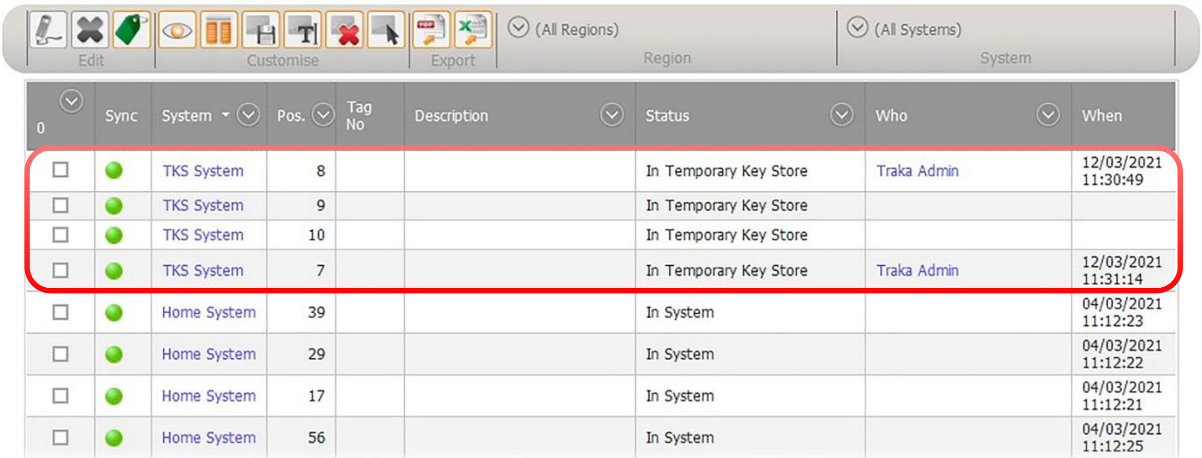
A record of removed items is viewable from the home system when an item that has been removed is selected in the System Viewer. A message will be displayed as shown below.



A record of items placed in the Temporary Key Store system can be viewed by selecting a deposited item at the System Viewer page.



Selecting the iFobs Icon from the Navigation Toolbar will also provide information as to which iFobs are currently out of the system and their location in the Temporary Key Store.

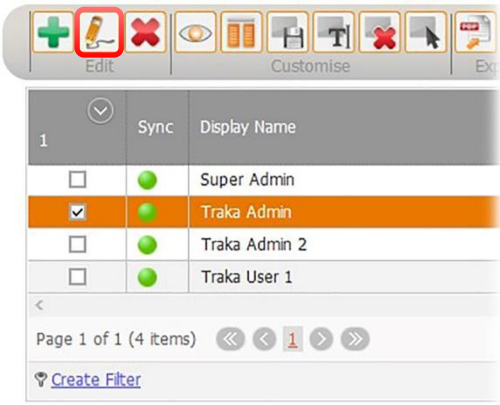


0	Sync	System	Pos.	Tag No	Description	Status	Who	When
☐		TKS System	8			In Temporary Key Store	Traka Admin	12/03/2021 11:30:49
☐		TKS System	9			In Temporary Key Store		
☐		TKS System	10			In Temporary Key Store		
☐		TKS System	7			In Temporary Key Store	Traka Admin	12/03/2021 11:31:14
☐		Home System	39			In System		04/03/2021 11:12:23
☐		Home System	29			In System		04/03/2021 11:12:22
☐		Home System	17			In System		04/03/2021 11:12:21
☐		Home System	56			In System		04/03/2021 11:12:25

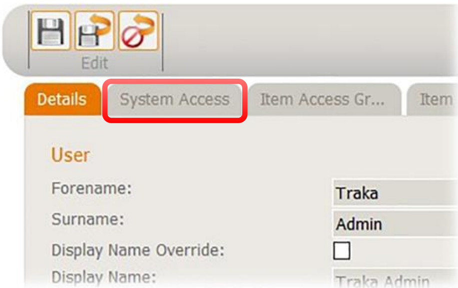
6.11.4 TEMPORARY KEY STORE OVERRIDE

A User with the Temporary Key Store Override function will be able to remove items from the Temporary Key Store system even if they have not been granted access to those items.

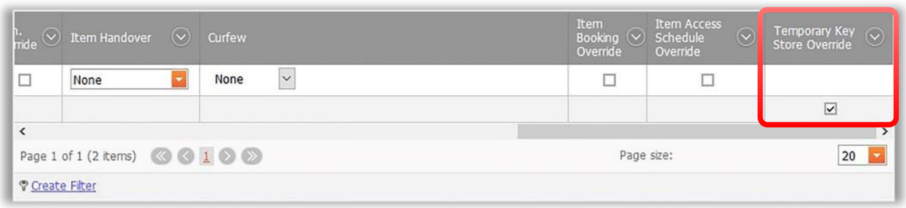
1. From the Navigation Toolbar, navigate to the Users page, select a User and then choose **Edit**.



2. At the **Edit User** page, select the **System Access** tab.



3. At the **System Access** page, scroll to the right of the system access grid and place a tick in the checkbox for **Temporary Key Store Override.**

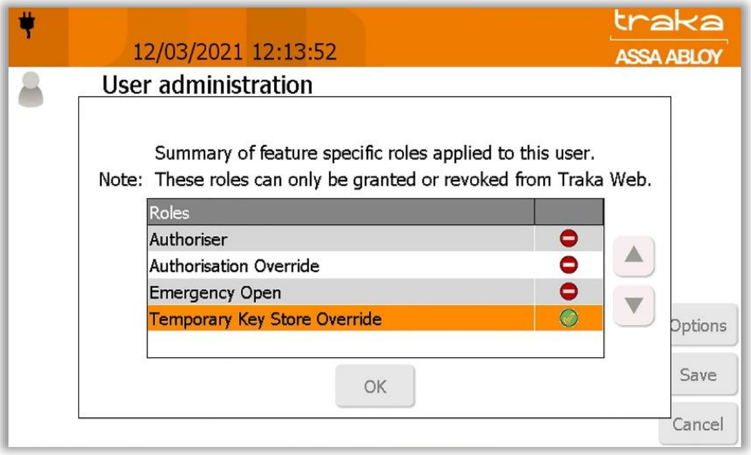


NOTE: The override option is only available for systems configured for Temporary Key Store. It will not allow users to remove items that they have not been granted access to, from non-Temporary Key Store systems.

4. Once completed, click on **Save & Return**.

The selected User will now have the permission to remove any items from the Temporary Key Store as required.

Although the Temporary Key Store Override permission cannot be set at the Traka Touch system, any override permissions a user has been given can be viewed in Roles within User Administration at the Temporary Key Store system.

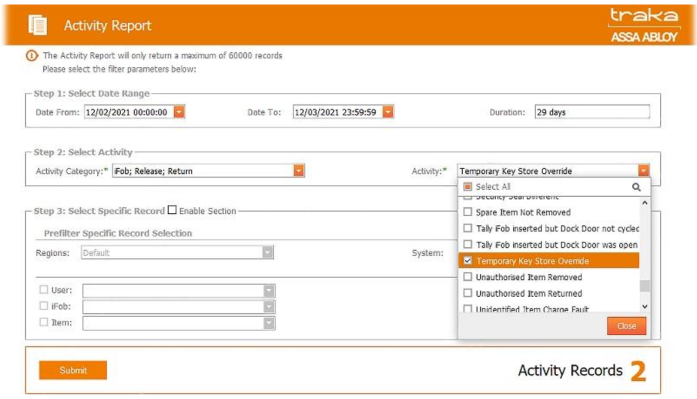


6.12 REPORTS

6.12.1 TEMPORARY KEY STORE ACTIVITY REPORT

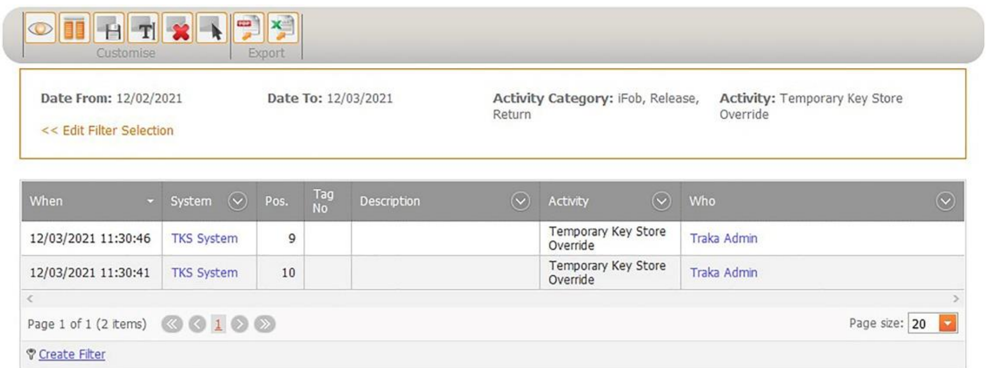
Any time that the Temporary Key Store Override permission is used, a recorded event is generated. The activity can be selected when creating an Activity Report.

1. Within Activity Reports, navigate through the **Activity** menu as shown and place a tick in the checkbox for **Temporary Key Store Override.**



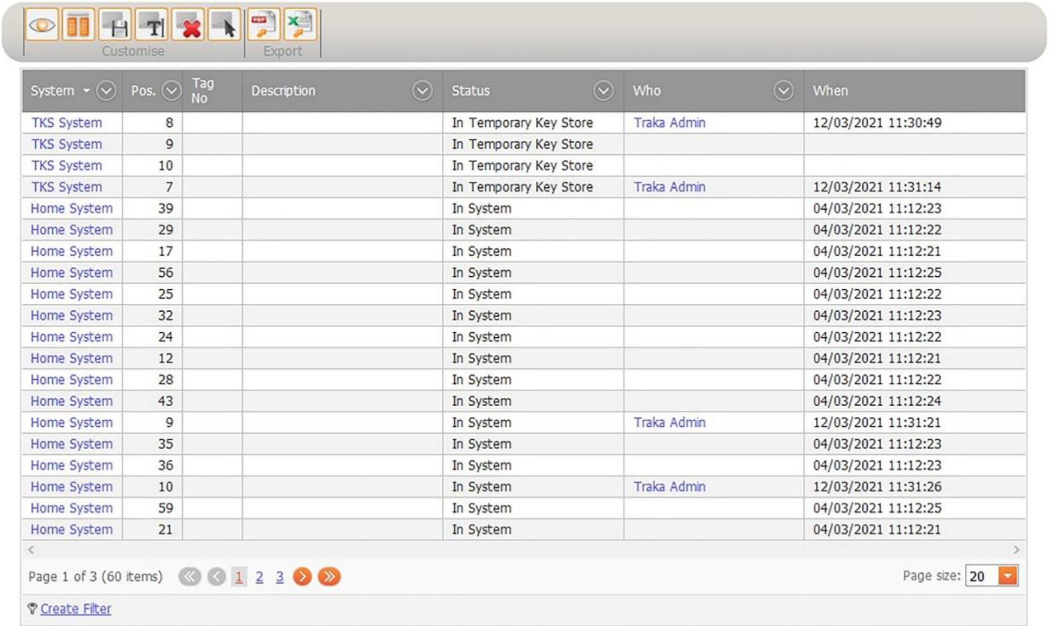
2. After completing the filter parameters for the report, click on the **Submit** button.

The report for Temporary Key Store and any other filtered parameters will then be shown.



6.12.2 CURRENT ITEM STATUS REPORT

A Current Item Status Report may be viewed by selecting the tab from the Status menu in Reports.



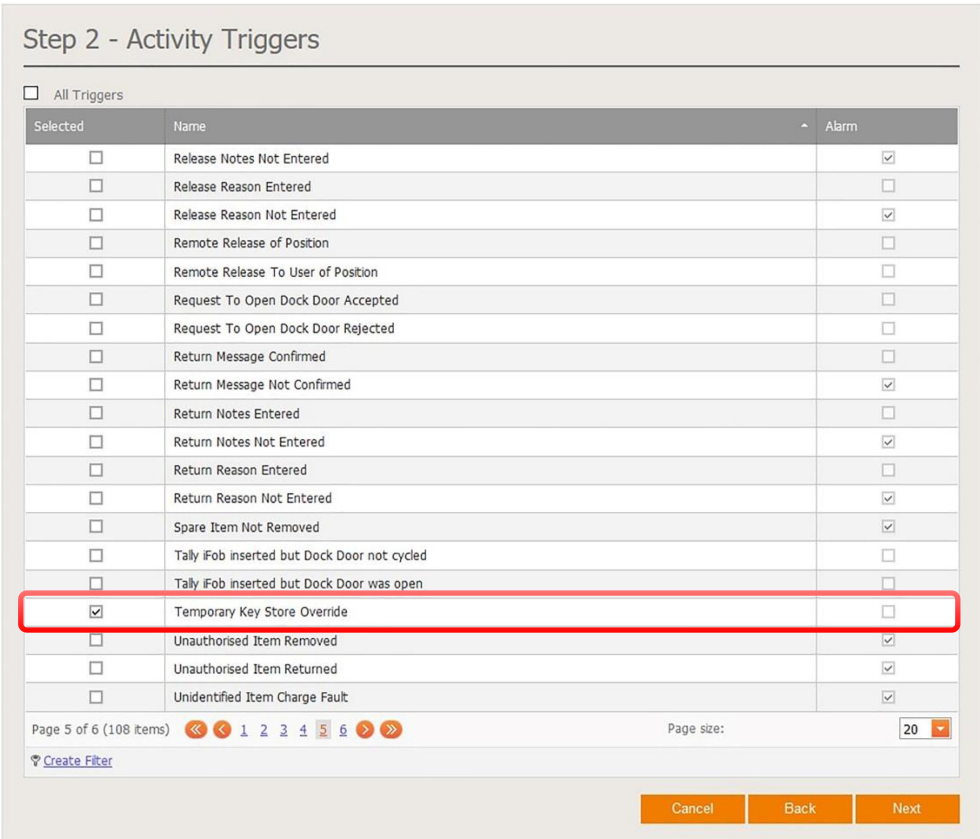
System	Pos.	Tag No	Description	Status	Who	When
TKS System	8			In Temporary Key Store	Traka Admin	12/03/2021 11:30:49
TKS System	9			In Temporary Key Store		
TKS System	10			In Temporary Key Store		
TKS System	7			In Temporary Key Store	Traka Admin	12/03/2021 11:31:14
Home System	39			In System		04/03/2021 11:12:23
Home System	29			In System		04/03/2021 11:12:22
Home System	17			In System		04/03/2021 11:12:21
Home System	56			In System		04/03/2021 11:12:25
Home System	25			In System		04/03/2021 11:12:22
Home System	32			In System		04/03/2021 11:12:23
Home System	24			In System		04/03/2021 11:12:22
Home System	12			In System		04/03/2021 11:12:21
Home System	28			In System		04/03/2021 11:12:22
Home System	43			In System		04/03/2021 11:12:24
Home System	9			In System	Traka Admin	12/03/2021 11:31:21
Home System	35			In System		04/03/2021 11:12:23
Home System	36			In System		04/03/2021 11:12:23
Home System	10			In System	Traka Admin	12/03/2021 11:31:26
Home System	59			In System		04/03/2021 11:12:25
Home System	21			In System		04/03/2021 11:12:21

Page 1 of 3 (60 items) 1 2 3 Page size: 20

Create Filter

6.12.3 EMAIL NOTIFICATIONS

A Trigger Event can be used to send an email notification when the Temporary Key Store Override option is used. For more information on email notification configuration, please refer to **TD0013-TrakaWEB Installation and Configuration Guide.**



Step 2 - Activity Triggers

☐ All Triggers

Selected	Name	Alarm
☐	Release Notes Not Entered	☑
☐	Release Reason Entered	☐
☐	Release Reason Not Entered	☑
☐	Remote Release of Position	☐
☐	Remote Release To User of Position	☐
☐	Request To Open Dock Door Accepted	☐
☐	Request To Open Dock Door Rejected	☐
☐	Return Message Confirmed	☐
☐	Return Message Not Confirmed	☑
☐	Return Notes Entered	☐
☐	Return Notes Not Entered	☑
☐	Return Reason Entered	☐
☐	Return Reason Not Entered	☑
☐	Spare Item Not Removed	☑
☐	Tally iFob inserted but Dock Door not cycled	☐
☐	Tally iFob inserted but Dock Door was open	☐
☑	Temporary Key Store Override	☐
☐	Unauthorised Item Removed	☑
☐	Unauthorised Item Returned	☑
☐	Unidentified Item Charge Fault	☑

Page 5 of 6 (108 items) 1 2 3 4 5 6 Page size: 20

Create Filter

Cancel Back Next

6.13 ITEM PAIRING

6.13.1 OVERVIEW

Item Pairing is a powerful security feature which can prevent users from taking too many critical keys or assets from Traka Touch systems simultaneously or prevent the removal of keys or assets when it is not safe to use them.

It allows the TrakaWEB administrator to arrange Items in pairs or groups. Moreover, you can decide how the paired items will behave. Item Pairing can be arranged in accordance with either of the two different rule types and you will need to choose which rule type is more appropriate for your chosen items:

Exclusive User Pairing	Lockout Pairing
• You can create pairs of items • Each pair will have one Primary item and one Secondary item • When you remove one paired item from the system, you will not be able to remove the second • When you have one item from the pair out of the system, a different user can remove the other one	• You can create groups of items • Each group will consist of one or more Primary items and one Secondary item • When at least one Primary item is out of the system, no user can remove the Secondary item • All the Primary items must be back in the system before the Secondary item can be removed • When the Secondary item is out of the system, no user can remove any of the Primary items

To demonstrate the power and potential application of the Item Pairing feature, consider the following examples:

- **Exclusive User Pairing:** A company has a security safe and two associated keys (the primary key and the spare) stored in a Traka Touch system. The feature will prevent an authorised user from taking both keys at once. One user can only take one key at a time, and they must return the first key to remove the other. Other users can remove the spare in the meantime, as they might need access to the safe as well
- **Lockout Pairing:** A company has an engine room and a number of electrical boxes in the engine room. There is one main engine key (the Secondary key) and a number of keys to different electrical boxes (Primary keys). The feature will prevent different users from removing the main engine key until all the keys to the electrical boxes have been returned. Conversely, when the main engine key is out of the system, no user will be able to remove any keys to the electrical boxes to prevent any damage to the equipment or harm to the personnel.

NOTE: You can set up as many rules per system as you can have possible item pairings, and one system can work with multiple rules of both types enabled on it.

NOTE: One item can only be assigned to one rule.

6.13.2 ITEM PAIRING: FRSS OR ADVANCED FIFO

Item Pairing can be used on Touch systems working in 2 mutually exclusive modes:

1. It can be set up on systems working in the Fixed Return to Single System (FRSS) mode OR
2. It can be set up on systems working in the Advanced First In-First Out (AFIFO) mode.

Should you require a change to your chosen configuration, please contact Traka or your Distributor.

6.13.3 LIMITATIONS

NOTE: At the moment, the Item Pairing feature is only available for Key Management systems.

Due to the nature of the Item Pairing feature, it is incompatible with the following features on TrakaWEB/Traka Touch:

- Random Return to Single System (RRSS)
- Random Return to Multiple Systems (RRMS)
- Temporary Key Store (TKS)
- DockSafe
- Rack Manager

6.13.4 ENABLE ITEM PAIRING

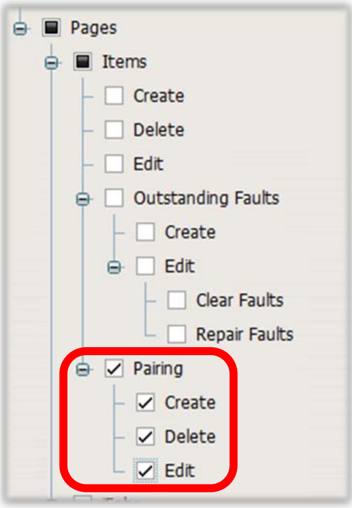
To enable Item Pairing on TrakaWEB, at least one of the systems connected to TrakaWEB must be configured to work with the Item Pairing function enabled. To enable Item Pairing for a specific system, you will need to upload an appropriate Config file onto that system.

You will need to decide whether the Item Pairing will be enabled on a FRSS system or a system working in the Advanced FIFO mode as your decision will affect which Config file will need to be uploaded on the affected system(s). To read more about Advanced FIFO, refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide**.

To obtain the relevant Config files with the Item Pairing enabled for your systems, contact Traka or your Distributor.

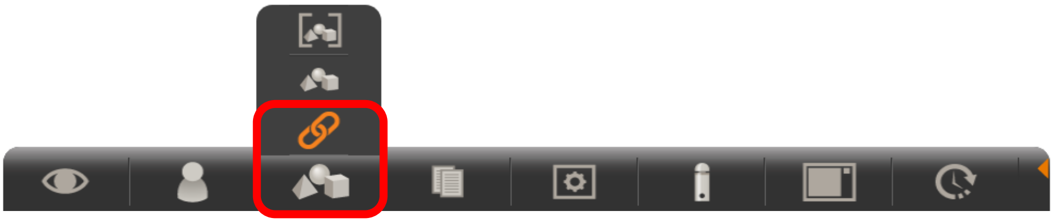
6.13.5 ITEM PAIRING SOFTWARE PERMISSIONS

As a TrakaWEB administrator, you may or may not have the necessary permissions to create, edit, or delete Item Pairing rules. To check if your Software Permissions Group has got appropriate permissions, make sure that the following checkboxes relating to the Item Pairing are ticked in the Edit options of your Software Permissions Group. The Item Pairing permissions can be found in the software permissions tree under **Web > Pages > Items > Pairing:**

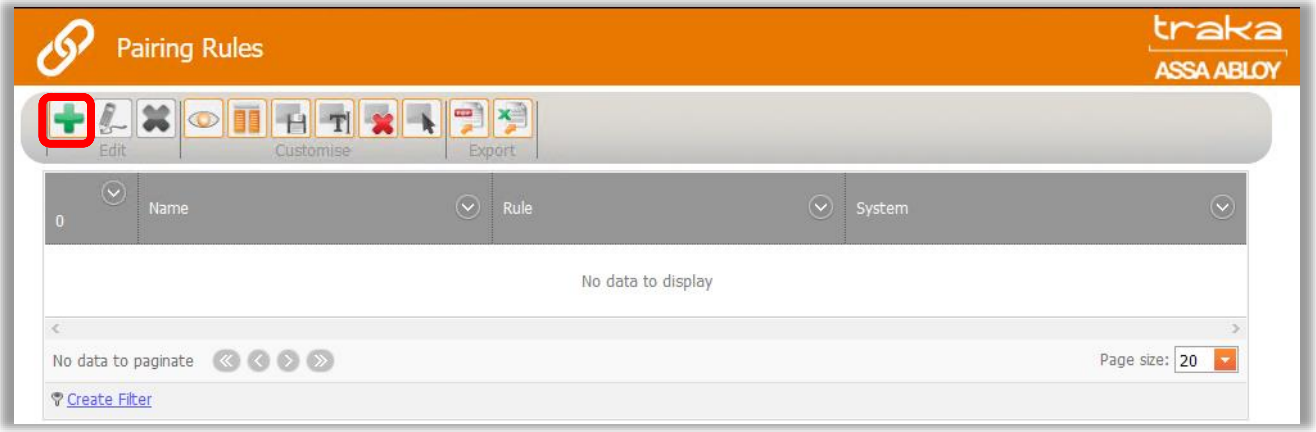


6.13.6 CREATE AN ITEM PAIRING RULE

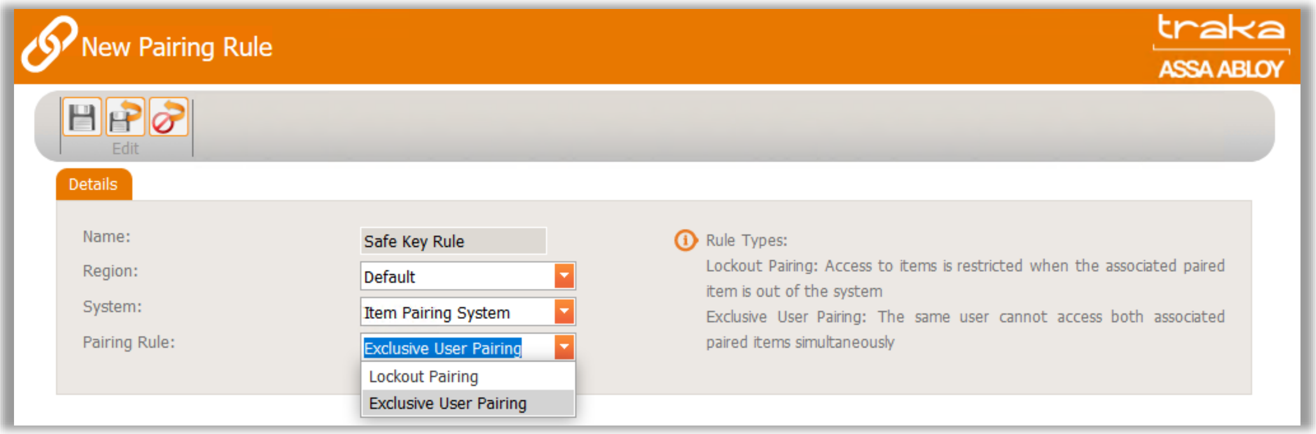
1. To create an Item Pairing rule, select **Items** on the Navigation Toolbar. The menu will expand and reveal the **Item Pairing** sub-menu represented by the chain links icon:



2. TrakaWEB will then display all the current Item Pairing rules that exist within the database. Click on the **Create** button on the Ribbon Toolbar.



3. You will be taken to a new page, where you will need to provide a name for the new rule, and then subsequently select the Region and the System which will be affected by the new rule, as well as select the Pairing Rule Type that you need to create.



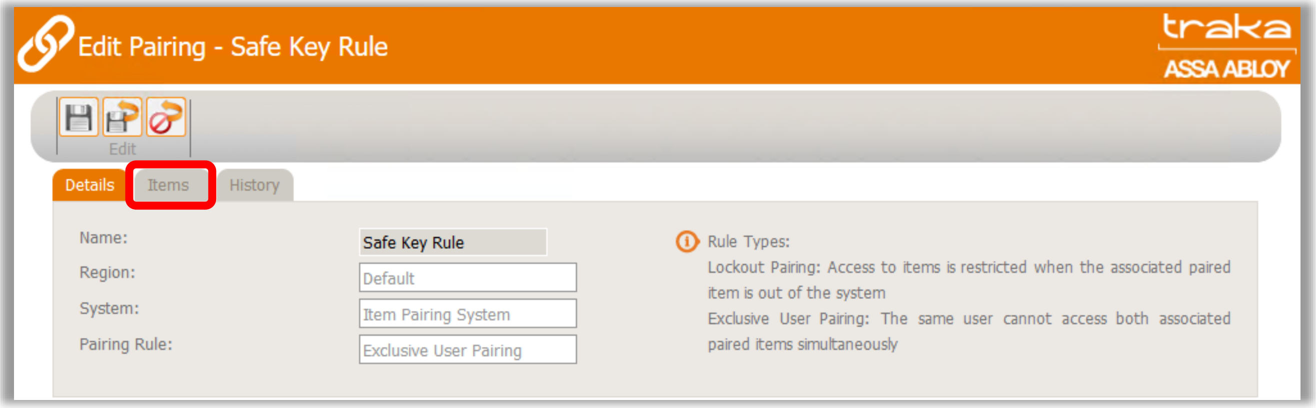
To decide which rule you should create, refer to the Item Pairing Overview section in this document.

NOTE: Once you have created the rule, you will not be able to change its selected Region, System, or Pairing Rule Type. If that is the case, you will need to delete the rule and create a new one instead.

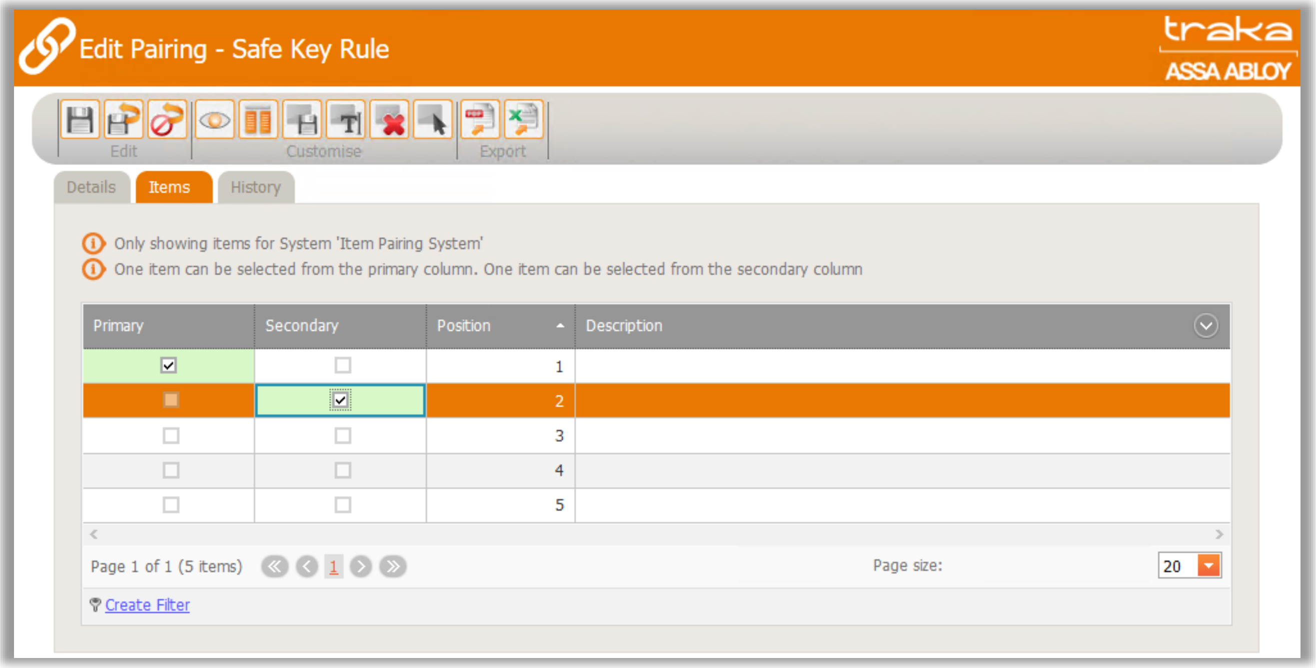
4. Once you have made your selection, click on **Save**.

The page will now update, and your selected Region, System, and Pairing Rule Type will be greyed out. You will also gain access to two new tabs: Items and History.

5. Select the **Items** tab.



6. Depending on the Item Pairing Rule you have chosen previously, select your Primary and Secondary Items by checking the boxes in the relevant columns next to the respective Items' positions.

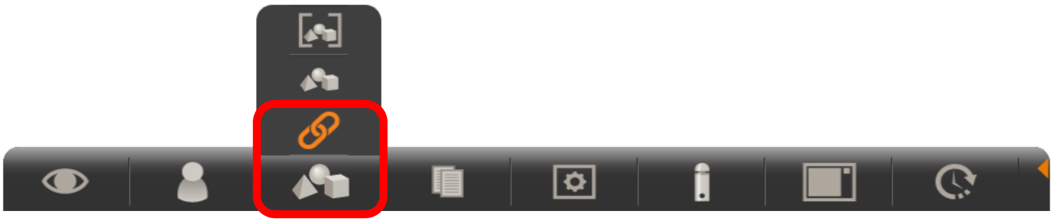


NOTE: In the Exclusive User Pairing, you may select only one Primary and one Secondary. In the Lockout Pairing, you may select multiple Primaries and one Secondary.

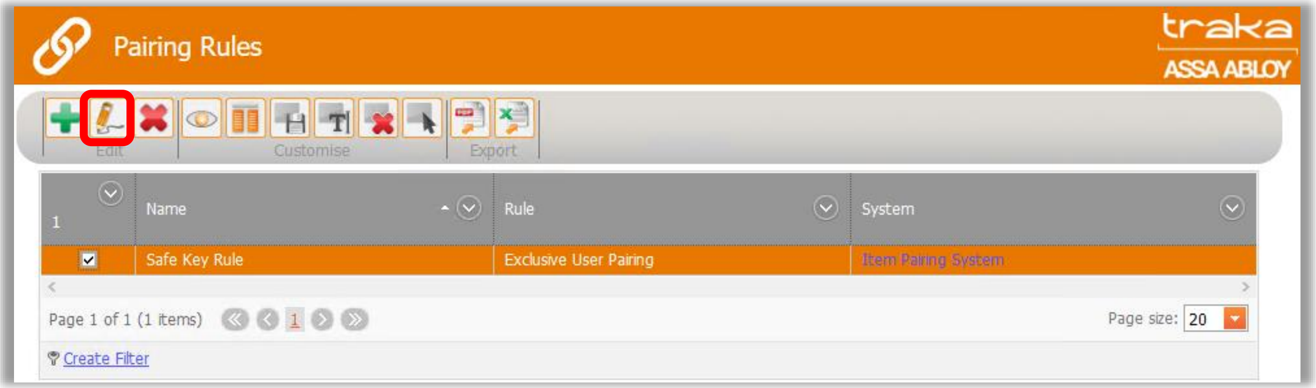
7. Once you have chosen your Items for the Item Pairing Rule, you can click on **Save and Return**.

6.13.7 EDIT AN ITEM PAIRING RULE

1. To edit an Item Pairing rule, select **Items** on the Navigation Toolbar. The menu will expand and reveal the **Item Pairing** sub-menu represented by the chain link icon:



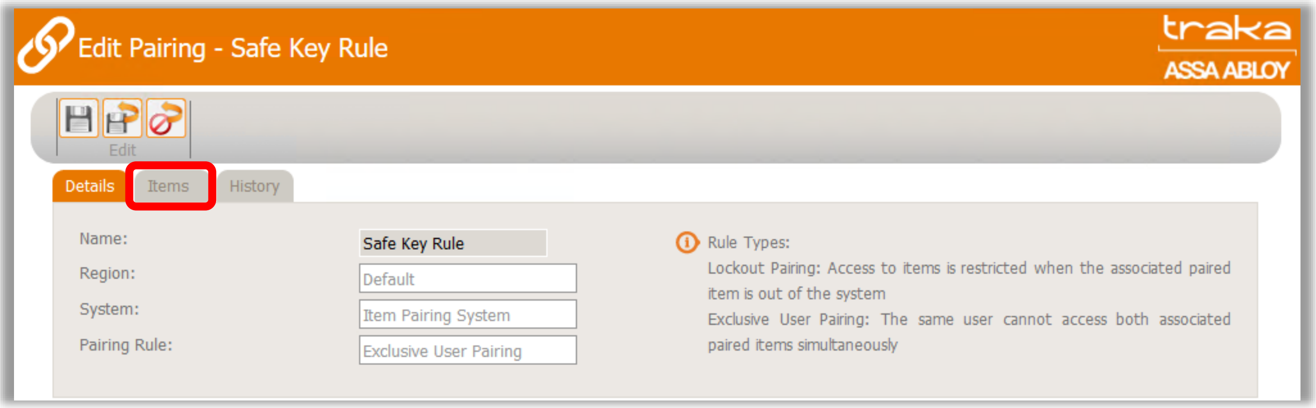
2. TrakaWEB will then display all the current Item Pairing rules that exist within the database. Select one of the existing Item Pairing rules and either click on **Edit** on the Ribbon Toolbar or double-click on the selected rule to start editing it.



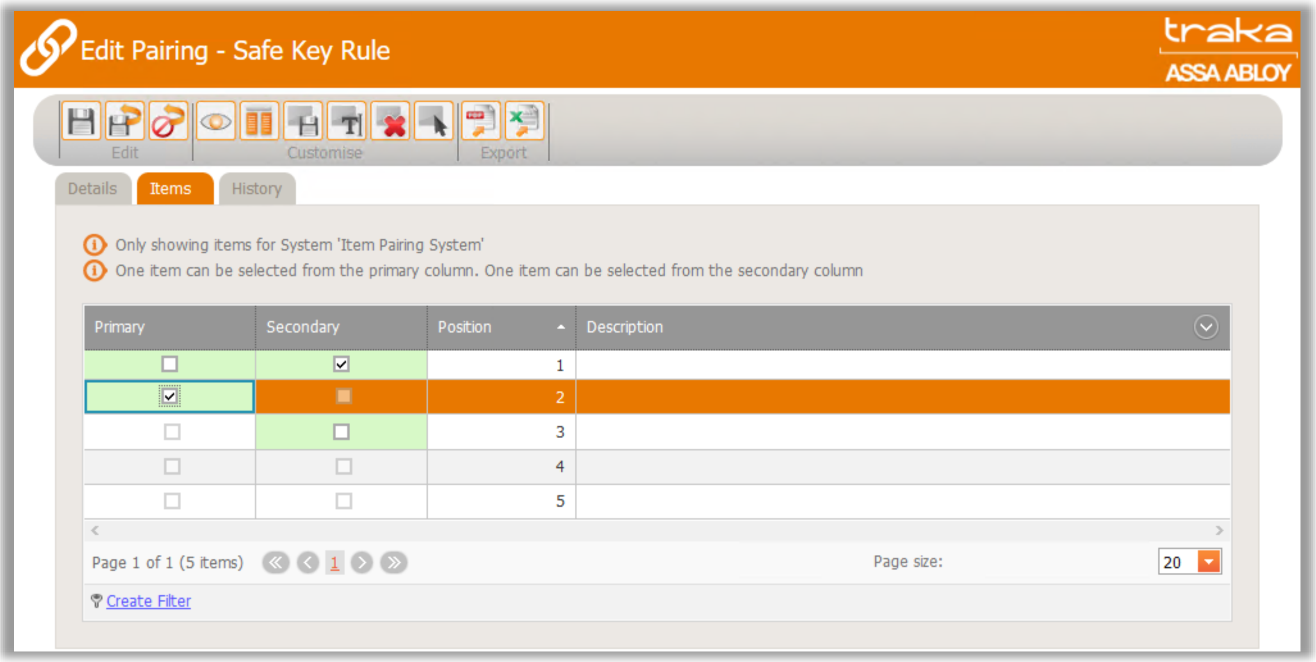
You will be redirected to the Edit Item Pairing rule **Details** page. You will notice that you cannot edit any of the Region, System, or Item Pairing Rule Type details.

NOTE: Once a rule has been created, you will not be able to change its selected Region, System, or Pairing Rule Type. If that is the case, you will need to delete the rule and create a new one instead.

3. Select the **Items** tab.



4. In the Items tab, change your selection of Primary and/or Secondary items in the Pairing Rule as required.

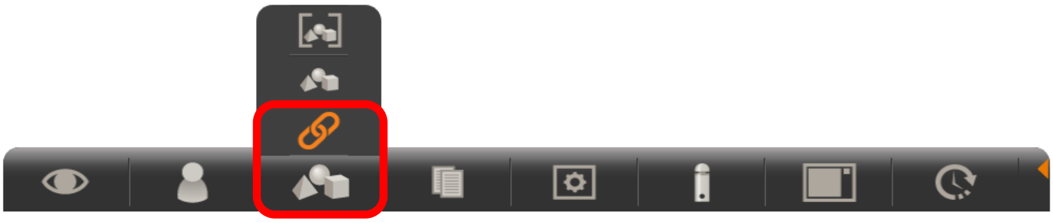


NOTE: In the Exclusive User Pairing Rule Type, you may select only one Primary and one Secondary. In the Lockout Pairing Rule Type, you may select multiple Primaries and one Secondary.

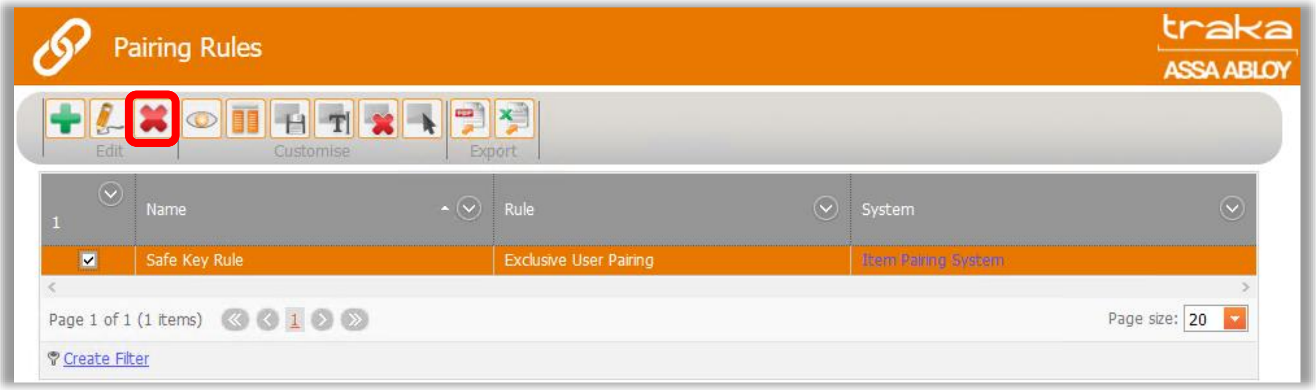
5. Click on **Save and Return**.

6.13.8 DELETE AN ITEM PAIRING RULE

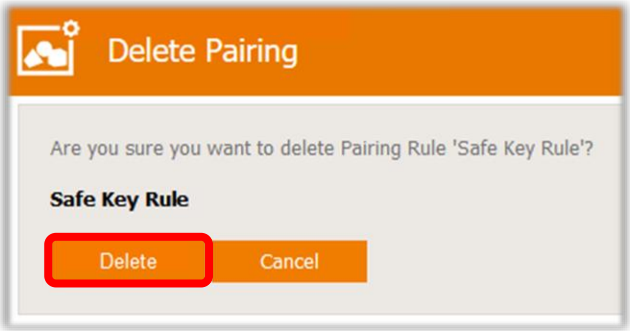
1. To delete an Item Pairing rule, select **Items** on the Navigation Toolbar. The menu will expand and reveal the **Item Pairing** sub-menu represented by the icon of chain links:



2. TrakaWEB will then display all the current Item Pairing rules that exist within the database. Select one of the existing Item Pairing rules that you wish to delete and click on **Delete** on the Ribbon Toolbar.



3. A new page will display where you will be asked to confirm the deletion of the selected Item Pairing Rule. Select **Delete**.



The rule will be deleted, and you will be taken back to the main Item Pairing menu.

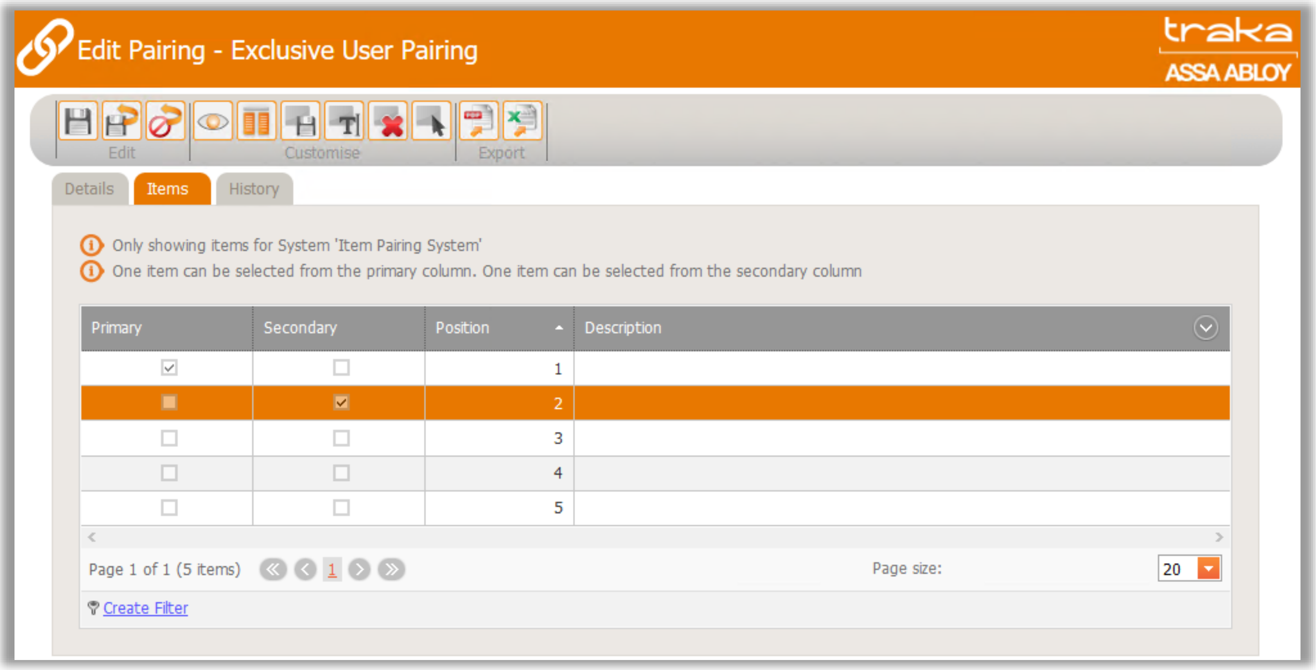
6.13.9 ITEM PAIRING ON FRSS SYSTEMS

When the Item Pairing feature is enabled on Fixed Return to Single System systems, the items associated with selected Item Pairing Rules are accessible at any time, provided that the Item Pairing Rule's conditions have been met and the user who is trying to access the items has been authorized to remove them from the affected system(s).

6.13.9.1 EXCLUSIVE USER PAIRING RULE

Setup

Once an Exclusive User Pairing Rule has been set in place in TrakaWEB, the feature will work on the selected system as soon as the synchronisation completes. In the example below, the following Exclusive User Pairing Rule has been created:

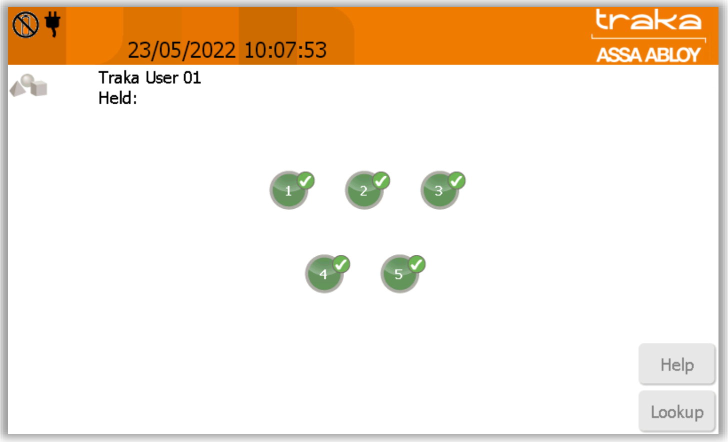


The item in Position 1 has been set as the Primary item, and the item in Position 2 has been set as the Secondary item.

Two users are registered on the system: Traka User 01 who has access to all the items stored in the system, and Traka User 02, who has only got access to the item in Position 1.

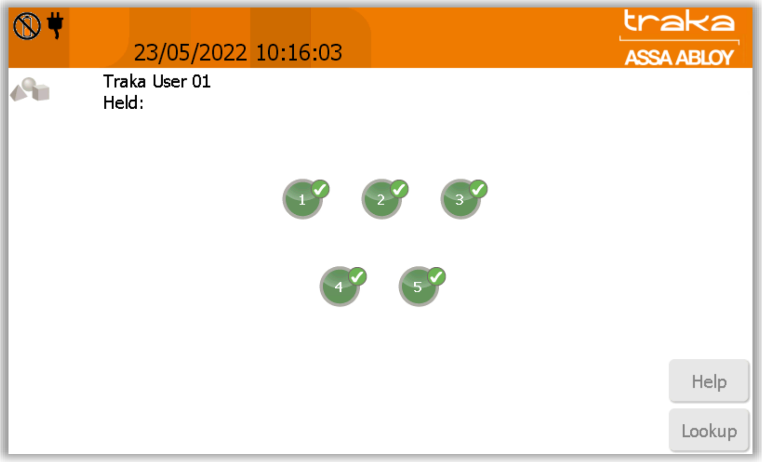
Application

1. When Traka User 01 logs into the affected Traka Touch system, they can remove any item from it. In the example below, the item in Position 1 has been chosen.



2. The moment they have taken the item from Position 1, which is the Primary item in the existing Item Pairing rule, the item in Position 2, which is the Secondary Item, will automatically become unavailable to that user.

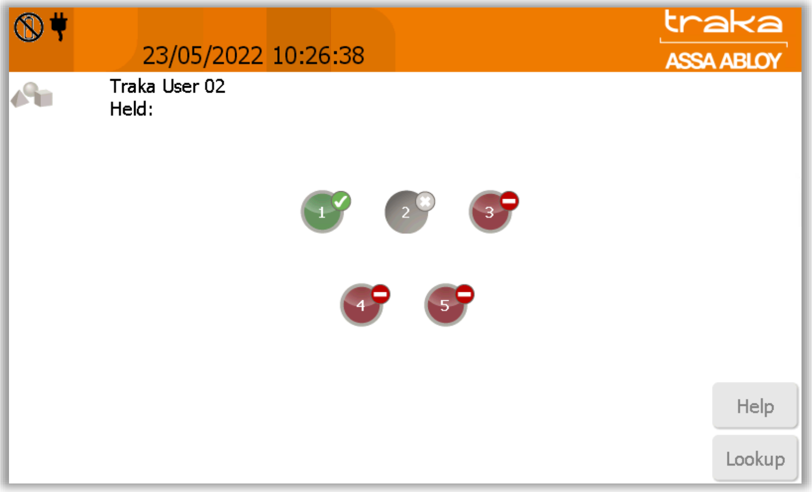
3. Traka User 01 logs in again to return the Primary Item to Position 1. Now, the Item in Position 2 becomes available to the user again.



4. If the Traka User 01 now removes the item from Position 2, the item in Position 1 will automatically become unavailable.

NOTE: This feature will prevent one user from removing both paired items from the system at any given moment and the user will need to return one item to remove the other.

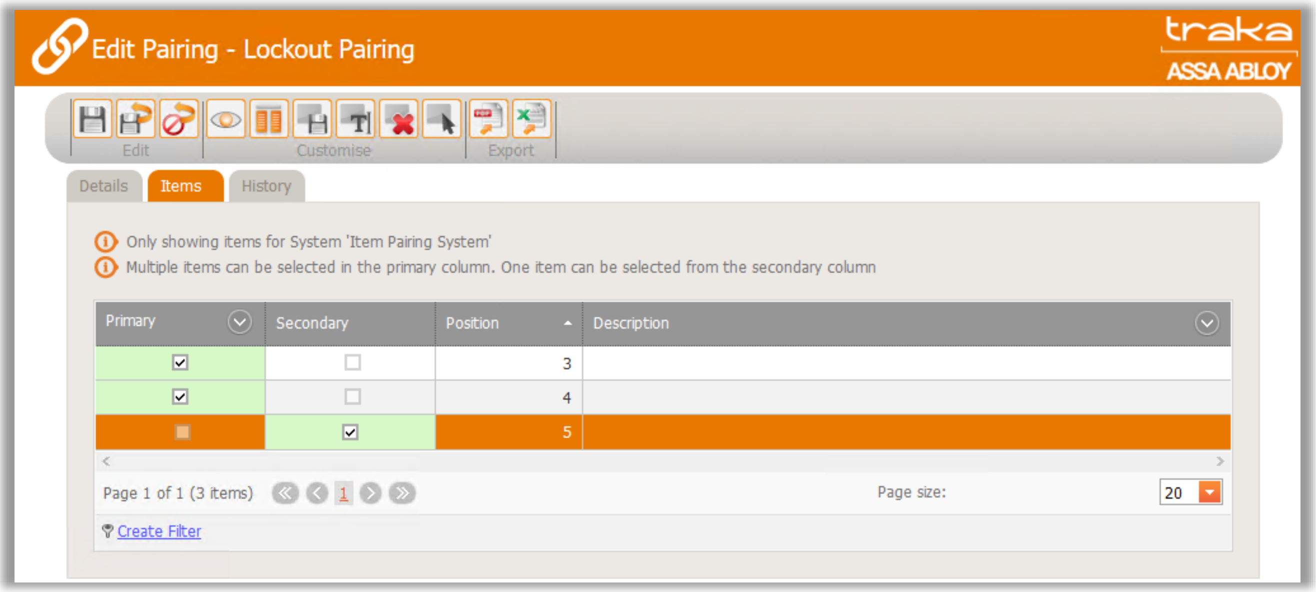
5. If the Traka User 02 logs in at that time, they will be able to remove the item from Position 1 (that is the only Item they are authorized to remove).



6.13.9.2 LOCKOUT PAIRING RULE

Setup

Once a Lockout Pairing Rule has been set in place in TrakaWEB, the feature will work on the selected system as soon as the synchronization completes. In the example below, the following Lockout Pairing Rule has been created:

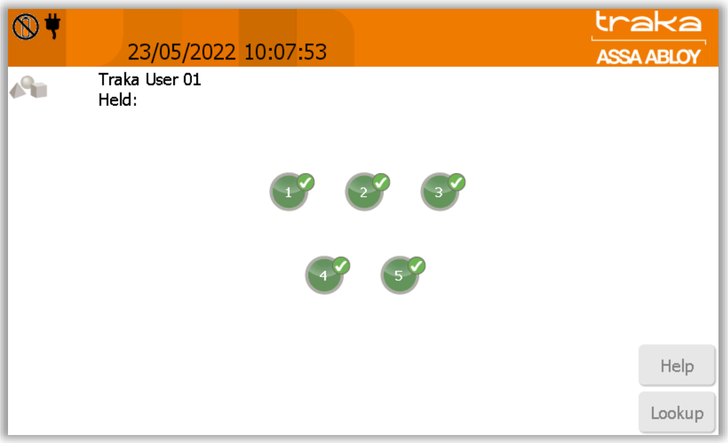


The items in Positions 3 and 4 have been set as the Primary items, and the item in Position 5 has been set as the Secondary item.

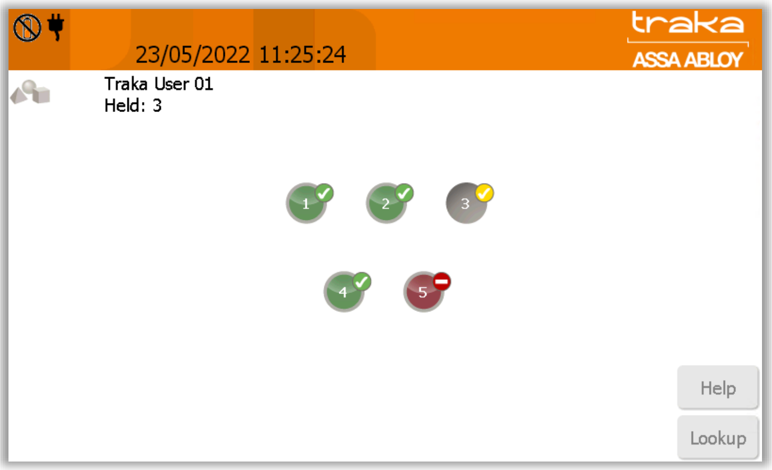
Two users are registered on the system: Traka User 01 who has access to all the items stored in the system, and Traka User 02 who has only got access to the items in Positions 4 and 5.

Application

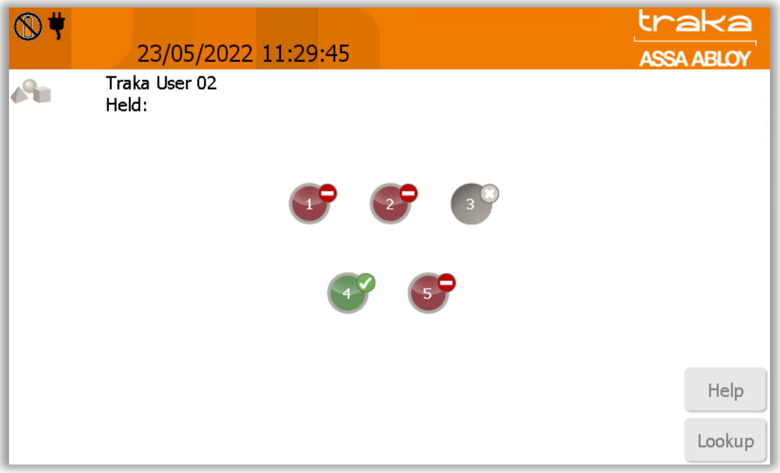
1. When Traka User 01 logs into the affected Traka Touch system, they can remove any item from it. They choose to remove the item in Position 3.



2. The moment they have taken the item from Position 3, which is one of the Primary items in the Item Pairing rule, the item in Position 5, which is the Secondary item, will automatically become unavailable, but the other Primary item in Position 4 is still available.



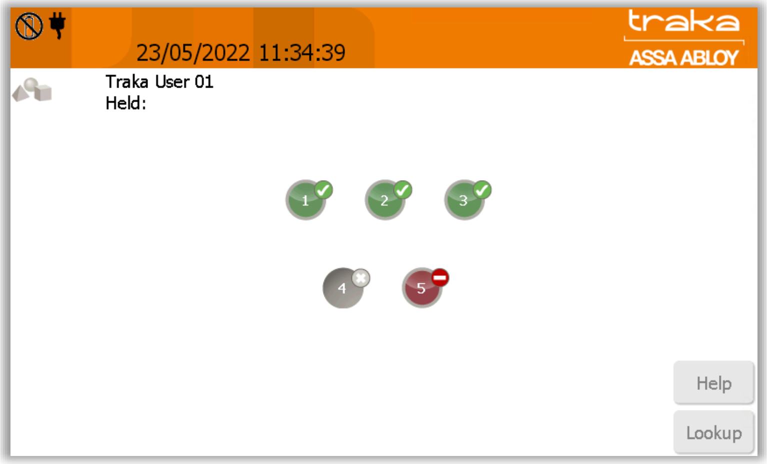
3. If the Traka User 02 logs in at that time, they will be able to remove the item in Position 4, but they will not be able to remove the item in Position 5.



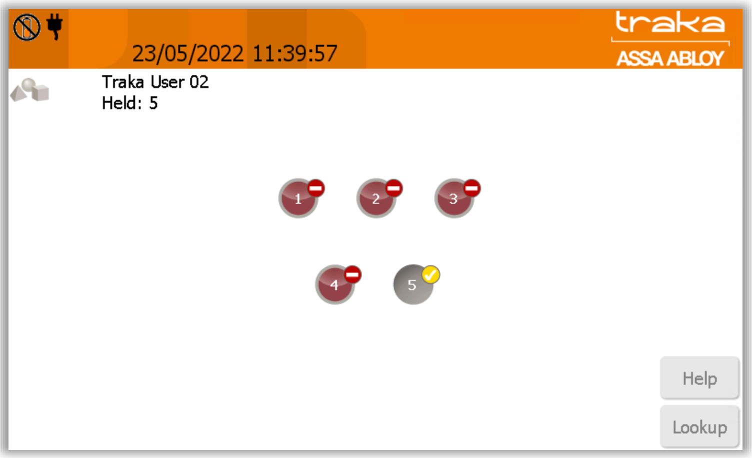
NOTE: As long as any Primary items are out of the system, the Secondary item will be unavailable, regardless of who is trying to access it.

4. Traka User 02 removes the other Primary item from Position 4.

5. When Traka User 01 logs in again and they return the item to Position 3, they will see that the Secondary item in Position 5 is still unavailable as the item in Position 4 is now out of the system. Traka User 01 logs out.

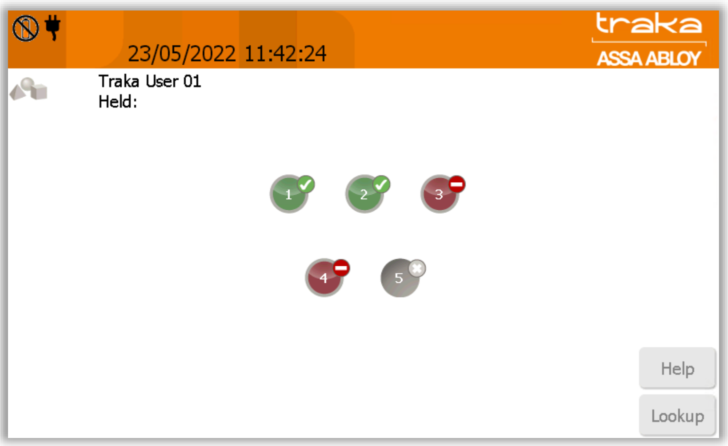


6. Traka User 02 logs in afterwards and returns the last Primary item to the system. They are now able to remove the Secondary item from Position 5. Traka User 02 removes that item.



NOTE: As long as the Secondary item is out of the system, no user can remove any of the Primary items.

7. When Traka User 01 logs into the system, they are not able to remove any of the Primary items as the Secondary item is still out of the system.



6.13.10ITEM PAIRING ON ADVANCED FIFO SYSTEMS

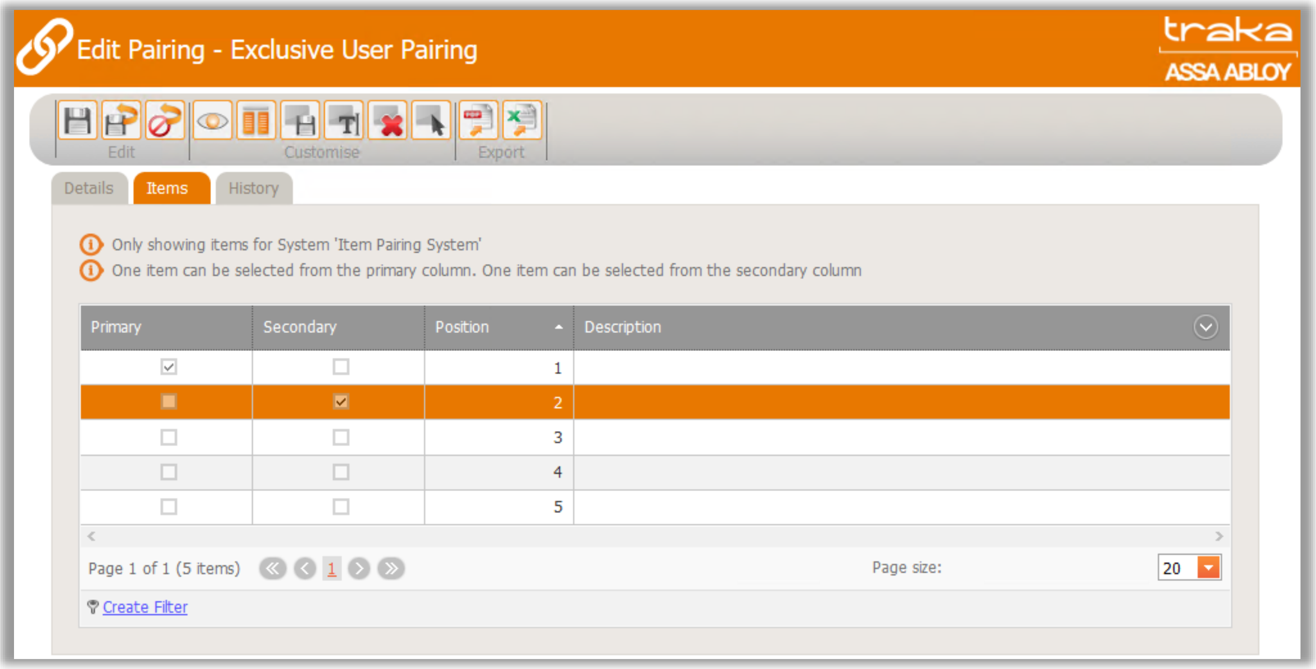
When the Item Pairing feature is enabled on Advanced FIFO systems, the items associated with selected Item Pairing Rules will follow the same rules which are in place for the Fixed Return to Single System systems, but they will also be accessible to the system users on a First In-First Out basis, provided that the Item Pairing Rule conditions have been met and the user who is trying to access items has been authorized to remove them from the affected system(s). To read more on the Advanced First In-First Out feature, please refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide**.

6.13.10.1 EXCLUSIVE ITEM PAIRING RULE

6.13.10.1.1 EXAMPLE 1 – ITEM PAIR WITHIN ONE COMMON ITEM ACCESS GROUP

Setup

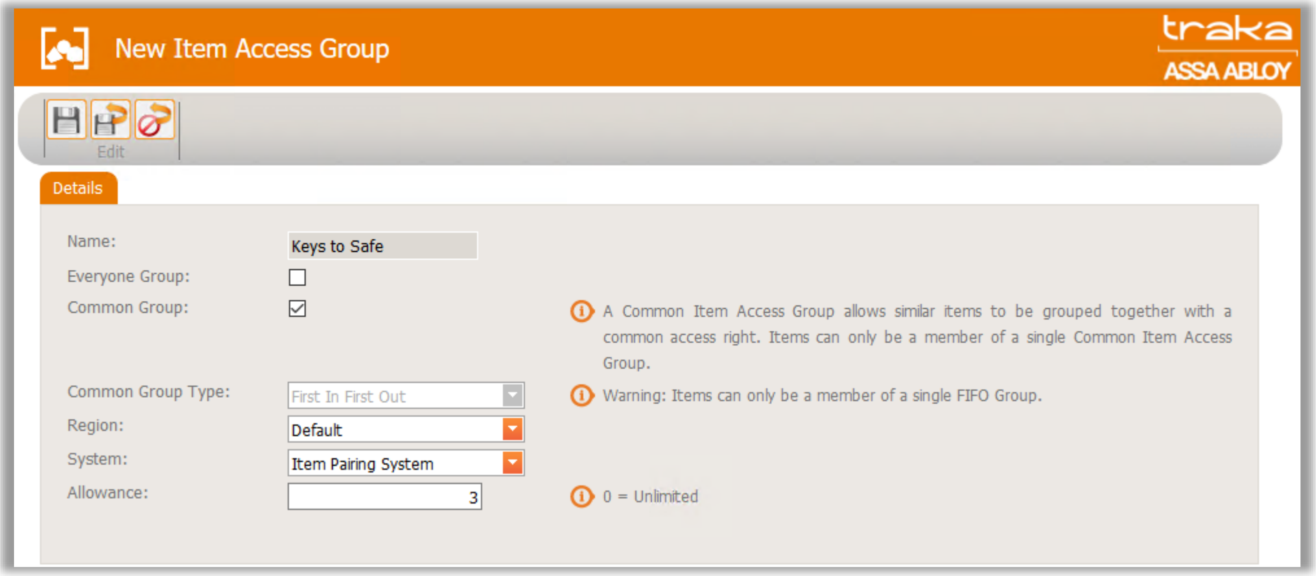
Once an Exclusive User Pairing Rule has been set in place in TrakaWEB, the feature will work on the selected system as soon as the synchronisation completes. In the example below, the following Exclusive User Pairing Rule has been created:



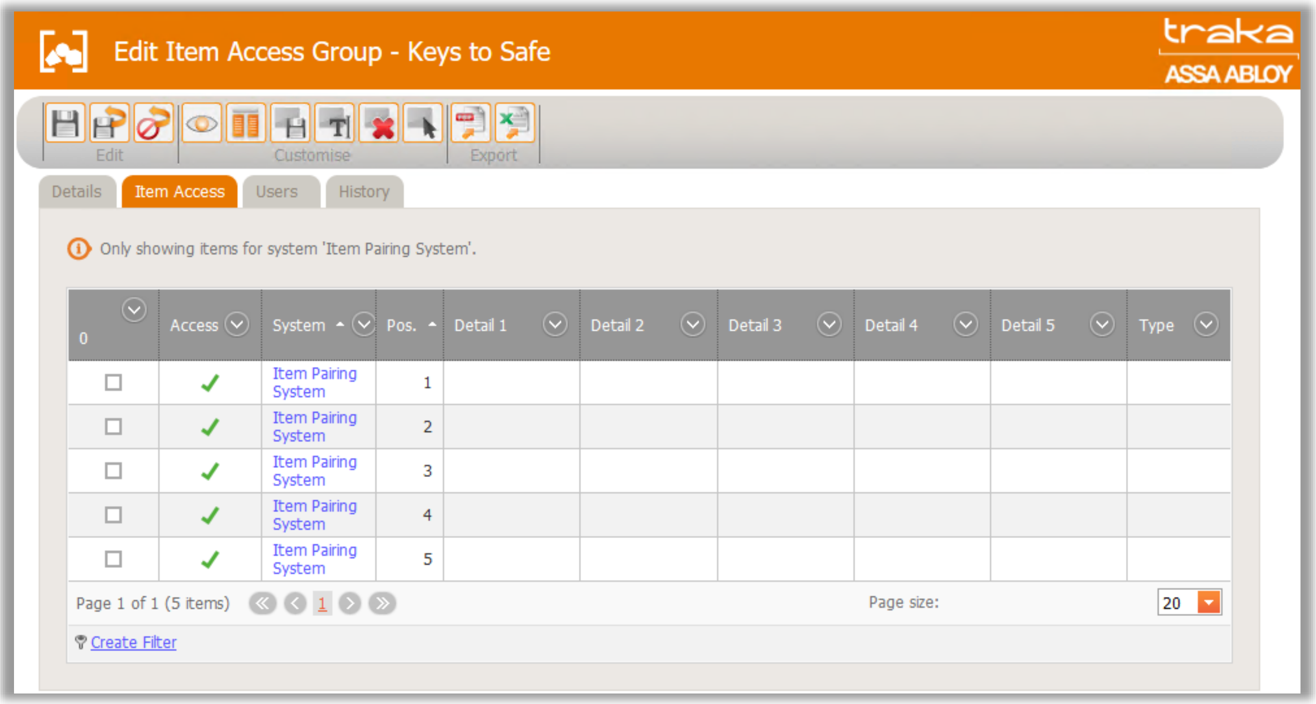
The item in Position 1 has been set as the Primary item, and the item in Position 2 has been set as the Secondary item.

Two users are registered on the system: Traka User 01 and Traka User 02.

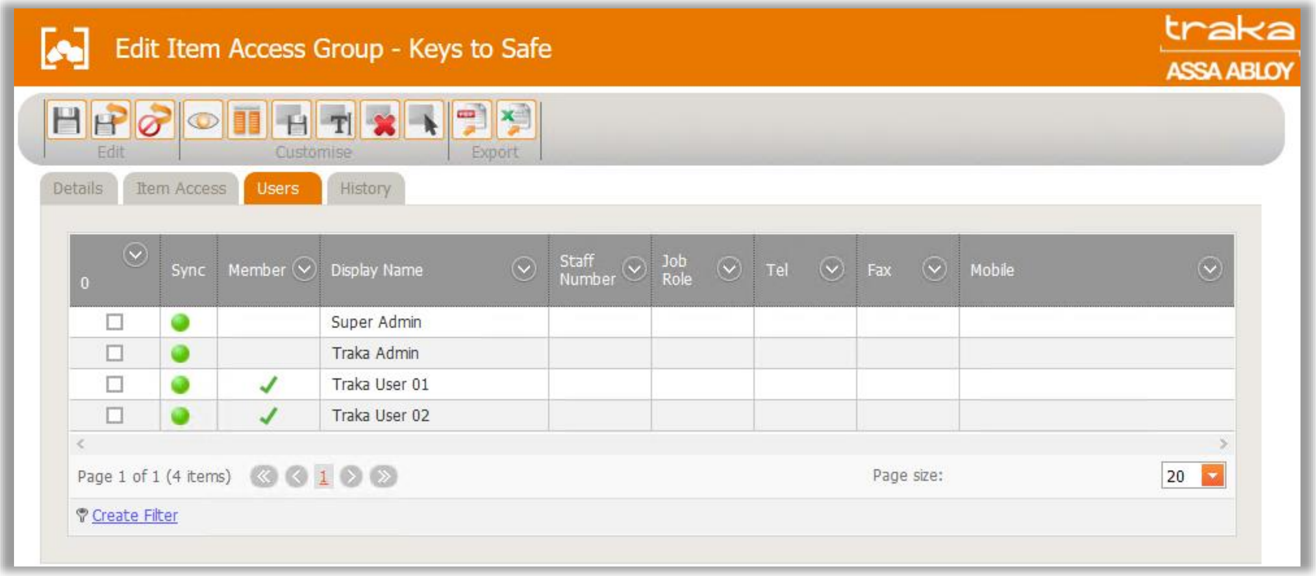
One Common Item Access Group (CIAG) has been set up for the affected system and the Item Allowance within that CIAG has been set to 3.



All 5 items from the affected system have been assigned to that Common Item Access Group.



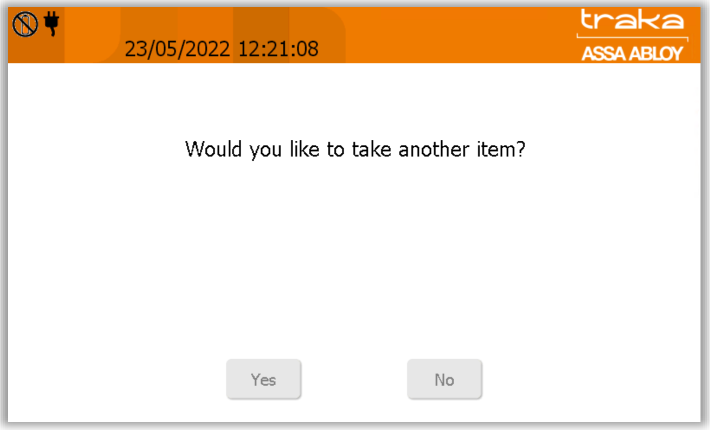
Both Traka User 01 and Traka User 02 have been made members of that CIAG.



Application

1. When Traka User 01 logs into the affected Traka Touch system, the system will automatically release the Item that has been in the system for the longest time. In this case, it is the item stored in Position 1.

2. Since the Item Allowance within this group is 3, the system asks the user if they want to remove another item from the system.



3. Traka User 01 selects Yes, and the system automatically releases the next item within that CIAG which has been in the system for the longest time, with the exception of the item in Position 2. The item in Position 2 is the Secondary item in the User Exclusive Pairing and, since Traka User 01 has already taken the Primary item from the pair, they will not be able to remove the item from Position 2, even if the item in Position 2 has been in the system for the longest amongst all the remaining items in that system. Traka User 01 will receive the next one in the queue instead.

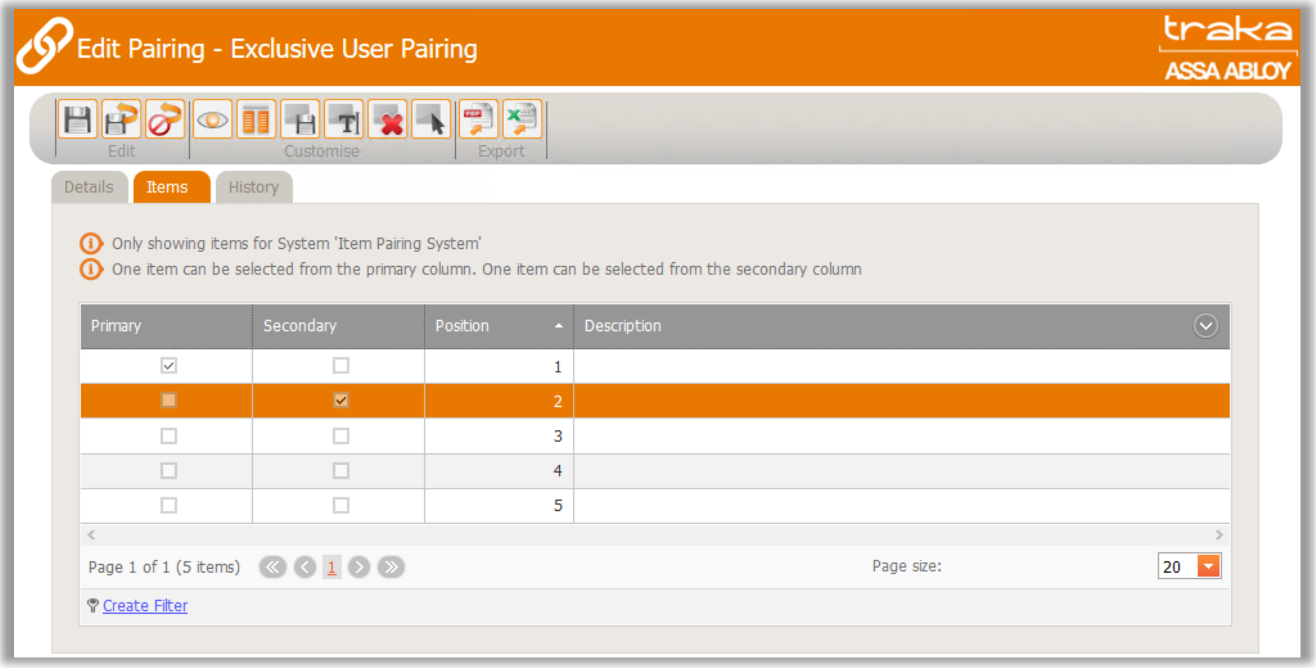
4. After taking the item from Position 3, Traka User 01 logs out.
5. When Traka User 02 logs in, the system will automatically release the item in Position 2 to them, as this is the item that has been in the system for the longest and this user does not have the Primary item from the pair that item in Position 2 belongs to.

All the other functionalities typical of the Advanced FIFO feature will apply as normal.

6.13.10.1.2 EXAMPLE 2 – ITEM PAIR DIVIDED BETWEEN TWO COMMON ITEM ACCESS GROUPS

Setup

Once an Exclusive User Pairing Rule has been set in place in TrakaWEB, the feature will work on the selected system as soon as the synchronisation completes. In the example below, the following Exclusive User Pairing Rule has been created:

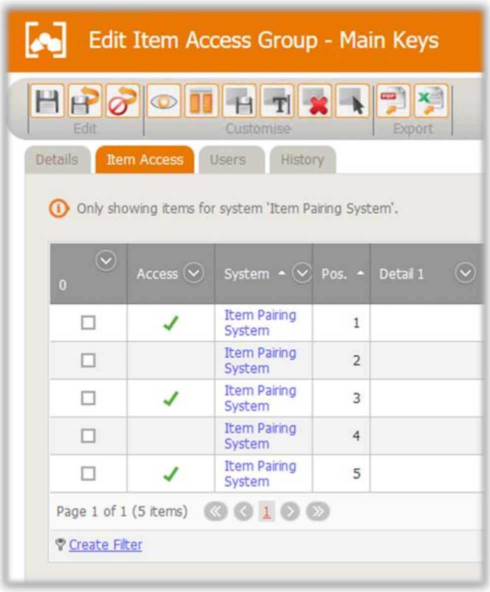


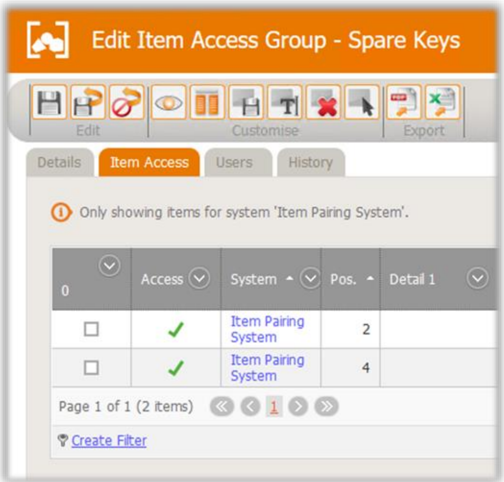
The item in Position 1 has been set as the Primary item, and the item in Position 2 has been set as the Secondary item.

Two users are registered on the system: Traka User 01 and Traka User 02.

Two Common Item Access Groups (CIAGs) have been set up for the affected system and the Item Allowance within each CIAG has been set to 2:

- Main Keys group which comprises items in Positions 1, 3, and 5
- Spare Keys group which comprises items in Positions 2 and 4.

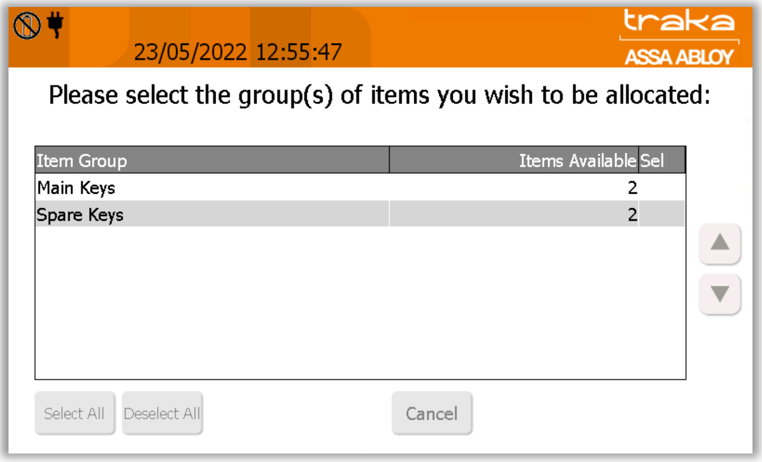




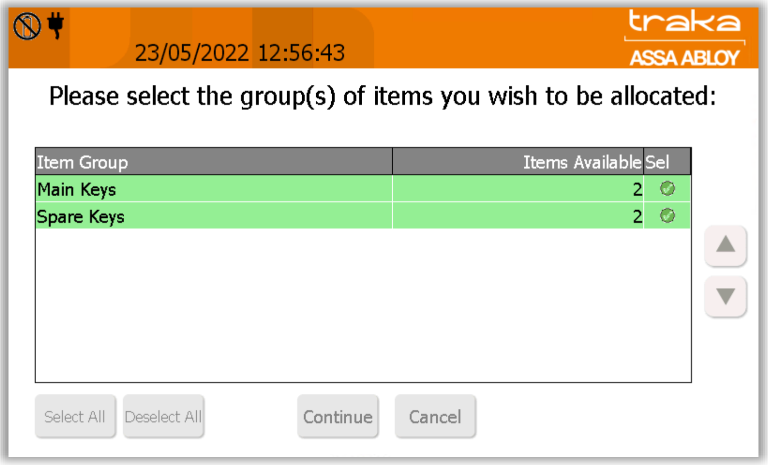
Both Traka User 01 and Traka User 02 have been assigned to both CIAGs.

Application

1. When Traka User 01 logs into the affected Traka Touch system, the system will ask which CIAGs the user needs to remove items from.



2. Traka User 01 chooses to remove items from both groups, selects them on the screen and clicks on Continue.



3. The system releases one item from the Main Keys group that has been in the system for the longest time and one item from the Spare Keys group that has been in the system for the longest time. In the example below, the system releases the items from Positions 1 and 4.

NOTE: As Traka User 01 has removed the item in Position 1 which is the Primary item in the Exclusive User Pairing Rule, the system will automatically ignore the item in Position 2 when handing out items from the

second CIAG, as in accordance with the Item Pairing rule one user cannot hold both the Primary and Secondary items simultaneously.

4. When Traka User 02 logs in and removes items from both CIAGs, the system will again release one item from each group automatically. This time, the system will release the item in Position 2 as Traka User 02 does not hold the item from Position 1 on them.

All the other functionalities typical of the Advanced FIFO will apply as normal.

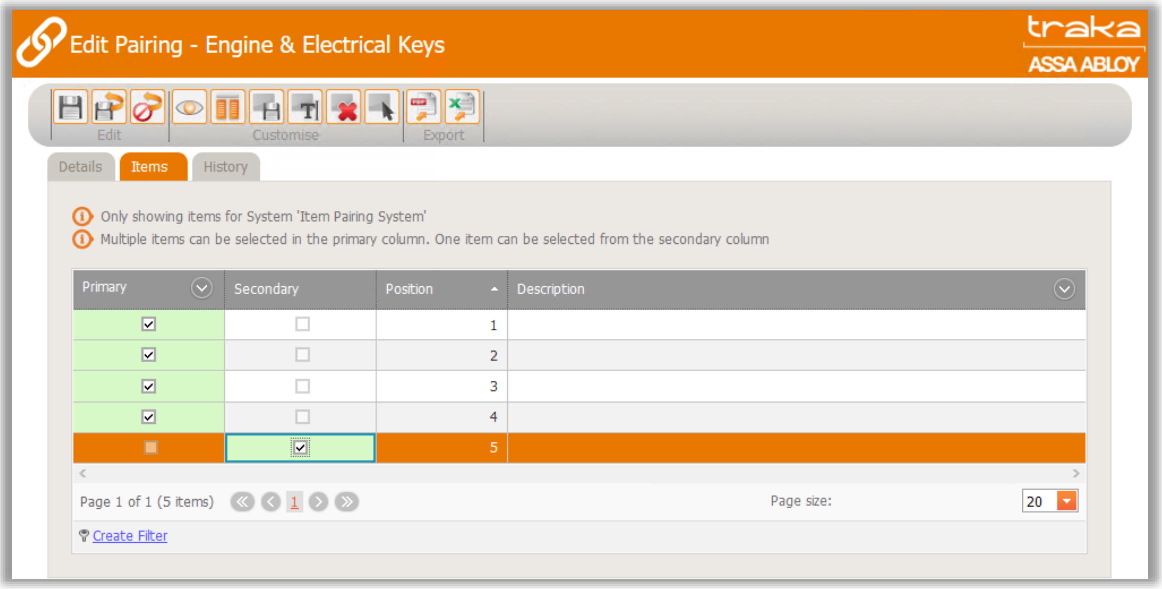
6.13.10.2 LOCKOUT PAIRING RULE

NOTE: With the Lockout Pairing Rule in place, we highly recommend assigning the Primary items into one or more CIAGs, and the Secondary Item to a separate CIAG. Although it is entirely possible to assign both the Primary items and the Secondary item into the same group, the system will be releasing them to authorized users in accordance with the First In-First Out principles. In this case, users would not be able to tell if the item they have received was one of the Primaries or the Secondary, and, if it were indeed the Secondary item, they would unknowingly block all other users from removing any of the Primaries.

6.13.10.2.1 EXAMPLE – ITEM PAIRING DIVIDED BETWEEN MULTIPLE COMMON ITEM ACCESS GROUPS

Setup

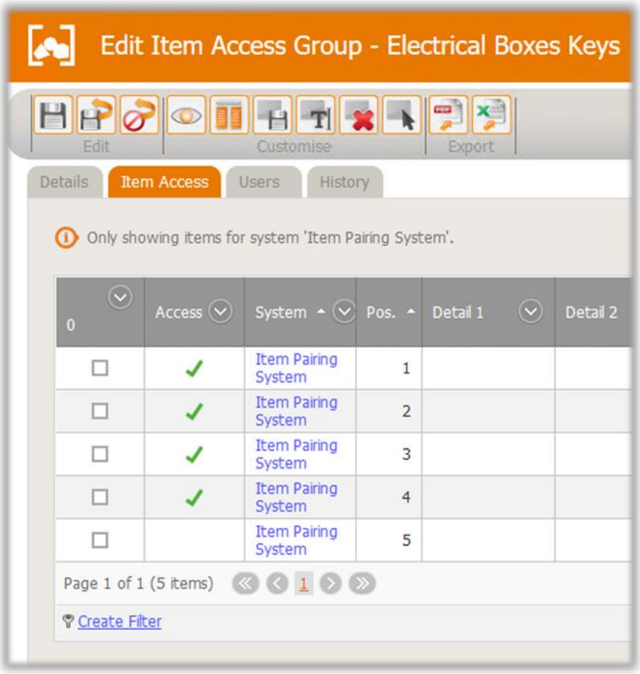
Once a Lockout Pairing Rule has been set in place in TrakaWEB, the feature will work on the selected system as soon as the synchronisation completes. In the example below, the following Lockout Pairing Rule has been set up:

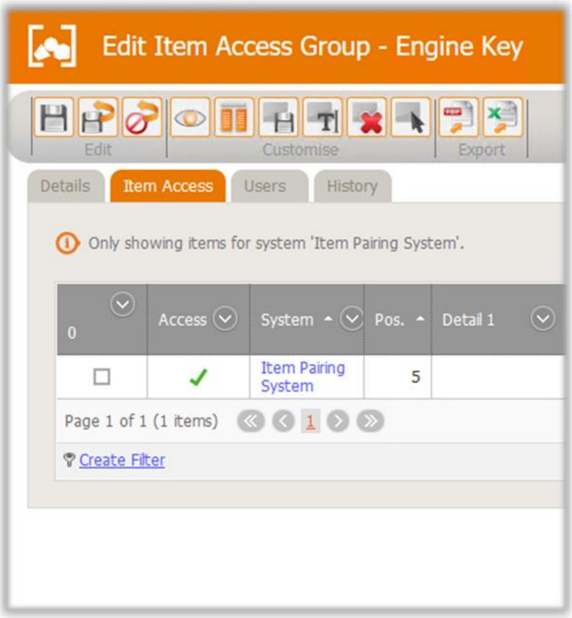


The items in Positions 1 to 4 have been set as the Primary items, and the item in Position 5 has been set as the Secondary Item.

Two Common Item Groups have been set up, one which will hold all the Primaries and the other which will hold the Secondary.

NOTE: You can divide your Primary items between multiple Common Item Access Groups as required. In the example below, all Primary items are shown as belonging to one CIAG only for simplicity. Similarly, more than one item may belong to the group containing the Secondary item. We only recommend not assigning both the Primaries and the Secondary items into the same group.

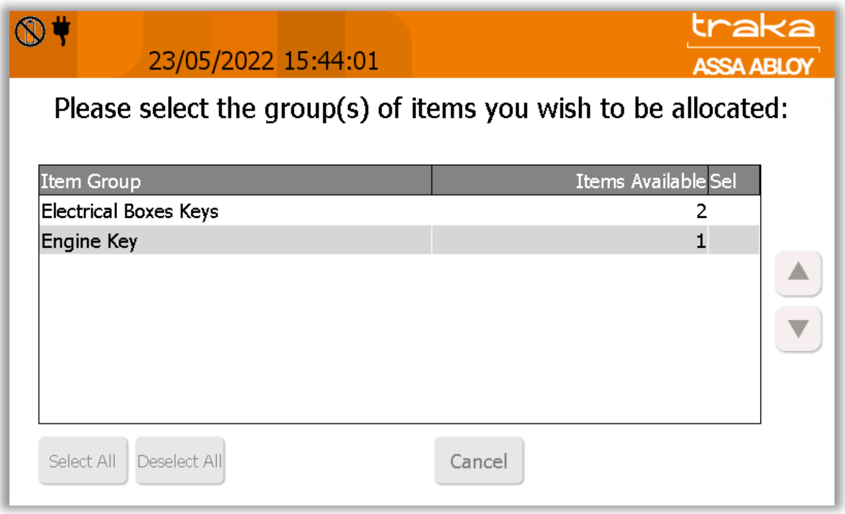




Two users have been registered on the system: Traka User 01 and Traka User 02. Both have been assigned to both CIAGs.

Application

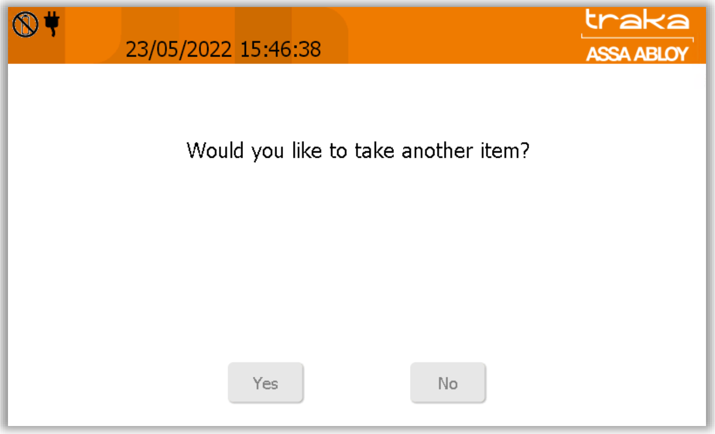
1. When Traka User 01 logs into the affected Traka Touch system, the system will ask which CIAGs the user needs to remove items from.



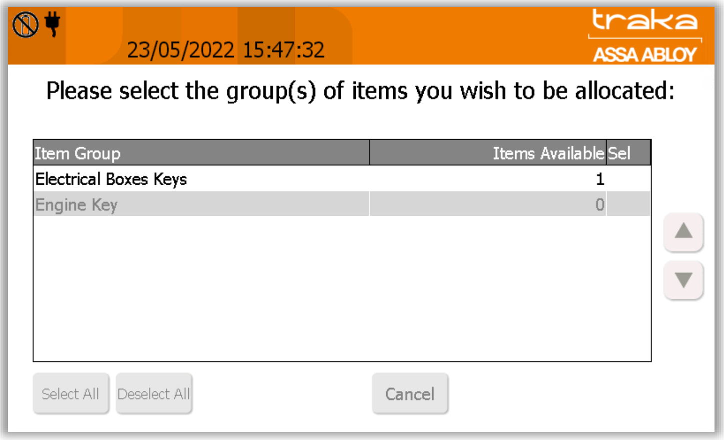
2. Traka User 01 selects the Electrical Boxes Keys (the CIAG with Primaries) and the system releases one key from that group to them. The system releases items from that group following the First In-First Out principles. In the example below, the item in Position 3 has been in the system the longest and this item will be released.

NOTE: Since Traka User 01 removed one of the Primary items, the access to the Secondary item will be automatically blocked to them and any other user.

3. Provided that the item allowance for the CIAG permits it, Traka User 01 is asked if they want to remove another item. They select Yes.

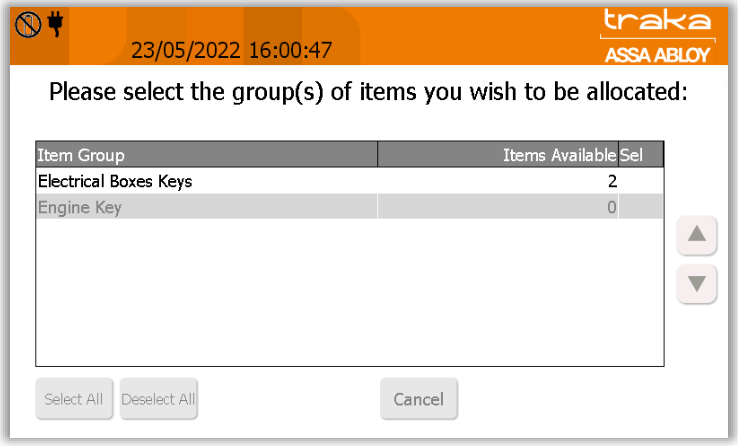


4. Traka User 01 is now taken to the CIAG selection screen where they can see that the Engine Key CIAG has become unavailable (is greyed out). This is because not all the Primaries are back in the system and the Engine Key group only contains one item, the Secondary item.



5. Traka User 01 cancels the operation and is automatically logged out.

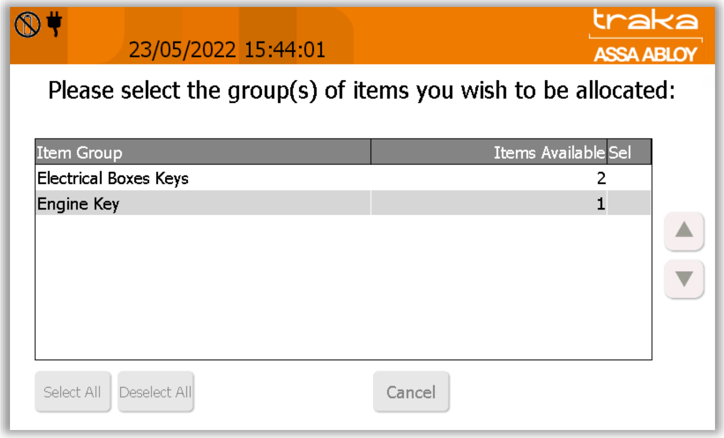
6. When Traka User 02 logs into the system, they are taken to the CIAG selection screen and will also see the Engine Key group unavailable. This is because one of the Primary items is still out of the system. Traka User 02 can only select to remove items from the Electrical Boxes Keys group. If they select that group, the system will release one item from that group in accordance with the First In-First Out principle.



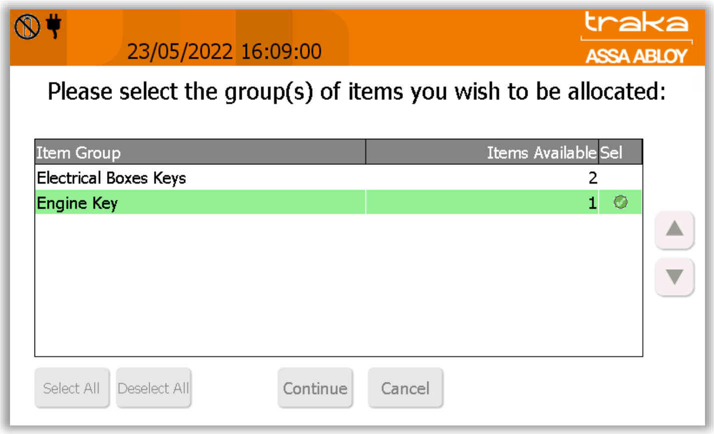
7. Traka User 02 does not remove any items and logs out.

8. Next, Traka User 01 logs in and returns one of the Primary items they have held.

9. Then Traka User 02 logs in again and they are taken to the CIAG selection screen.

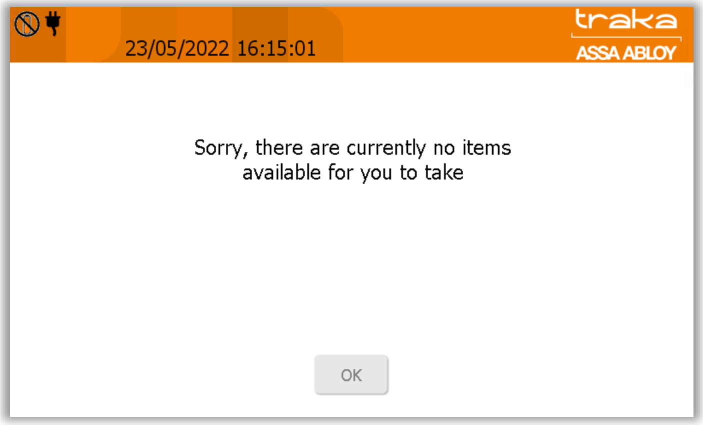


10. Since all the Primary items from the Electrical Boxes Keys group are now back in the system, Traka User 02 is allowed to remove an item from the Engine Key group.

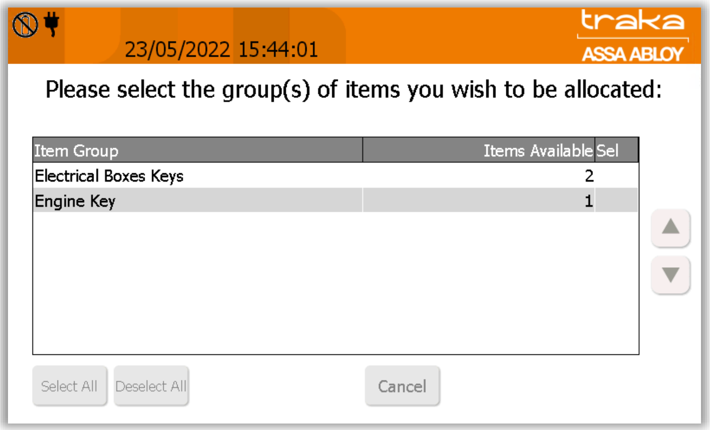


11. Since the item in the Engine Key group is the Secondary item, its removal blocks all the Primary items in the system. No user is now allowed to remove them until the Secondary item has been returned. Since the Electrical Boxes Keys CIAG consists only of the Primary items, all of them become automatically unavailable. Traka User 02 is automatically logged out.

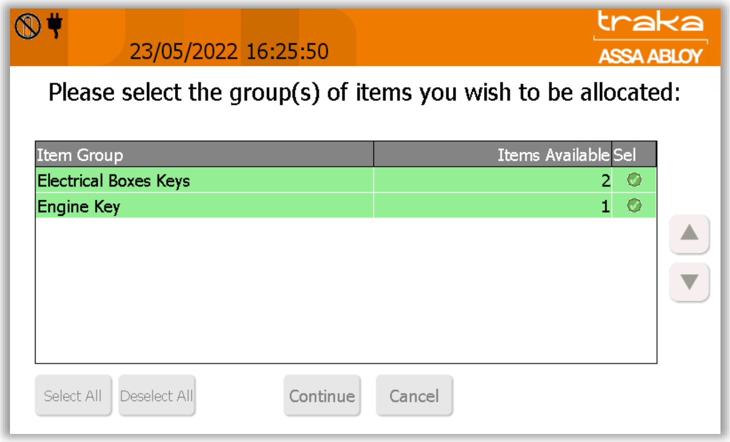
12. If Traka User 01 tries to log in then, a message will appear on screen informing them that they have been recognized but there are no items available for them to take.



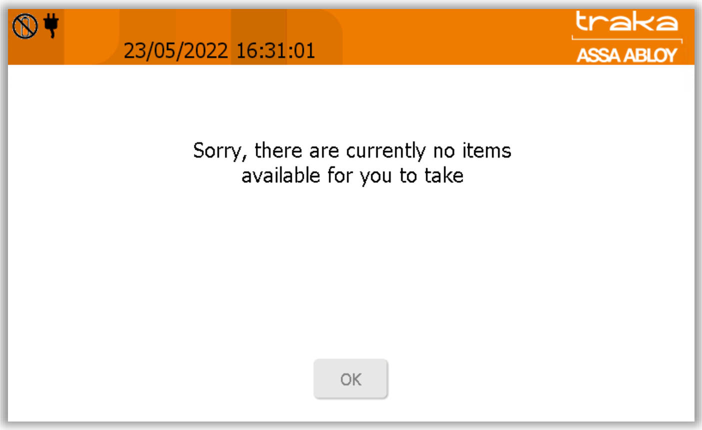
13. Once the Secondary item from the Engine Key CIAG has been returned by Traka User 02, the users regain access to the affected CIAGs.



NOTE: If a user chooses to remove items from more than one CIAG, and one of the selected CIAGs contains Primary items and another one contains the Secondary item, then the system will release the item with the smallest Position number first, regardless of which group that item belongs to, following the First In-First Out principle.



Once the first item has been removed, the system will check if the item has been associated with any Item Pairing Rules. If it was a Primary item, the system will then be unable to release the Secondary item. If it is the Secondary item, the system will be unable to release any of the Primary items. It will then show the following message.



All the other functionalities typical of the Advanced FIFO will apply as normal.

6.13.11 REMOTE RELEASE WITH ITEM PAIRING

It is not possible to Remote Release to an active user on a position that is subject to either Lockout Pairing or Exclusive User Pairing. However, a Remote Release can be applied to an anonymous user even if the selected position is subject to Item Pairing rules.

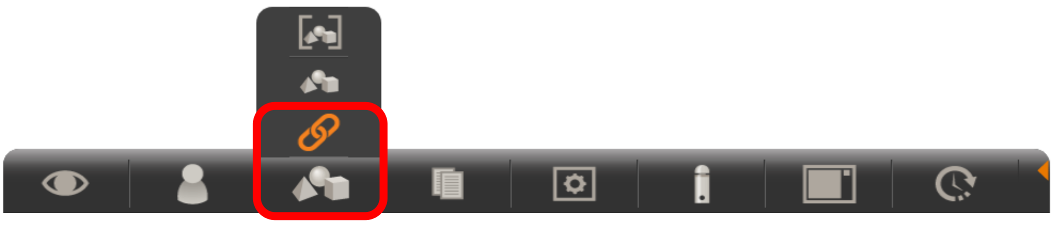
6.13.12 NO OVERRIDE FOR ITEM PAIRING

Since the Item Pairing is a security feature, for the safety of users and property there is no option available to grant users permissions to override the Item Pairing.

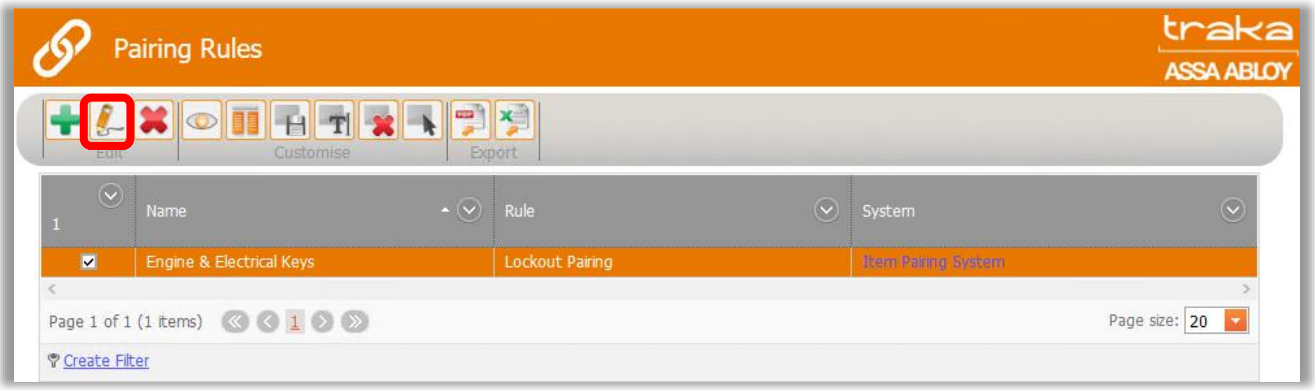
6.13.13 ITEM PAIRING HISTORY

For the purposes of audit, all the changes in the Item Pairing Rules are recorded in the History tab for each Item Pairing rule.

1. To access the History tab for your chosen Item Pairing Rule, select **Items** on the Navigation Toolbar. The menu will expand and reveal the **Item Pairing** sub-menu represented by the chain link icon:

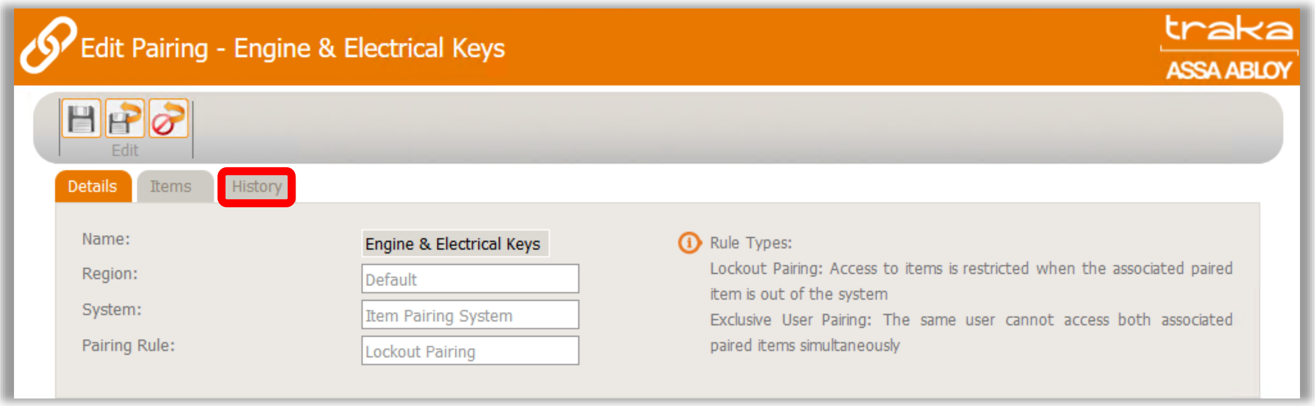


2. TrakaWEB will then display all the current Item Pairing rules that exist within the database. Select one of the existing Item Pairing rules and either click on **Edit** on the Ribbon Toolbar or double-click on the selected rule to start editing it.

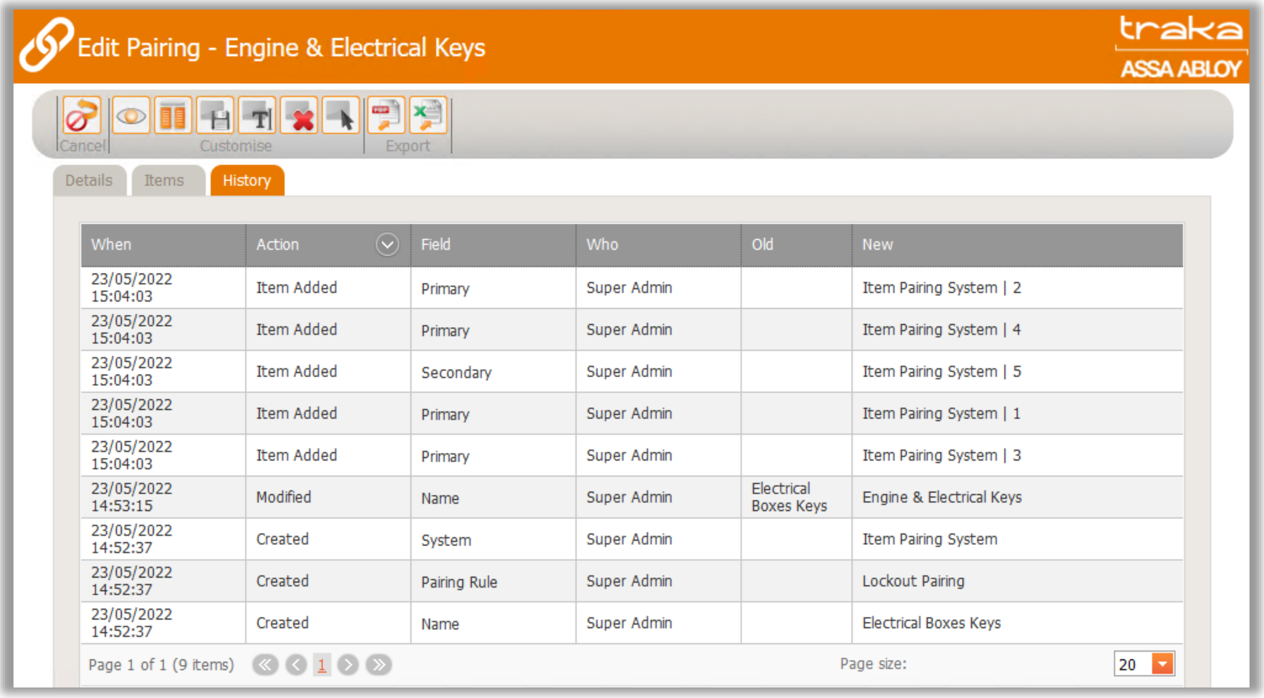


You will be redirected to the Edit Item Pairing rule **Details** page.

3. Select the **History** tab.



You will then see the recorded history of all the changes to that Item Pairing Rule.

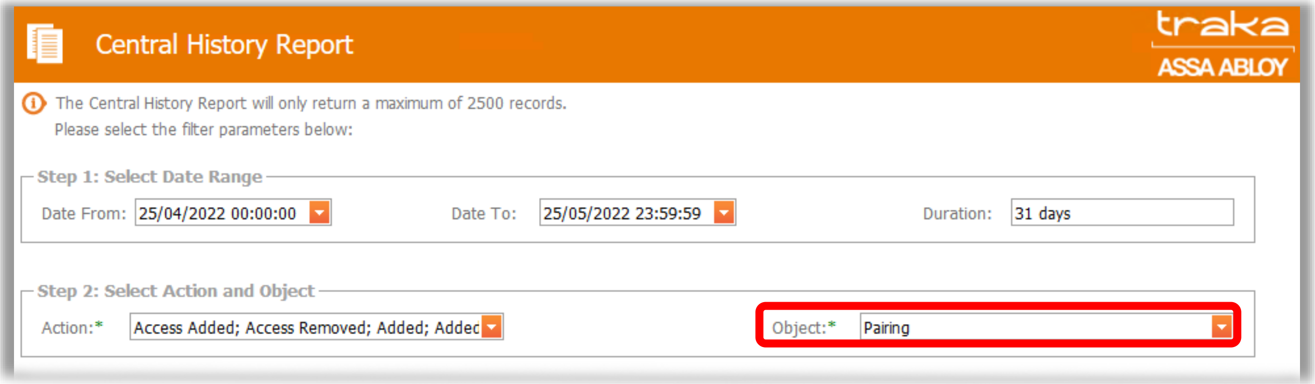


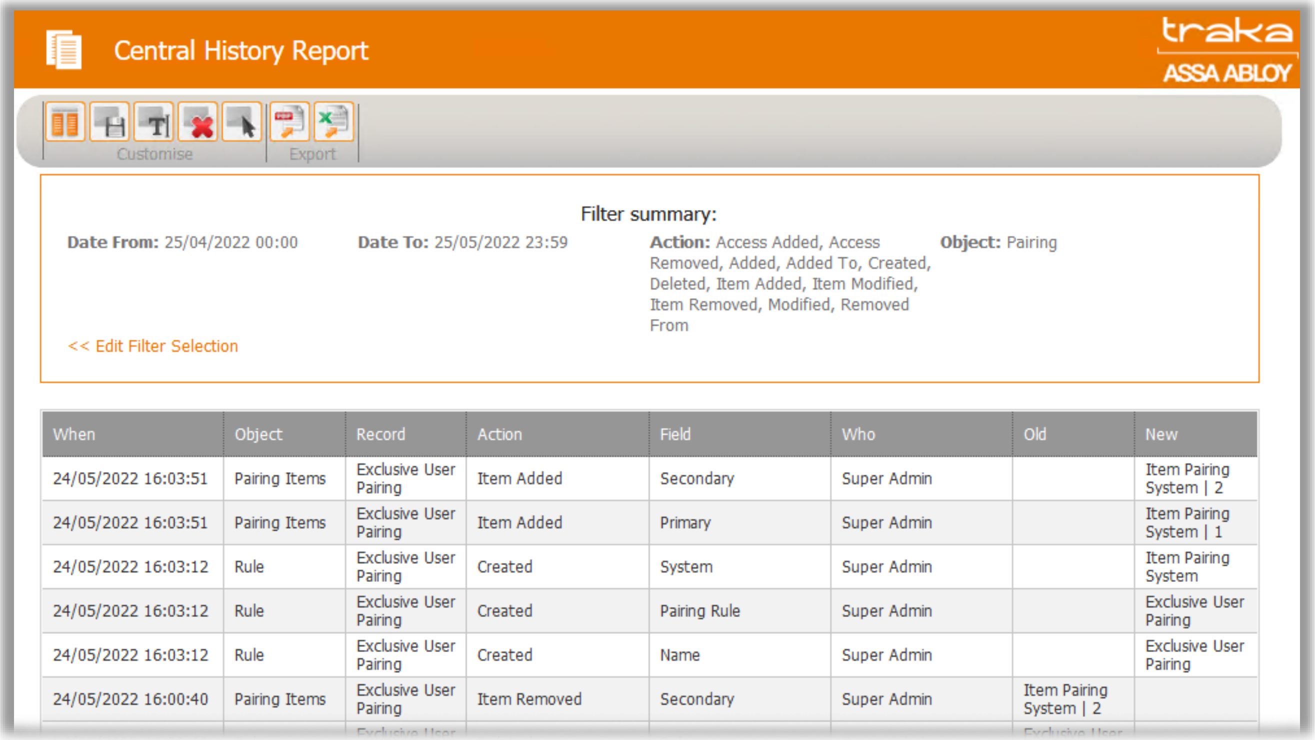
When	Action	Field	Who	Old	New
23/05/2022 15:04:03	Item Added	Primary	Super Admin		Item Pairing System | 2
23/05/2022 15:04:03	Item Added	Primary	Super Admin		Item Pairing System | 4
23/05/2022 15:04:03	Item Added	Secondary	Super Admin		Item Pairing System | 5
23/05/2022 15:04:03	Item Added	Primary	Super Admin		Item Pairing System | 1
23/05/2022 15:04:03	Item Added	Primary	Super Admin		Item Pairing System | 3
23/05/2022 14:53:15	Modified	Name	Super Admin	Electrical Boxes Keys	Engine & Electrical Keys
23/05/2022 14:52:37	Created	System	Super Admin		Item Pairing System
23/05/2022 14:52:37	Created	Pairing Rule	Super Admin		Lockout Pairing
23/05/2022 14:52:37	Created	Name	Super Admin		Electrical Boxes Keys

Page 1 of 1 (9 items) Page size: 20

6.13.14ITEM PAIRING IN TRAKAWEB REPORTS

All the events related specifically to the Item Pairing Rules will be visible in the Central History Report. You can also create a Central History Report and specifically choose **Pairing** as the Object for the report. To read more on how to generate such a report, please refer to the Central History Report section in this document.

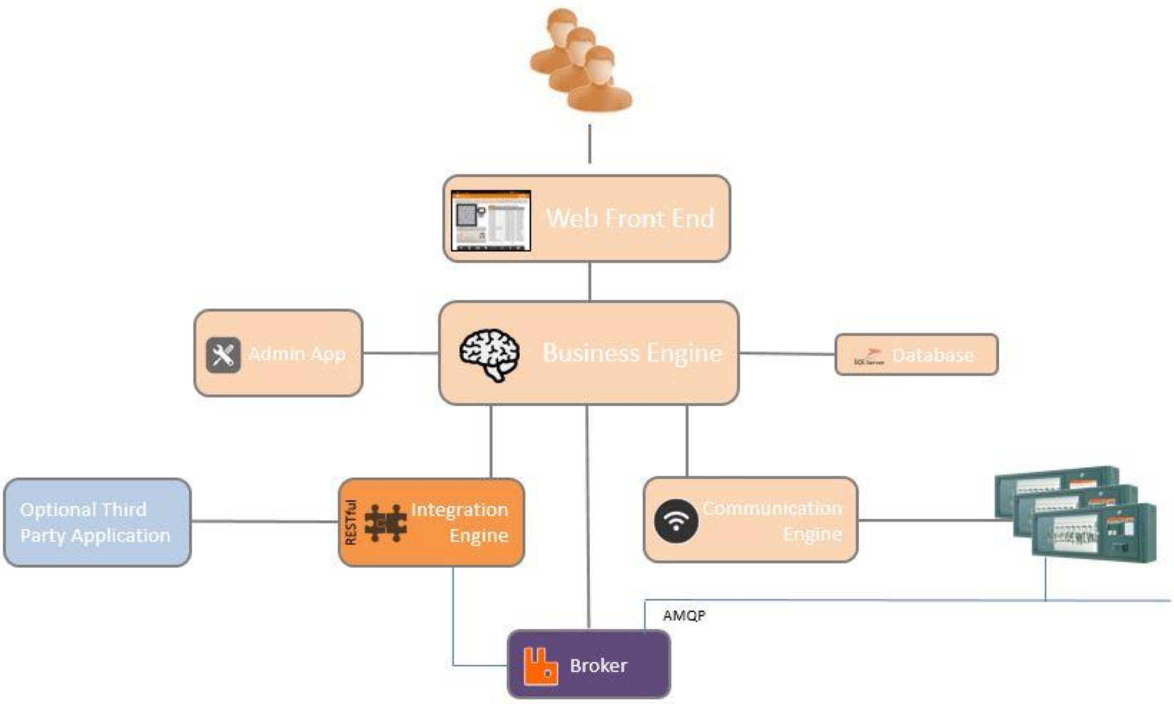




When	Object	Record	Action	Field	Who	Old	New
24/05/2022 16:03:51	Pairing Items	Exclusive User Pairing	Item Added	Secondary	Super Admin		Item Pairing System | 2
24/05/2022 16:03:51	Pairing Items	Exclusive User Pairing	Item Added	Primary	Super Admin		Item Pairing System | 1
24/05/2022 16:03:12	Rule	Exclusive User Pairing	Created	System	Super Admin		Item Pairing System
24/05/2022 16:03:12	Rule	Exclusive User Pairing	Created	Pairing Rule	Super Admin		Exclusive User Pairing
24/05/2022 16:03:12	Rule	Exclusive User Pairing	Created	Name	Super Admin		Exclusive User Pairing
24/05/2022 16:00:40	Pairing Items	Exclusive User Pairing	Item Removed	Secondary	Super Admin	Item Pairing System | 2	

6.14 REAL-TIME UPDATE SERVICE (RTUS)

The Real-Time Update Service is a cost option feature that will provide Real-Time State Change information from Traka Touch to the Integration Engine v2 using a Message Broker on a system-by-system basis.



This in turn will provide events in real-time to a third-party application based upon the current status of the items held by the user which in turn can grant or revoke access rights to or from a user within a third-party application when Item State Changes are detected via RTUS. An example could be, preventing a user from leaving site if they have not returned keys or assets.

The Comms status is monitored continually, and email notifications can be sent if one or more components that make up RTUS should fail. For example:

- The Traka Touch System goes offline
- The Message Broker goes offline
- The Integrated Engine v2 goes offline

RTUS will work with the following products:

- Traka Touch Key Cabinets (locking & non-locking strips)
- Traka Touch Lockers with RFID
- Traka Touch Lockers with RFID & FIFO
- Other optional features such as Fault Logging, Fuel, Distance & Location, Item Booking

RTUS is not compatible with 16bit Systems or Traka Touch Lockers without RFID.

For more information regarding the setup and configuration of RTUS, please refer to **TD0165 – Real Time Update Service Setup & Configuration Guide.**

6.15 SCHEDULED REPORTS

6.15.1 SCHEDULED REPORTS OVERVIEW

The Filtered Reports/Scheduled Reports is a none cost option feature that may be setup by the user as required. A Filtered Report can be configured by the end-user and then combined with the Scheduled Reports feature.

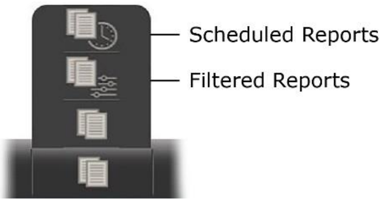
A maximum of 500 reports maybe created, and once configured, the Scheduled Report can be submitted as an email notification in either PDF or Excel format.

The Email notification will need to be configured in the Business Engine before it is usable in TrakaWEB. For detailed information on how to configure this, please review the 'Email Configuration' section in the latest version of the **TrakaWEB Installation & Configuration Guide – TD0013.**

For more information on the setup and configuration of Scheduled Reports, please refer to **TD0013 – TrakaWEB Installation & Configuration Guide.**

Whilst both Filtered and Scheduled Reports may be configured separately, both will be required to be effective. They also both have their own individual permissions in the Software Permissions Groups.

The option for selecting both Filtered Reports and Scheduled Reports is located on the Navigation Toolbar within the Reports tab.



The Scheduled Reports feature may be configured to periodically submit Filtered Reports by email. Examples include:

- Current Item Status Reports
- Activity Reports
- Overdue Reports
- Curfew Item Status Reports

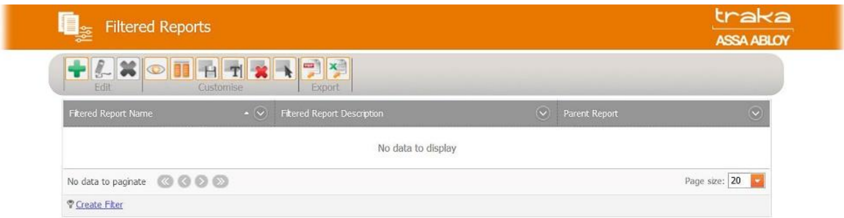
Whilst Scheduled Reports requires many of the same installation requirements as RTUS, the Integration Engine is not used, but an additional Reporting Engine is provided with the installation files.

6.16 FILTERED REPORTS

Filtered Reports are configured separately from Scheduled Reports, they will however require a Scheduled Report to be created for submission. Configuration of Filtered Reports is divided into 7 steps.

3. To create a Filtered Report. Select the **Filtered Reports** icon from the Reports tab on the Navigation Toolbar.

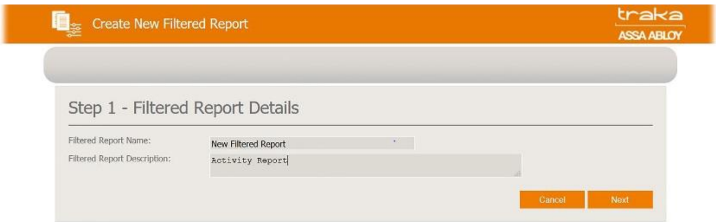
You will now be taken to the Filtered Reports Landing Page.



4. To create a new Filtered Report click **Create**  on the Ribbon Toolbar.

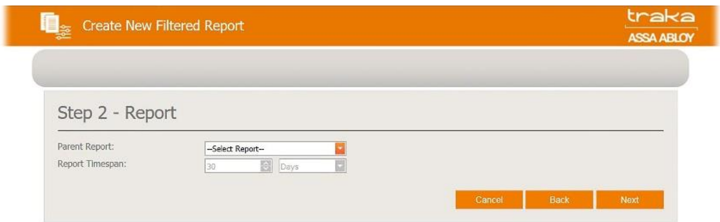
Step 1 – Filtered Report Details

3. At the **Filtered Report Details** page, complete the details as shown in the example below. Once completed, click on **Next.**

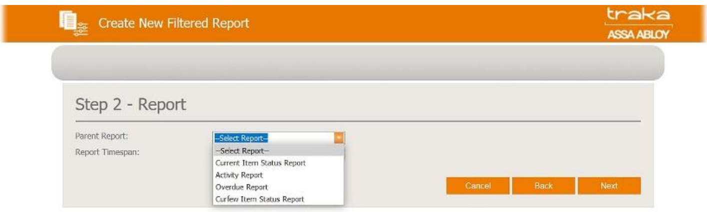


Step 2 - Report

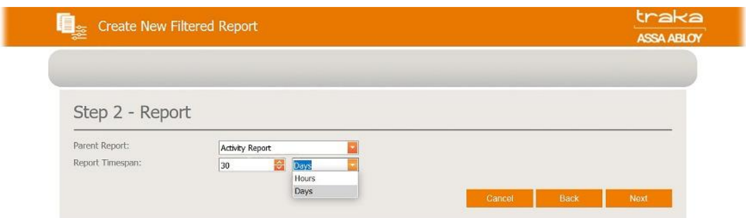
The next step will require you to select the Parent Report and the Report Timespan.



4. From the drop down menu, select the required report.



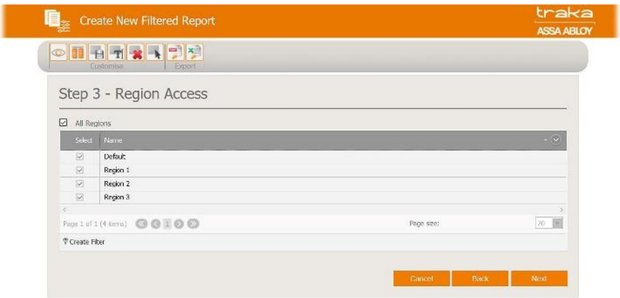
5. Next, use the arrow buttons to select a timespan. The default is set to 30 days. The timespan may also be changed from days to hours as required.



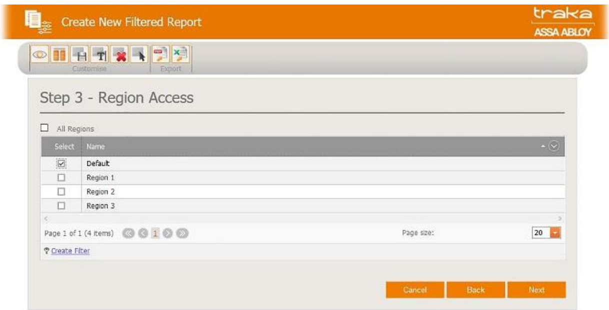
6. Once you have made your selection, click on **Next** to continue.

Step 3 - Regions

The next step will require you to select from your list of available regions. By default, all regions will be selected.



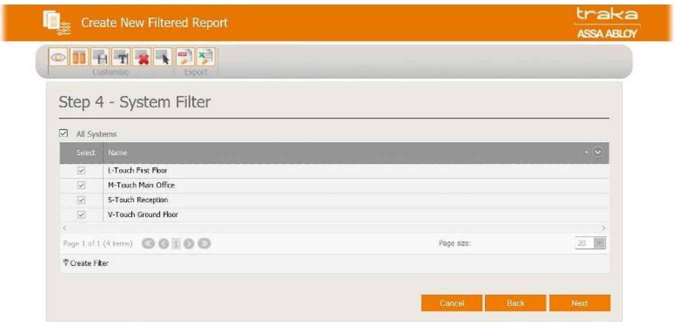
Deselecting the **All Regions** check box will enable you to select regions individually.



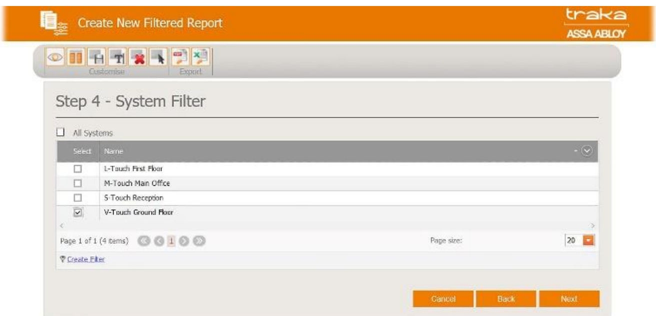
7. Once you have completed your region selection, click on **Next** to continue.

Step 4 – System Filter

At the next page, you will be required to select from the list of available systems. By Default, all the available systems will be selected.



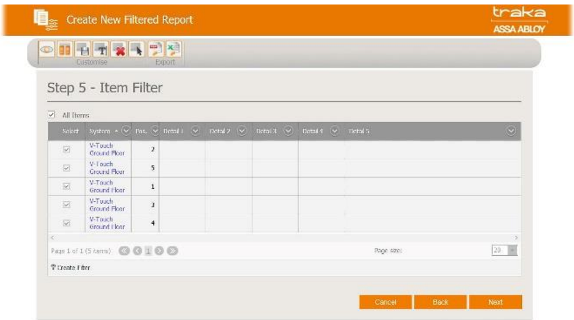
By deselecting the **All Systems** check box, you can select systems individually.



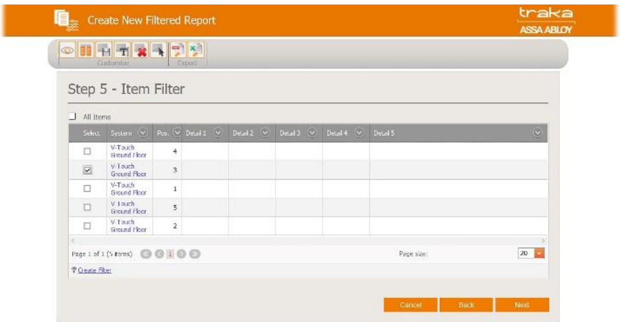
8. Once you have selected the required systems, click on **Next** to continue.

Step 5 – Item Filter

The next page will require you to choose which items you wish to add to the filter. The default setting is for all available items to be selected as shown.



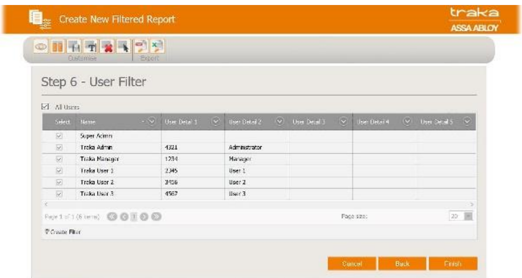
By deselecting the **All Items** check box, you can select items individually.



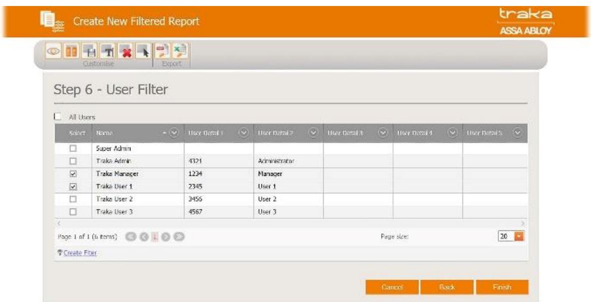
9. Once you have selected the required items, click on **Next** to continue.

Step 6 – User Filter

At the **User Filter** page, you will be required to select from the list of available users. By default, all available users will be selected.



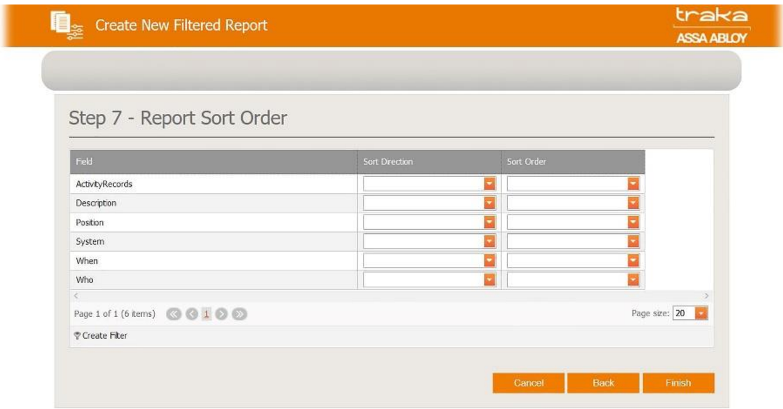
By unchecking the **All Users** check box, available users may be selected individually.



10. Once you have completed the User selection, click on **Finish** to complete the process.

Step 7 – Report Sort Order

The **Report Sort Order** page will enable you to arrange the filtered report according to your requirements. It comprises of 2 customisable sections based on the selections made in the previous steps.

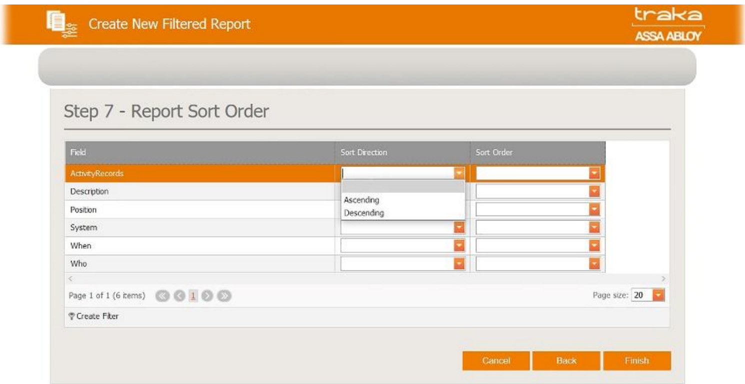


Field

The Field comprises of a list of 6 report options. These are based on the Filtered Report chosen in step 2

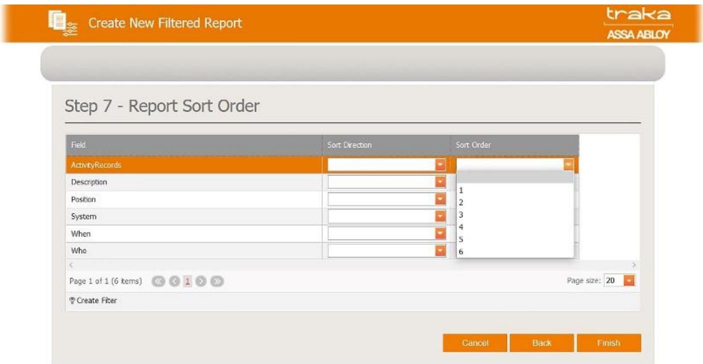
Sort Direction

The Sort Direction will enable you to choose between ascending and descending from the drop down menus.



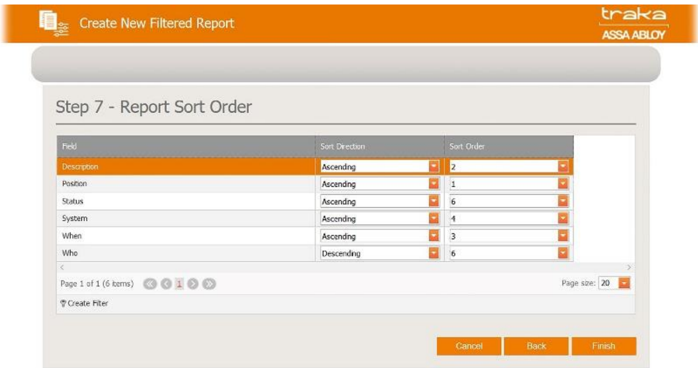
Sort Order

The Sort Order will enable you to set the order that you would like the report to be presented. From the drop-down menus, you are able to change the number value from between 1 – 6.

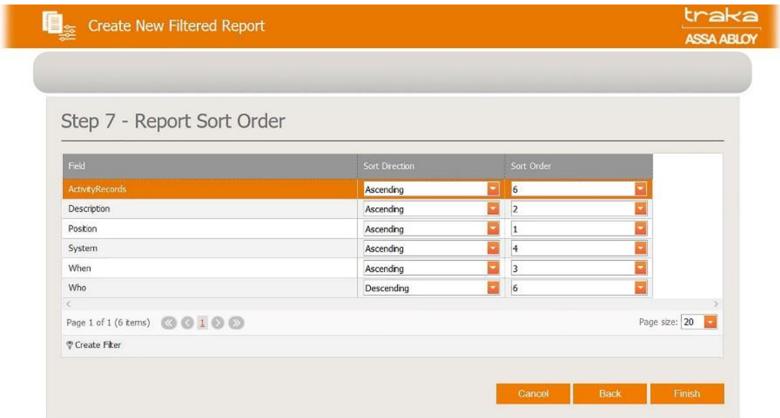


The following examples typically show the Field options based on the available selected Filtered Report options.

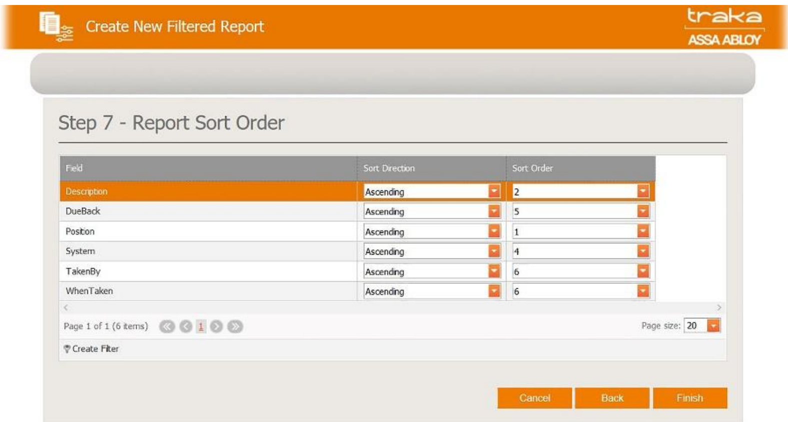
Current Item Status Report



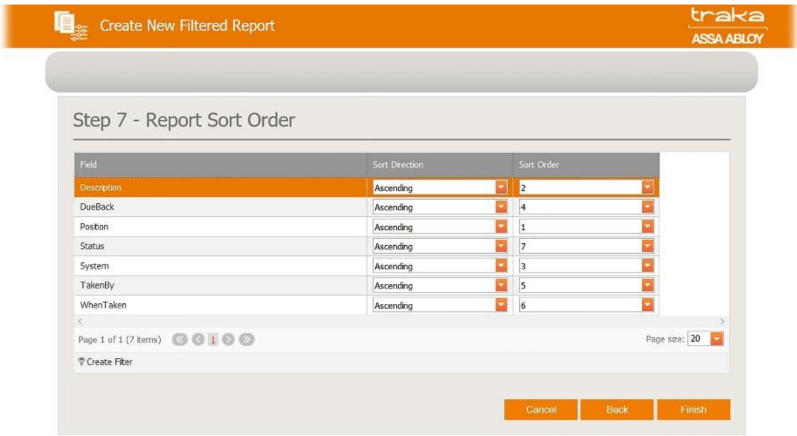
Activity Report



Overdue Report



Curfew Item Status Report



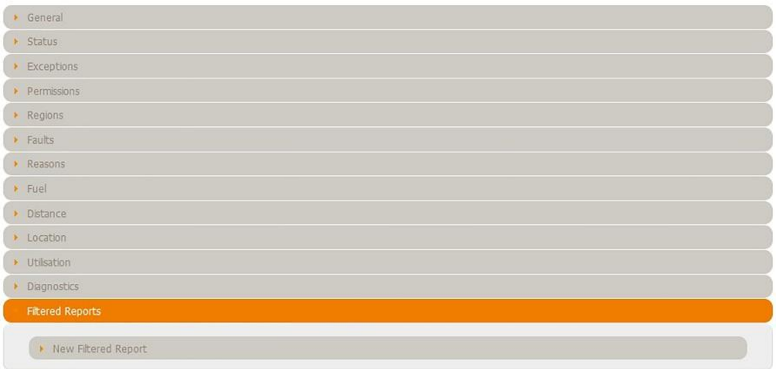
1. Once you have finished editing the Sort Order, click on the **Finish** button.

6.16.1 GENERATING A FILTERED REPORT

Once created, it is possible to generate a Filtered Report, which may be downloaded as a PDF or an Excel spreadsheet. The default number of rows is set to 250. Users can however choose between 1 and 5000 as required.

1. From the Navigation Toolbar, select **View Reports** from the **Reports** menu.

2. At the **Reports** page, select the **Filtered Reports** tab.



3. Next, choose the required Filtered Report and select the required download option.

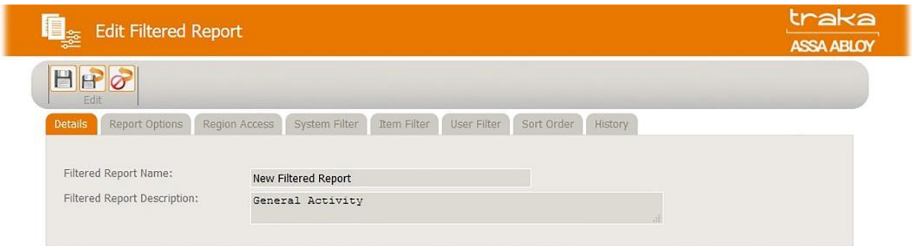
6.16.2 EDITING A FILTERED REPORT

NOTE: If the Filtered Report is associated to a Scheduled Report, it cannot be deleted.

2. Select the Filtered Report you wish to edit.

3. Either double click on the chosen Filtered Report or click on the **Edit** button on the Ribbon Toolbar.

This will enable you to navigate through the previous steps and edit any required information.



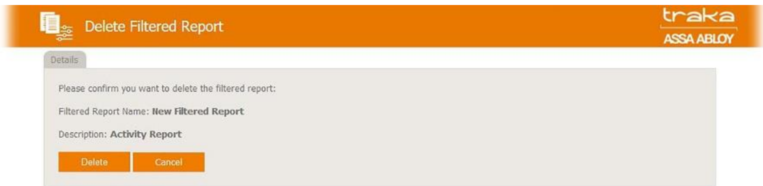
NOTE: A History tab is also available to show an audit of any changes.

6.16.3 DELETING A FILTERED REPORT

1. Select the Filtered Report you wish to delete.

4. Next, click on the **Delete** button on the Ribbon Toolbar.

A message will then appear requesting confirmation that you wish to delete the Filtered Report.



5. Click on delete again to remove the Filtered Report.

The Filtered report will then be removed.

If the Filtered Report is associated with a Scheduled Report, it cannot be deleted and you will receive the following message:

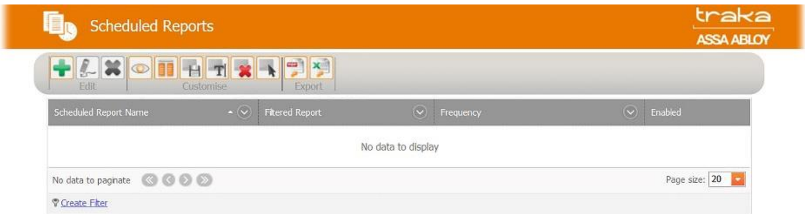
In this instance, you will be required to delete the associated Scheduled Report first, before the filtered report will be deleted.

6.17 SCHEDULED REPORTS

Scheduled Reports can be configured separately from Filtered Reports, whilst they can be created and submitted, they will not display any information without the Filtered Report content. The configuration of Scheduled Reports is divided into 5 steps.

1. To create a Scheduled Report. Select the **Scheduled Reports** icon from the Reports tab on the Navigation Toolbar.

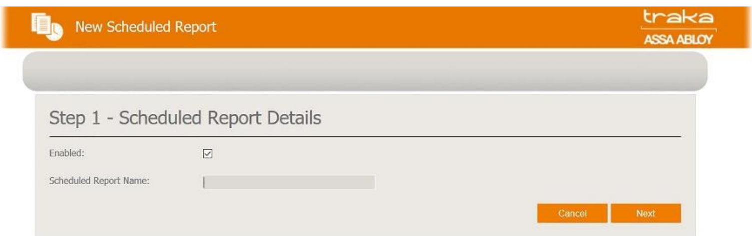
You will now be taken to the Scheduled Reports Landing Page.



2. To create a new Scheduled Report click **Create**  on the Ribbon Toolbar.

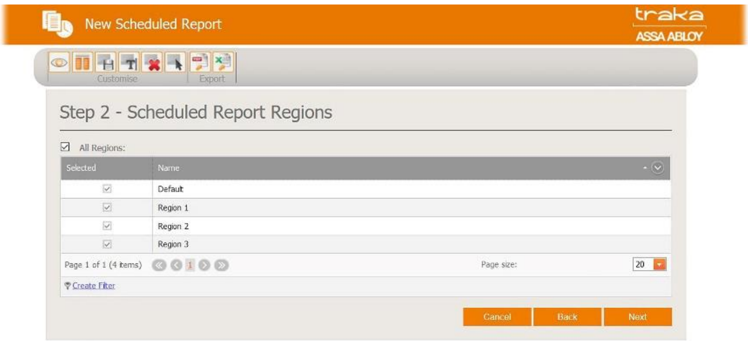
Step 1 – Scheduled Report Details

3. At the **Scheduled Report Details** page, complete the details as required. By default, the **Enabled** check box will be ticked. This will determine if the current Scheduled Report will be active. Once completed, click on **Next.**

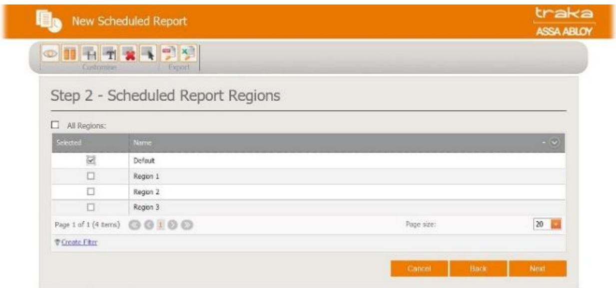


Step 2 – Scheduled Report Regions

4. At the next page, you will be required to select the regions for the Scheduled Report. By default, all available regions will be selected.



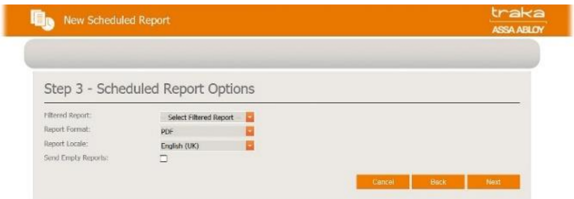
Unchecking the **All Regions** checkbox will enable you to select individual regions.



5. Once you have made your selection, click on **Next** to continue.

Step 3 – Scheduled Report Options

The next step will require you to select the Scheduled Report Options.



Filtered Report:

Select from a list of existing Filtered Reports

Report Format:

Choose from either PDF or Excel as the submitted report

Report Locale:

Select a language for the report

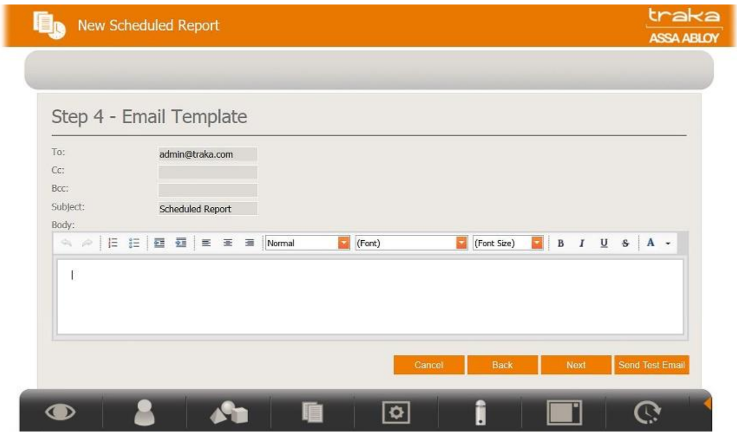
Send Empty Reports:

Enabling this check box will allow reports containing no information to be sent

6. Once you have made the required selections, click on **Next** to continue.

Step 4 – Email Template

At the next page, you will be required to fill out the details for the email template. This will include the recipients email address, the subject name and the main body text as required. If needed, a test email may be sent by clicking on the **Send Test Email button**.

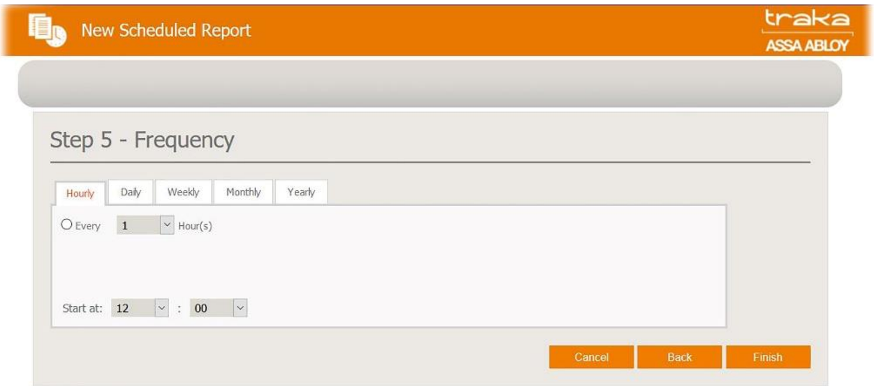


7. Once you have completed the email template, click on **Next** to continue.

Step 5 - Frequency

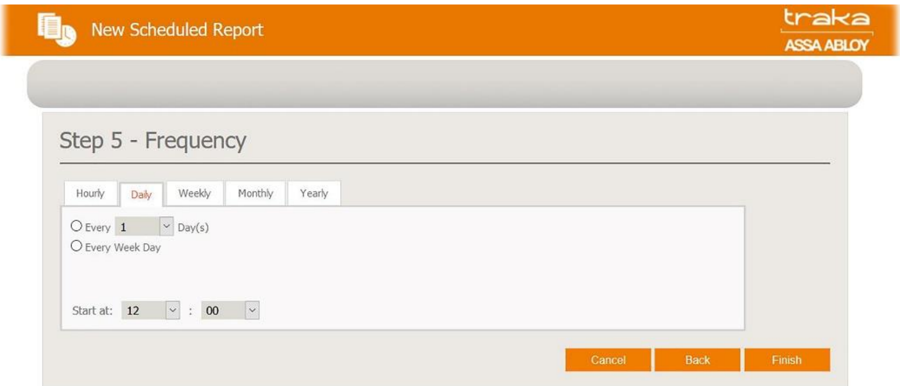
At the next page, you will be required to select the frequency for when the Scheduled Report will be sent. Below is an overview of the options for each tab.

Hourly



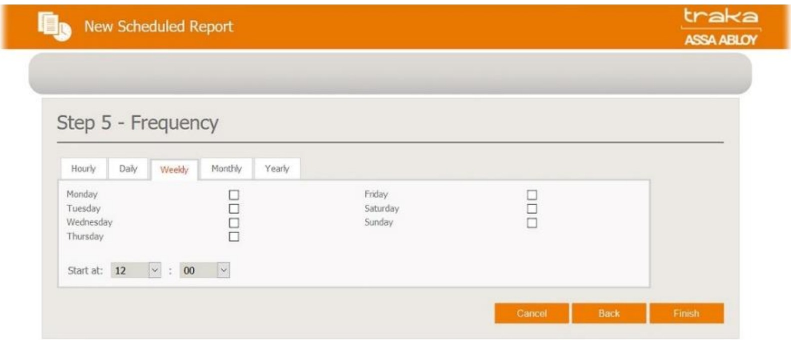
- Select the **Every** option to determine the hourly frequency between 1 and 24 hours.
- Set the start time.

Daily



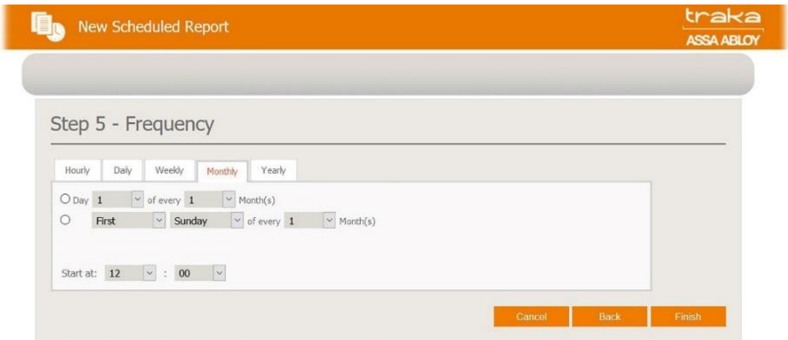
- Select the **Every** option for the frequency of days between 1 and 31 *or* select **Every Week Day**
- Select a start time

Weekly



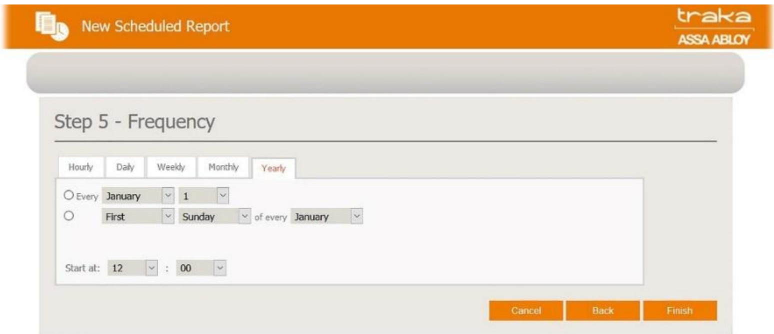
- Select which days of the week the Scheduled Report will be sent
- Select a start time

Monthly



- Select Day 1-31 of every 1-12 month(s) *or* select First-Fourth, Sunday-Saturday of every 1-12 Month(s)
- Select a start time

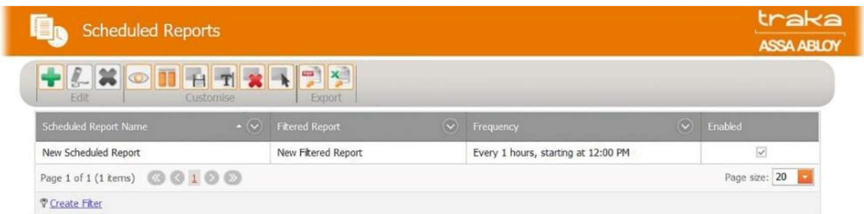
Yearly



- Select Every January-December 1-31 *or* select First-Fourth Sunday-Saturday of every January-December
- Select a start time

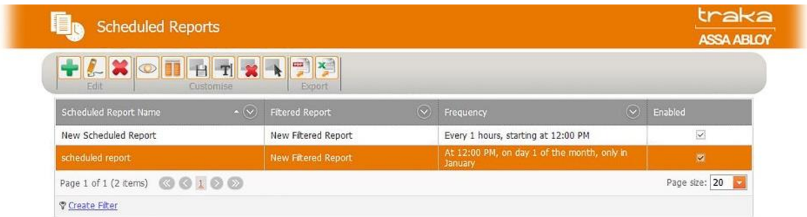
1. Once you have completed setting the Scheduled Report Frequency, click on the **Finish** button.

The next page will provide a summary of the Scheduled Report.



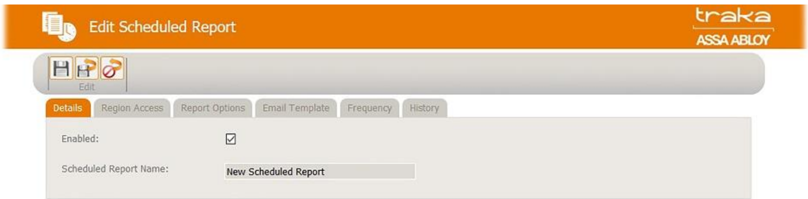
6.17.1 EDITING A SCHEDULED REPORT

1. Select the Scheduled Report that you wish to edit.



2. Either double click on the chosen report or click the **Edit** button on the Ribbon Toolbar.

This will enable you to navigate through the previous steps and edit any required information.

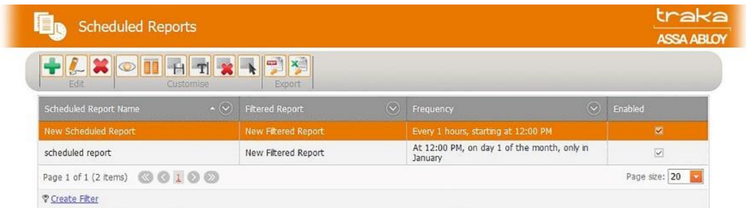


NOTE: A History tab is also available to show an audit of any changes

6.17.2 DELETING A SCHEDULED REPORT

Note: There are no restrictions for deleting a Scheduled Report

1. Select the Scheduled Report that you wish to delete.



2. Next, click on the **Delete** button on the Ribbon Toolbar.

A message will then appear requesting confirmation that you wish to delete the Filtered Report.

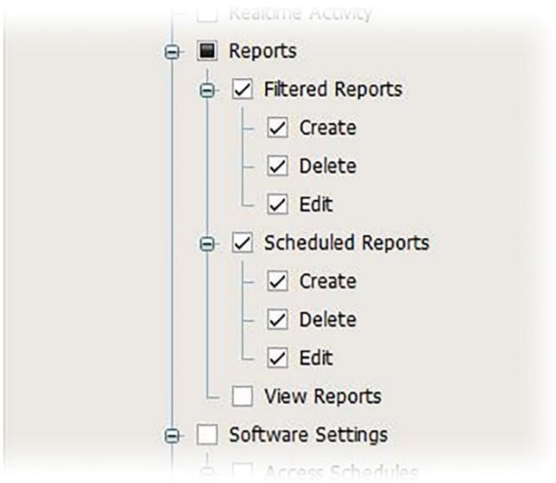
3. Click on delete again to remove the Scheduled Report.

The Scheduled Report will then be removed.

6.17.3 SOFTWARE PERMISSIONS

Both Filtered Reports and Scheduled Reports have individual Software Permissions. These can be applied in the Software Permissions Groups. The permissions can be applied to adding, editing or deleting either Filtered Reports or Scheduled Reports or both.

1. From the Software Permissions Groups, select the permissions for a selected User to have access to as shown.



6.18 TRAKAWEB FIFO & ADVANCED FIFO

6.18.1 INTRODUCTION

The First In/First Out (FIFO) features were created to further assist organisations in managing their assets more effectively. FIFO was designed to even out asset usage, allowing devices with charging the maximum opportunity to recharge. Therefore minimising downtime as much as possible.

NOTE: FIFO and AFIFO cannot be used on the same locker system. However, they can be used within the same instance of TrakaWEB.

NOTE: FIFO and AFIFO do not monitor charging of assets or battery levels, only which asset has been in the system the longest, therefore having the most charge available.

6.18.2 STANDARD FIFO ON TRAKAWEB OVERVIEW

FIFO is a feature that allows the ability to automatically release the item that has been in the locker system the longest, based on the idea that this would have the most charge available as it had been in the locker charging for the longest time and to ensure that items are wear levelled.

For more in-depth information on Standard FIFO on TrakaWEB, please refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide.**

6.18.3 ADVANCED FIFO FOR LOCKERS ON TRAKAWEB OVERVIEW

Advanced First In/ First Out (AFIFO) builds upon FIFO and allows the management of more than one type of asset in the same locker, in the same logged-in session. For example, a user could take the Smartphone and Tablet that have been in the locker the longest.

NOTE: Advanced FIFO for Lockers requires TrakaWEB, therefore cannot be used on a standalone Traka Touch.

For more in-depth information on Advanced FIFO on TrakaWEB, please refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide.**

6.18.4 ADVANCED FIFO FOR KEY CABINETS ON TRAKAWEB OVERVIEW

Advanced FIFO is an optional facility within TrakaWEB that allows authorised users to select one or more types of item from a key cabinet system. For each type of item, the system will automatically issue the item that has been in the key cabinet for the longest, therefore spreading the workload over the group of items and, in the case of keys to equipment or vehicles which recharge while at their stations, maximising the time spent on charge.

NOTE: Advanced FIFO for Key Cabinets requires TrakaWEB, therefore cannot be used on a standalone Traka Touch.

For more in-depth information on Advanced FIFO on TrakaWEB, please refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide.**

6.19 ALLOWANCE ACROSS SYSTEMS (AAS)

6.19.1 INTRODUCTION

Allowance Across Systems (AAS) is a cost option feature which will enable users to take specific items of the same type assigned to a Common Item Access Group (CIAG) from across multiple Advanced FIFO and Fixed Return systems. The Allowance Across Systems functionality will be dependent on the Real Time Update Service (RTUS) which will provide an up to date and accurate access rights calculation which will be performed across all systems.

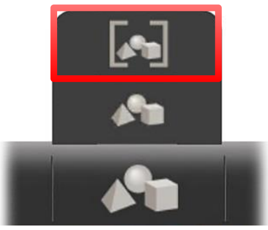
A configuration will be required to enable the Allowance Across Systems feature which can be obtained from Traka.

For more information on the setup and configuration of RTUS, refer to **TD0165 – TrakaWEB Real Time Update Service Setup & Configuration Guide.** For more information on the setup and configuration of Advanced First in/First out, please refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide.**

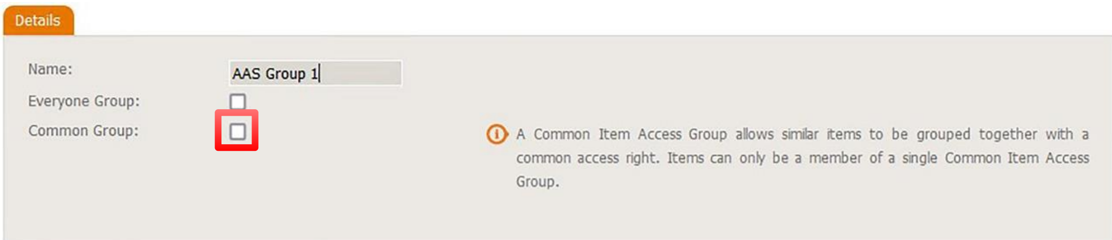
6.19.2 SETTING UP ALLOWANCE ACROSS SYSTEMS – (ADVANCED FIFO)

A Common Item Access Group will need to be created to enable the functionality of AAS which will enable items of the same type to be grouped together in a single group.

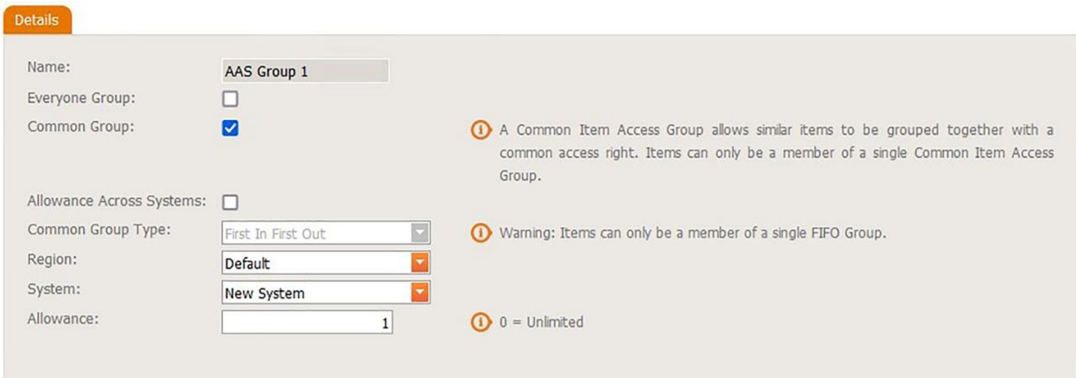
1. Select the Item Access Groups icon from the Navigation Toolbar.



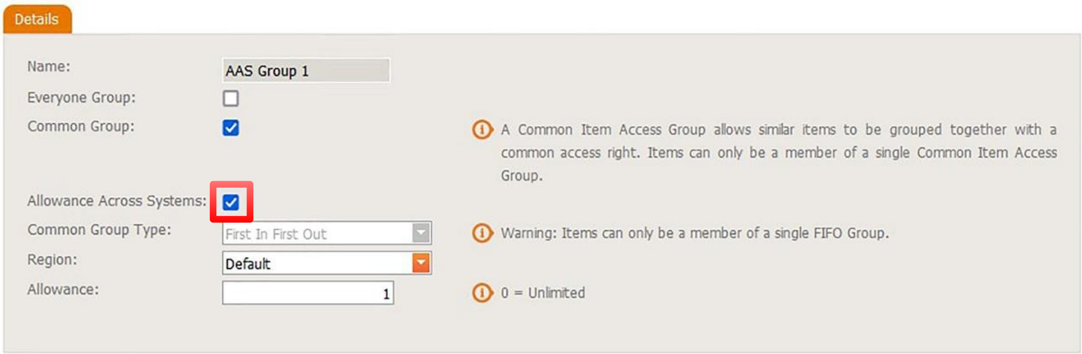
2. At the Item Access Groups page, select the  Create button.
3. Next, enter a name for the group and then place a tick in the **Common Group** check box.



Selecting this check box will enable you to access the AAS functionality as shown below.



4. Place a tick in the check box for **Allowance Across Systems.**



You will notice that the **System** dropdown menu is no longer visible. This is due to the option only being applicable to one system and by definition, Allowance Across Systems is applicable across multiple systems.

NOTE: If all the systems are set as First In First Out, the dropdown menu for Common Group Type will be unavailable.

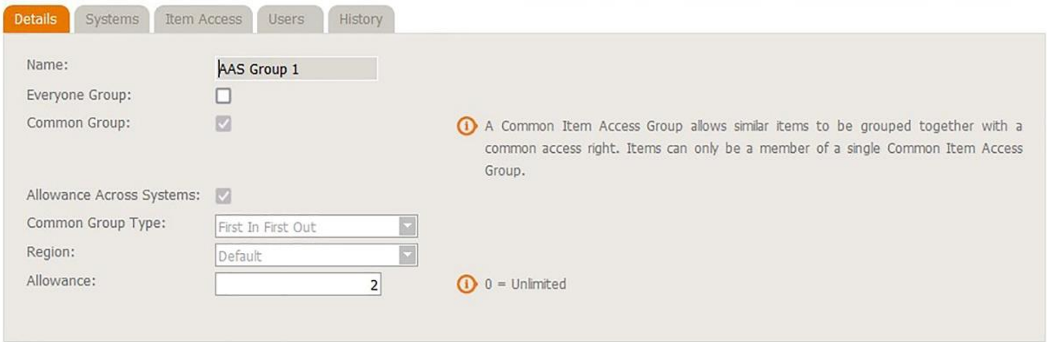
5. Select a specific region from the **Region** dropdown menu that you wish to assign the group to.

6. Assign an allowance value in the **Allowance** box. The default value is set to 1. If the value is set to 0, then that would allow the user to take as many items from the group as they would like. In this example, the item allowance has been set to 2.

7. Once complete, click on **Save.**

NOTE: Once saved, you will only be able to edit the Name, Everyone Group and Allowance options.

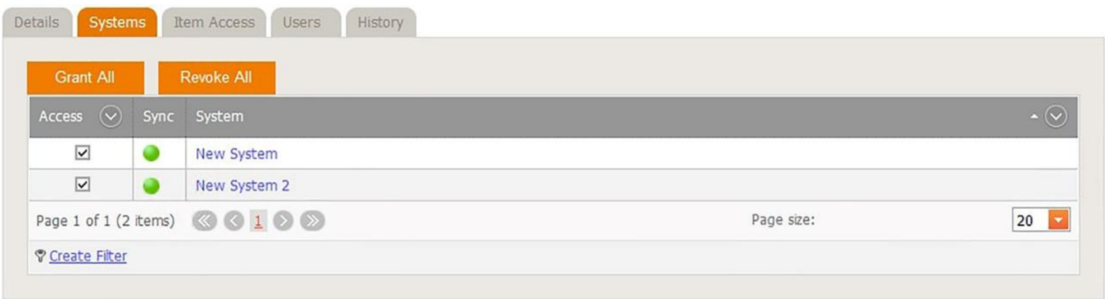
You will notice that after saving, four new tabs will be made available.



8. Click on the **Systems** tab.

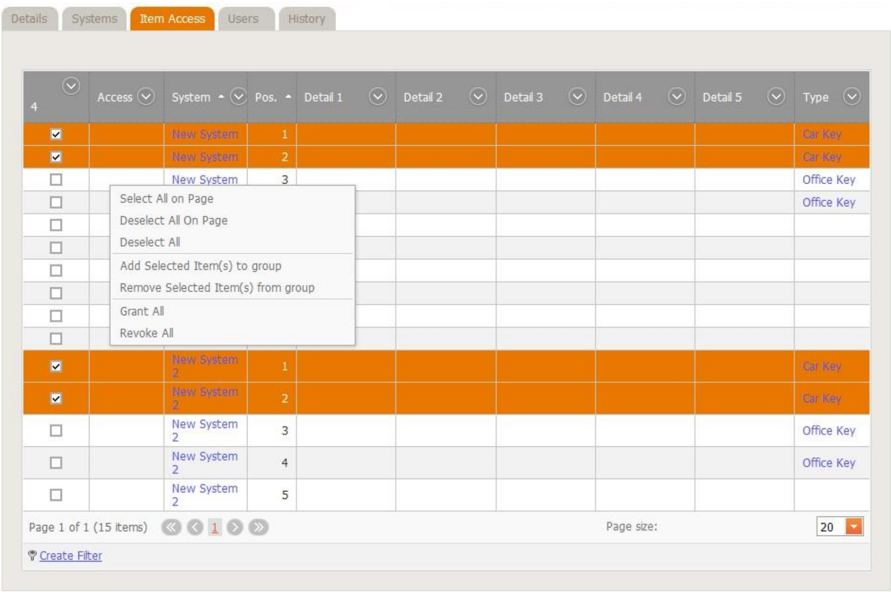
The **Systems** tab will a list of all the available systems within the selected region.

9. Select the systems that you wish to add to the group. You can choose to select and deselect them individually or use the **Grant All** and **Revoke All** buttons.

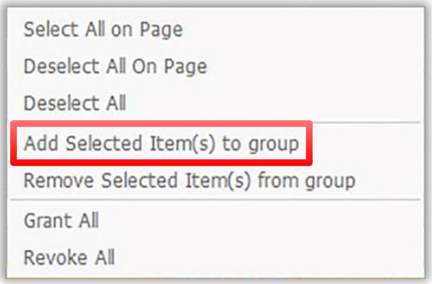


10. Next, select the **Item Access** tab.

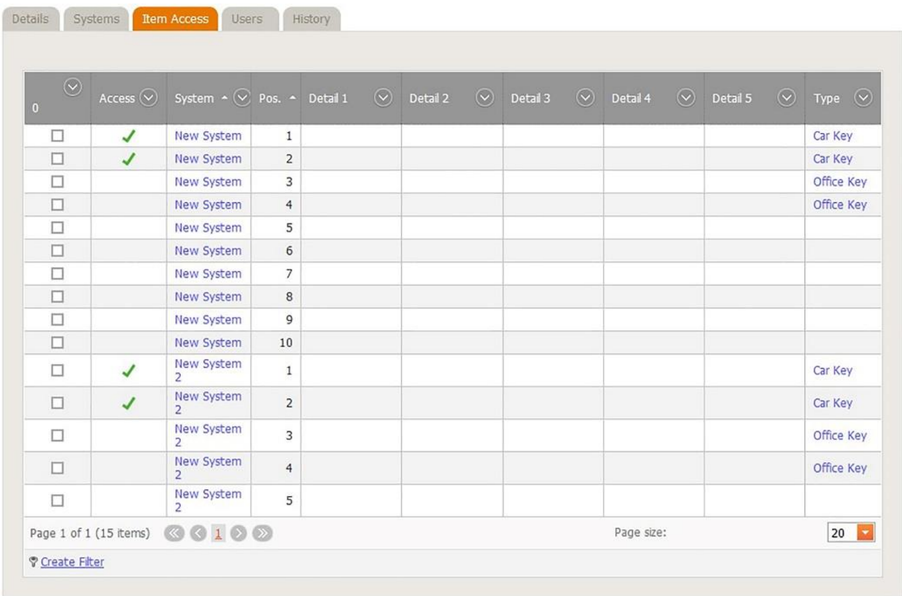
The **Item Access** tab will list all the items from the previously selected systems. You may choose to select items individually or by using the **Multi-Select/Multi-Edit** function, you can select all the items at once. In this example, 2 items from each system have been selected.



11. Next, right click within the grid and choose the **Add Selected Item(s) to Group.**



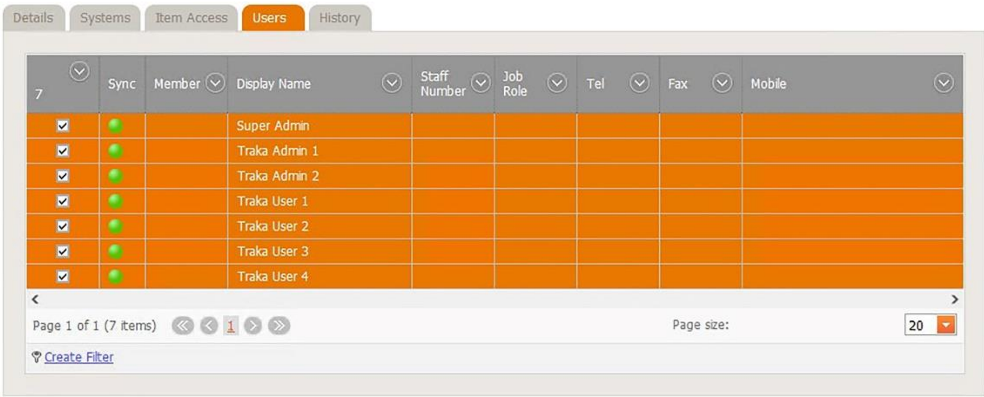
After confirmation, you will now see a green tick against the selected items indicating that they have now been added to the group.



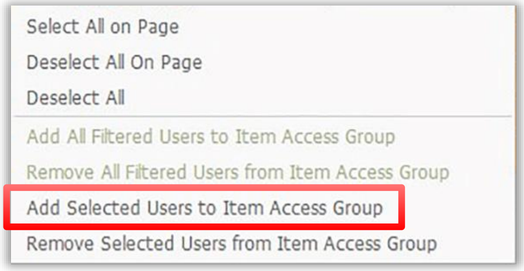
12. Now select the **Users** tab.

The **Users** tab will display a list of all the available users who have been granted access to the selected systems.

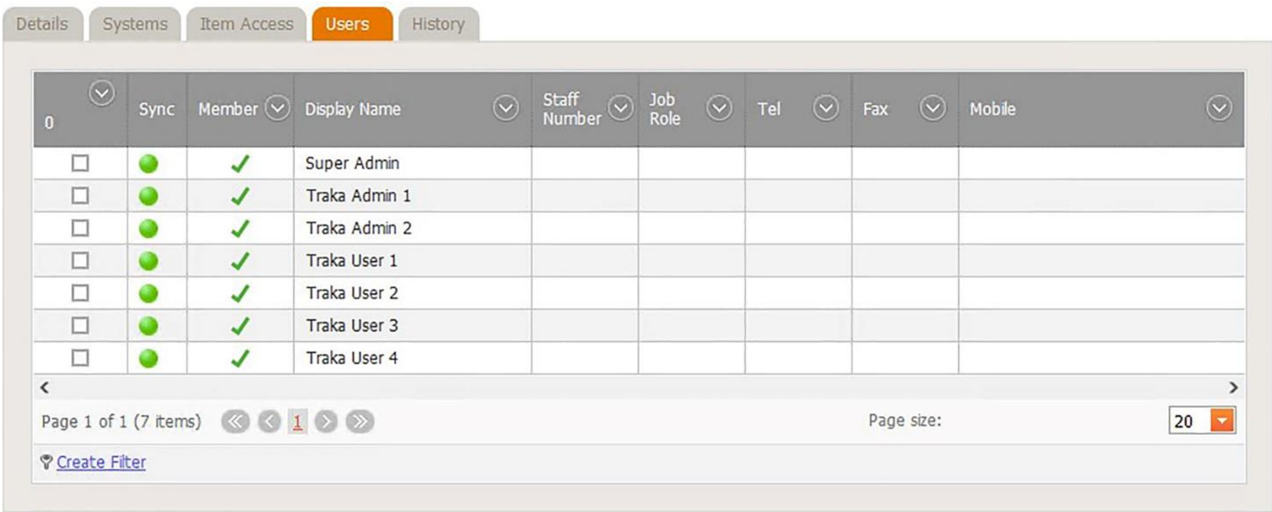
13. Select which users you wish to assign to the group.



14. Right click within the grid and select **Add Selected Users to Item Access Group.**



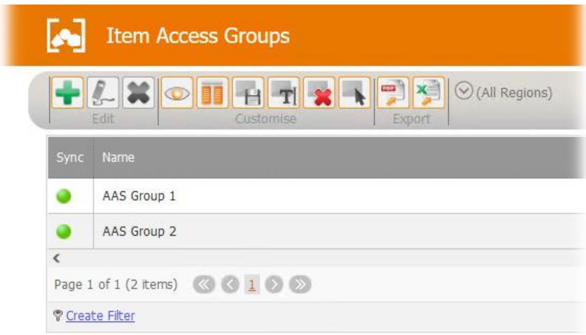
After confirmation, you will now see a green tick against the selected users indicating that they have now been added to the group.



15. Once completed, click on the **Save and Return** button.

Should you wish to make any changes to the Common Item Access Group, you may return to the **Item Access Groups** page and select the group you wish to edit and then click on the edit button. You will then be taken back though steps as shown above.

NOTE: If you have more items to which you wish to allow access to across multiple systems, they must each be assigned to a different Common Item Access Group as items can only be a member of a single group.



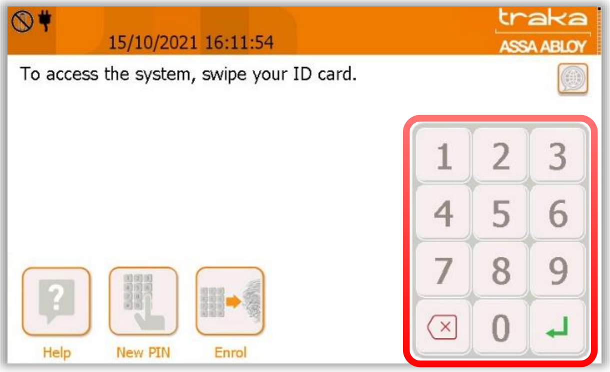
6.19.3 USING ALLOWANCE ACROSS SYSTEMS - (ADVANCED FIFO)

The following section describes the process of using Allowance Across Systems. In this example, 2 systems have been configured to utilise the feature. 2 Common Item Access groups have been created with 4 items in each and divided across both systems. To demonstrate the functionality, users have been granted an allowance of 2 items from each group.

A User is able to take up to the allowance for a group from just one of the systems or across both systems. For example, if group A consists of 2 items on System 1 and 2 items on System 2 then a user with access to the group could take one item from both systems or both items from just one of the systems. Once the allowance of 2 for that group has been met, they cannot remove any more items that belong to that group from either system.

6.19.4 TAKING & RETURNING ITEMS – NON-ADMIN USER - (ADVANCED FIFO)

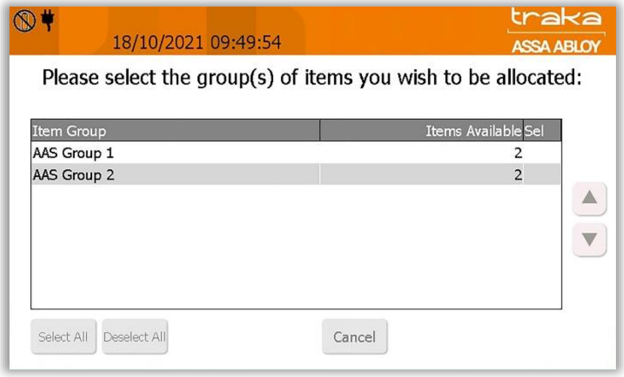
1. Log into system 1 using either keypad, card reader or fingerprint.



System #1

System #2

Once logged in, a list of groups that the user has been allocated access to will be displayed.

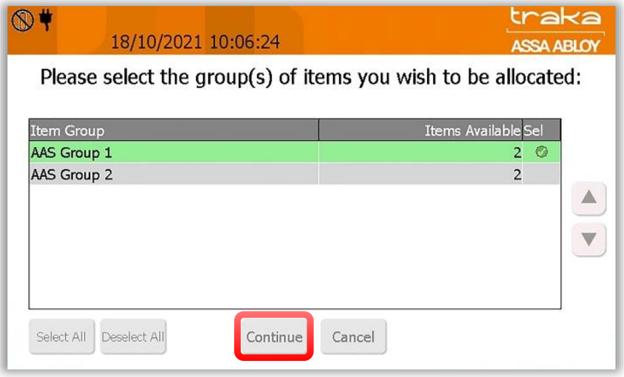


System #1

System #2

You will have the option to select individual groups or select all the available groups by pressing the **Select All** button. This may be cancelled by selecting **Deselect All.** The **Items Available** column will display your item allowance for the groups that you have been granted access to.

2. Select the required groups and then click on **Continue.**



System #1

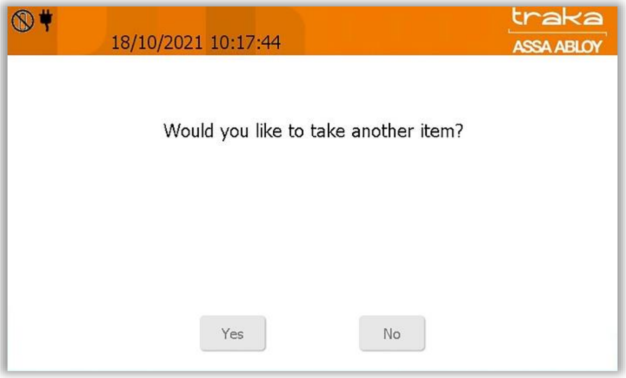
System #2

The door will open, and the first available item will be accessible.

System #1

System #2

After the Item has been taken, close the door. A message will appear asking if you would like to take another item.

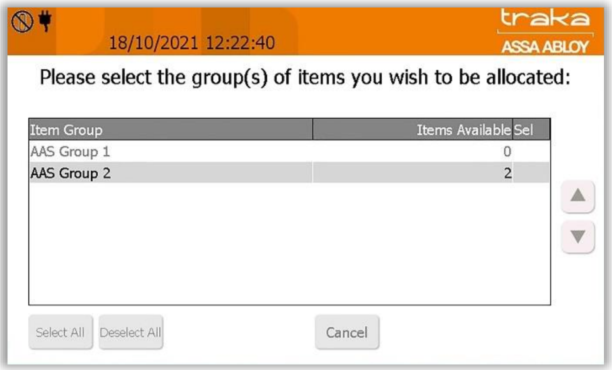


System #1

System #2

Selecting **Yes** will take you through the process of removing the next available item.

Once your allowance for that item type has been reached, the option to remove any more items from that group will appear greyed out on the screen as shown below.



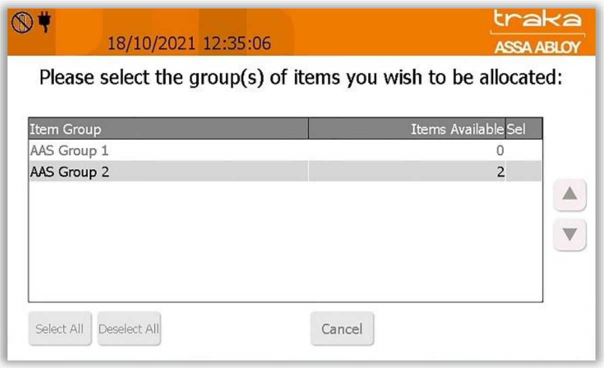
System #1

System #2

NOTE: You will still have the option to select items from other available groups that you have been granted access to.

As the item allowance is applicable across systems, you may log into another system which will grant you with the same permissions.

System #1



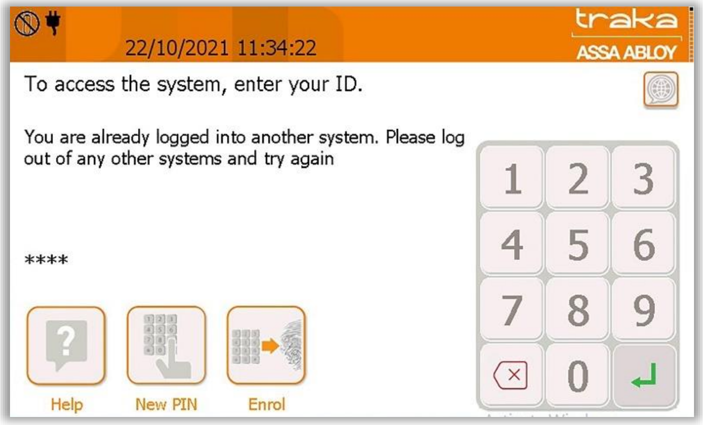
System #2

Providing there are still available items, if another user logs into the system, they will be able to take items that they have been granted access to.

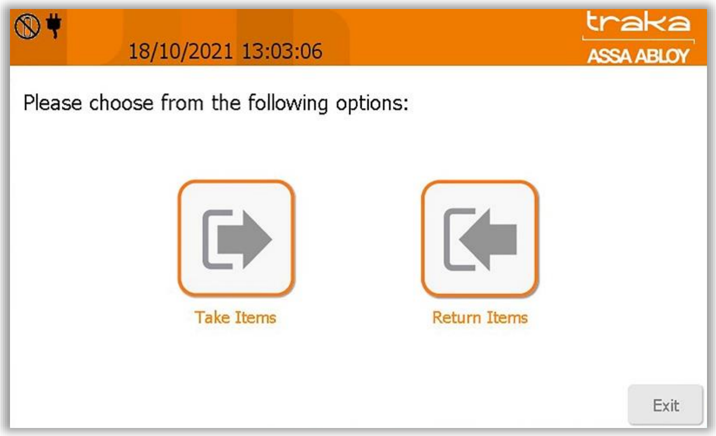
System #1

System #2

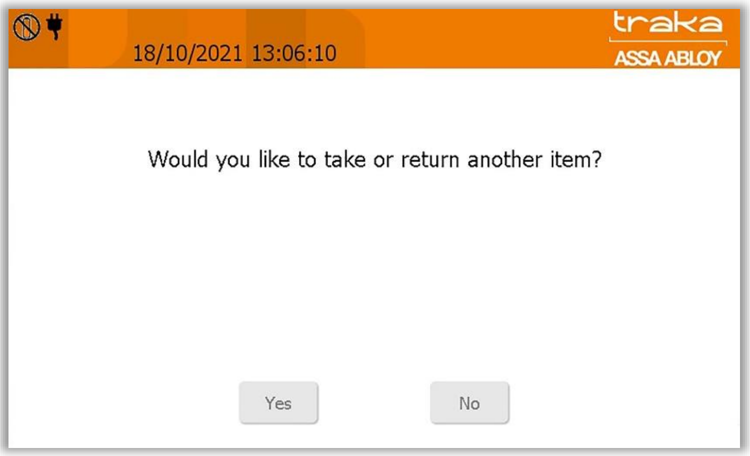
NOTE: A non-admin user cannot log into more than 1 system at a time when Allowance Across Systems has been activated on that system. This does not apply to an admin user.



If you already have items in your possession, you may still return to a system to take more items that you have access to. In this instance, when you login, the system will give you the option to either take an item or return an item that you already hold.

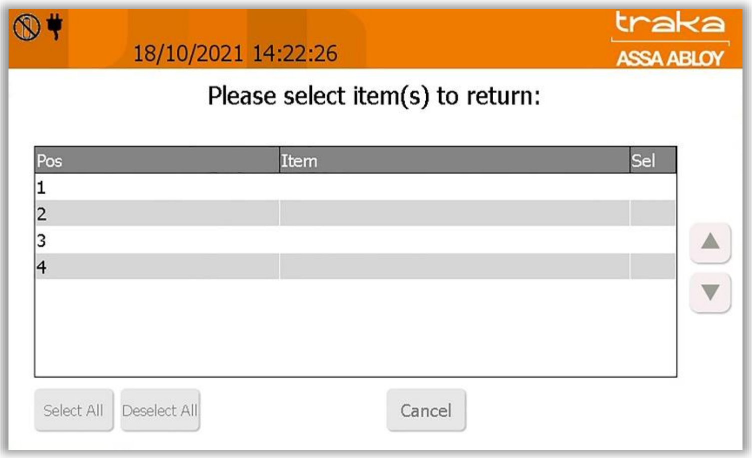


3. Once you have taken or returned an item, close the door and you will see the following message:

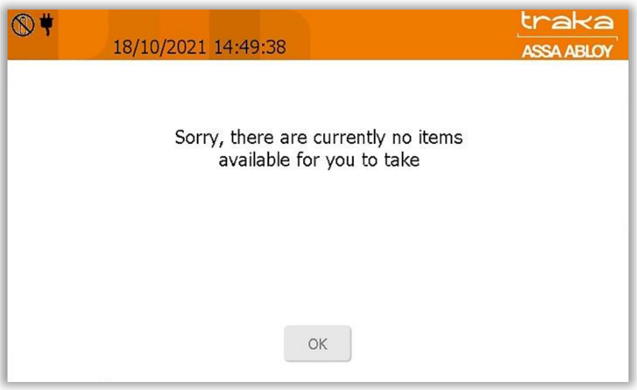


Selecting **Yes** will open the door and allow you to take an available item. Selecting **No** will automatically log you out of the system.

Once you have reached your item allowance limit, when you next log into the system, you will only have the option to return items.



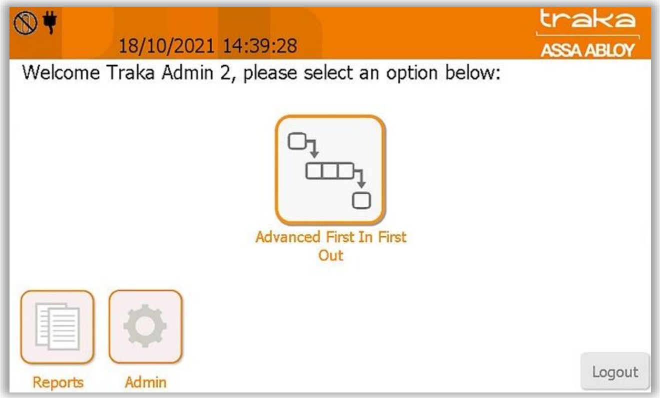
Once all available items from all assigned groups have been taken, you will be presented with the following message informing you that there are no more available items to take.



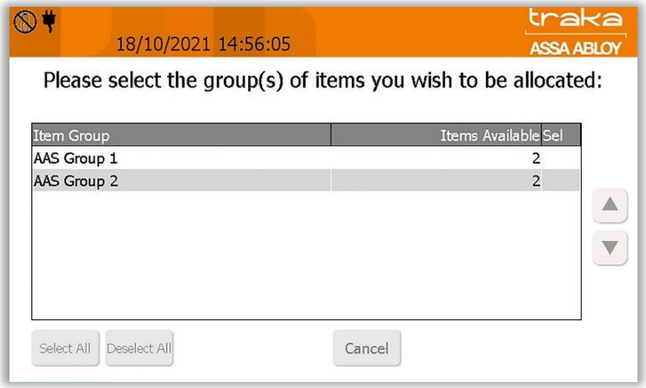
6.19.5 TAKING & RETURNING ITEMS – ADMIN USER - (ADVANCED FIFO)

As an admin user, the same Allowance Across Systems rules will apply as a non-admin user. An admin user will however be able to perform admin activities in Traka Touch.

1. After logging into the system as an admin user, select the **Advanced First In First Out** button as shown here.



You will then immediately be shown a list of the groups that are available to you.



You will now be able to perform the same Allowance Across Systems activities as outlined in the previous section.

6.19.6 OVERRIDE OPTIONS - (ADVANCED FIFO)

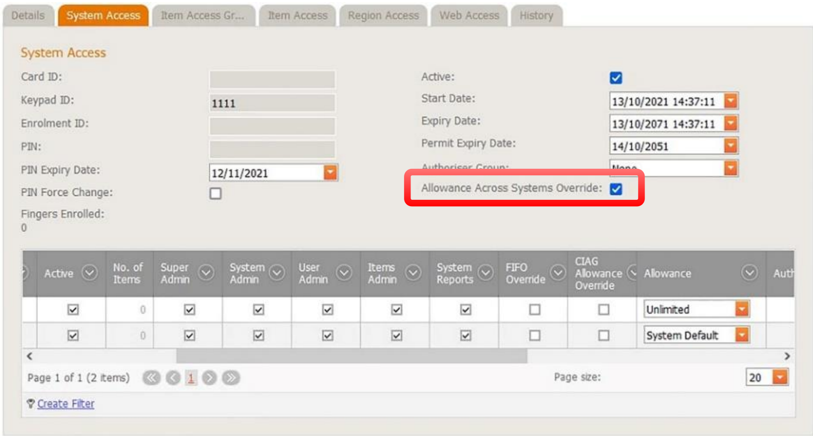
The Allowance Across Systems Override option will allow a user with the permission granted to remove all authorised items from all groups across all systems, overriding the allowance limit. The option to enable the permission is performed in TrakaWEB.

There are 3 separate override options available for Allowance Across Systems in TrakaWEB which can be set individually.

Allowance Across Systems Override:

This option will override the other options and will allow access to all items in their groups on any of the relevant systems.

1. From the Users Page, select a User to whom you wish to grant the override permission and then navigate to the **Edit User** page.
2. Place a tick in the check box for **Allowance Across Systems Override.**



With the override permission enabled. The user will then be able to remove all the available items from across all systems.

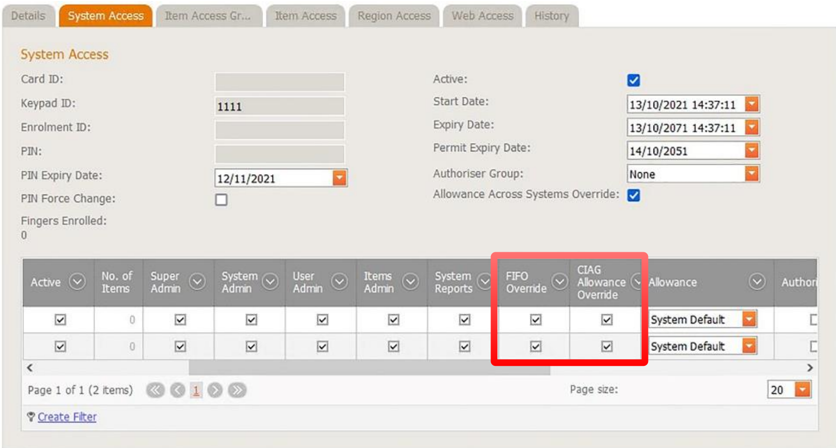
FIFO Override:

This will give a user with one or more CIAG's assigned, access to those groups via **I Know What I Want** or **I Need To Search** as well as the Advanced FIFO button up to the limit of the Common Item Access Group.

CIAG Allowance Override:

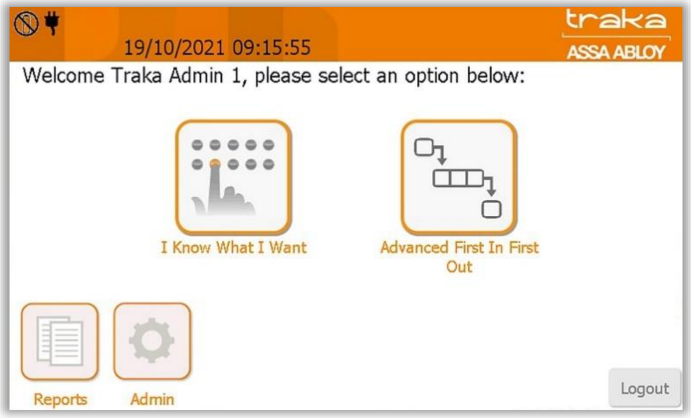
This option removes the allowance limit for non-AAS Common Item Access Groups, so the user can now remove all items from their assigned groups.

From the System Access Grid, you can additionally choose to allocate a user with the **FIFO Override** and/or **CIAG Allowance Override.** With these enabled the user can choose from either the **First In First Out** option or **I Know What I Want.**

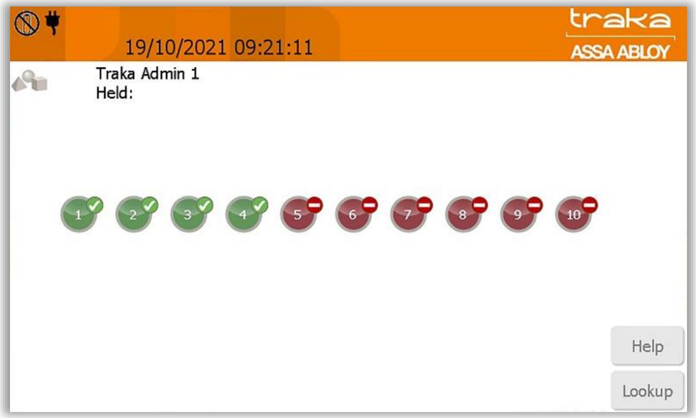


3. With all override options assigned, log into an AAS enabled system.

You may now choose from either the **I know What I Want** option or **Advanced First In First Out** when logging in.



4. Select the **I Know What I Want** button.



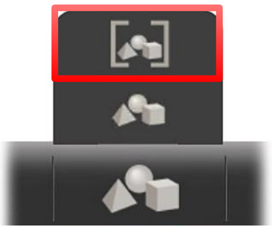
The Common Item Access Groups will no longer appear on the screen. You will now be able to remove any items assigned to you from any AAS enabled system, regardless of the Common Item Access Group they belong to.

Selecting the **Advanced First In First Out** button will still permit you to remove all items from all groups across all systems as described at the start of this section.

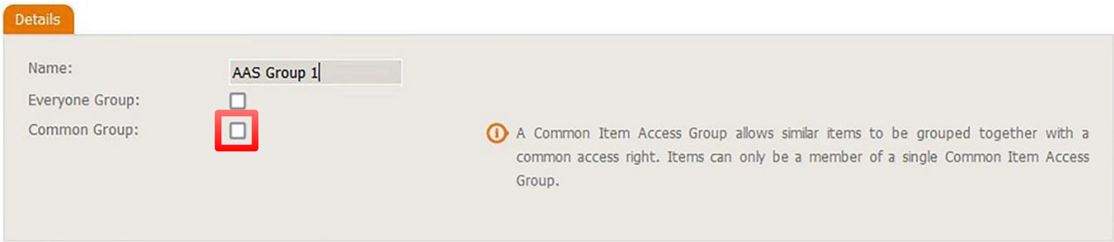
6.19.7 SETTING UP ALLOWANCE ACROSS SYSTEMS – (FIXED RETURN)

A **Common Item Access Group** will need to be created to enable the functionality of AAS which will enable items of the same type to be grouped together in a single group.

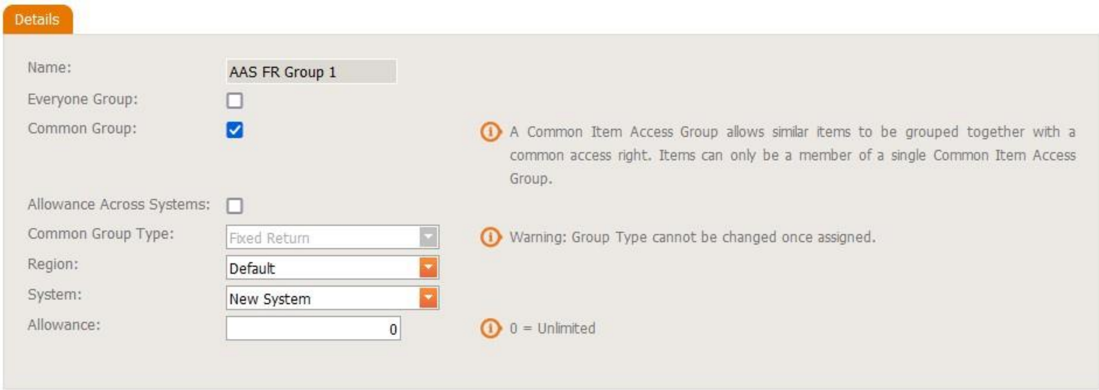
1. Select the Item Access Groups icon from the Navigation Toolbar.



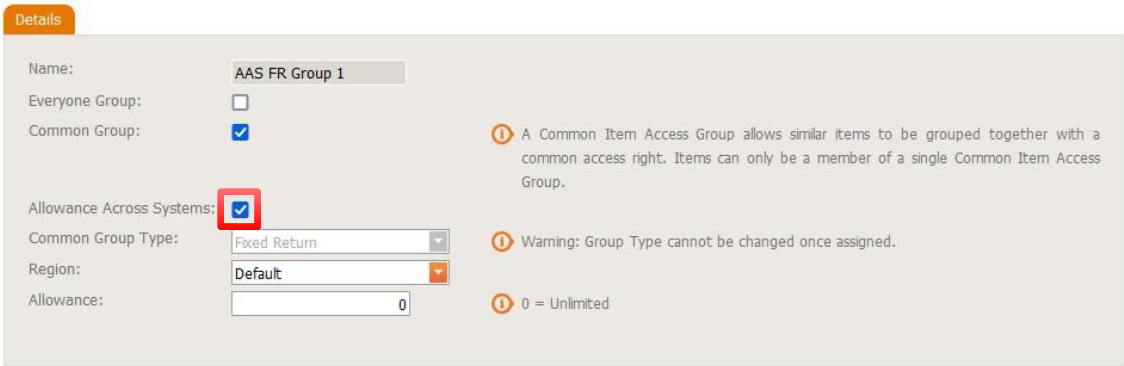
2. At the Item Access Groups page, select the  Create button.
3. Next, enter a name for the group and then place a tick in the **Common Group** check box.



Selecting this check box will enable you to access the AAS functionality as shown below.



4. Place a tick in the check box for **Allowance Across Systems.**



You will notice that the **System** dropdown menu is no longer visible. This is due to the option only being applicable to one system and by definition, Allowance Across Systems is applicable across multiple systems.

NOTE: If all the systems are set as Fixed Return, the dropdown menu for Common Group Type will be unavailable.

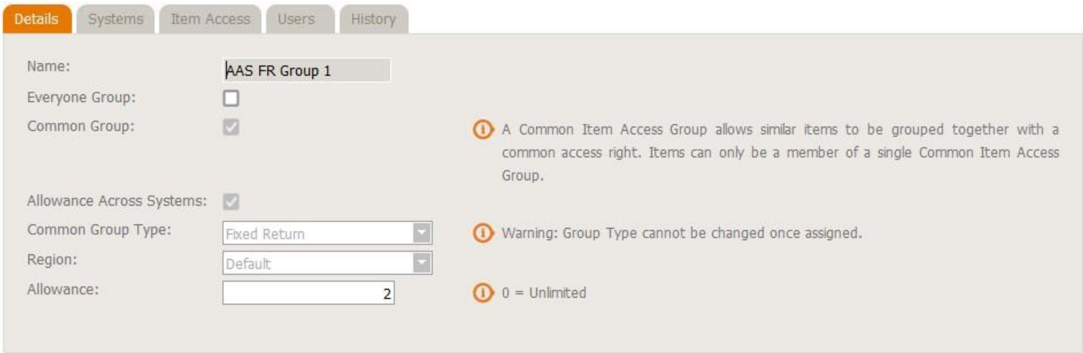
5. Select a specific region from the **Region** dropdown menu that you wish to assign the group to.

6. Assign an allowance value in the **Allowance** box. The default value is set to 0. This value will allow the user to take as many items from the group as they would like. In this example, the item allowance has been set to 2.

7. Once complete, click on **Save.**

NOTE: Once saved, you will only be able to edit the Name, Everyone Group and Allowance options.

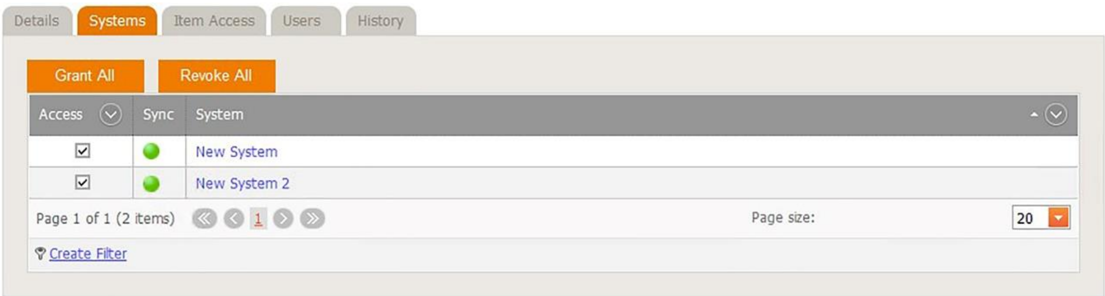
You will notice that after saving, four new tabs will be made available.



8. Click on the **Systems** tab.

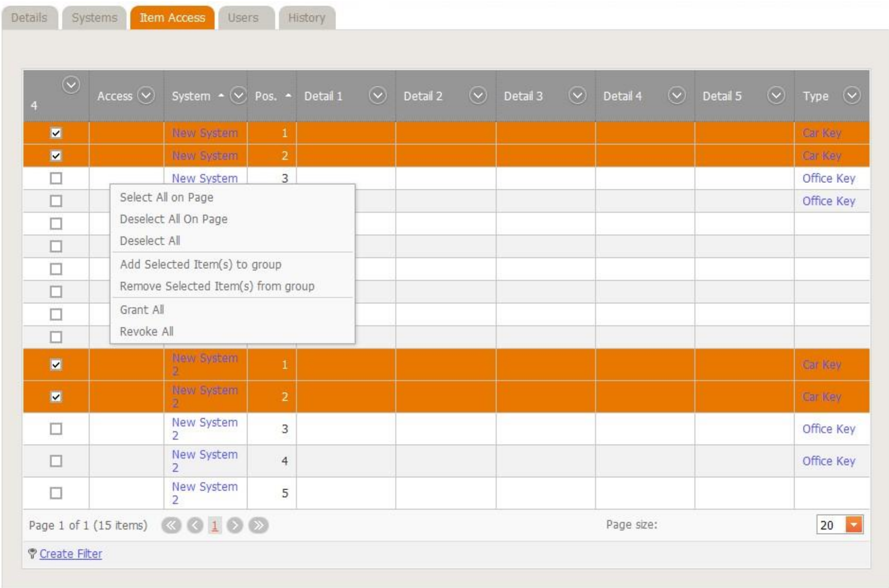
The **Systems** tab will list of all the available systems configured for both Fixed Return and Allowance Across Systems within the selected region.

9. Select the systems that you wish to add to the group. You can choose to select and deselect them individually or use the **Grant All** and **Revoke All** buttons.

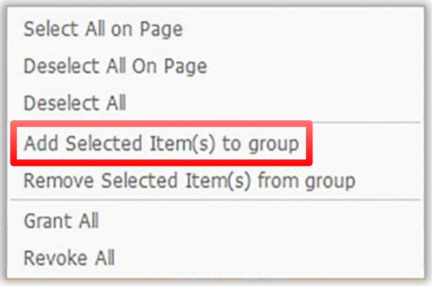


10. Next, select the **Item Access** tab.

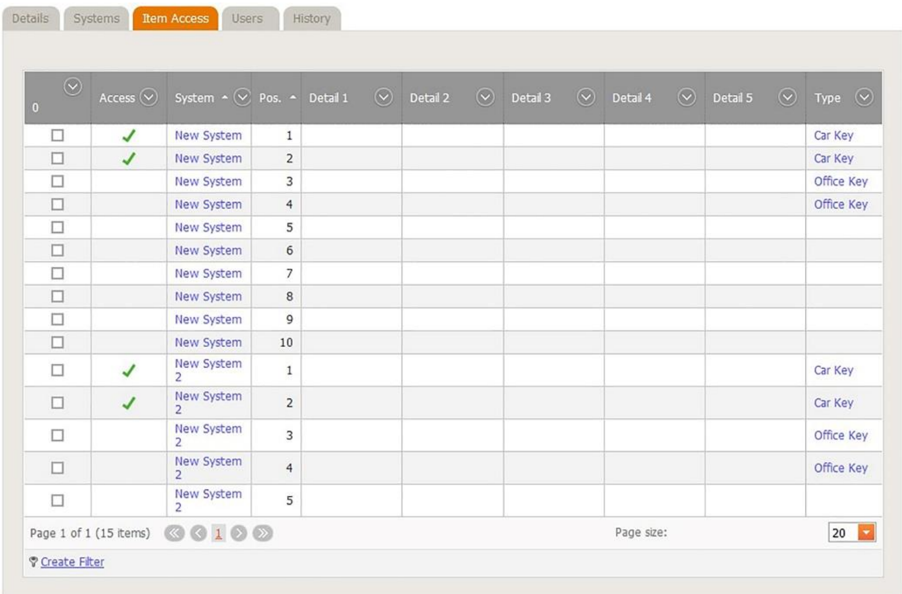
The **Item Access** tab will list all the items from the previously selected systems which are not already part of an Item Access Group. You may choose to select items individually or by using the **Multi-Select/Multi-Edit** function, you can select all the items at once. In this example, 2 items from each system have been selected.



11. Next, right click within the grid and choose the **Add Selected Item(s) to Group.**



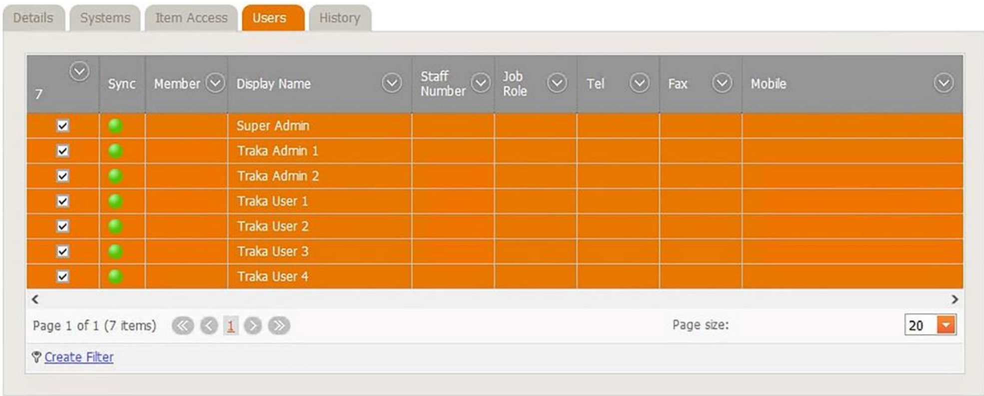
After confirmation, you will now see a green tick against the selected items indicating that they have now been added to the group.



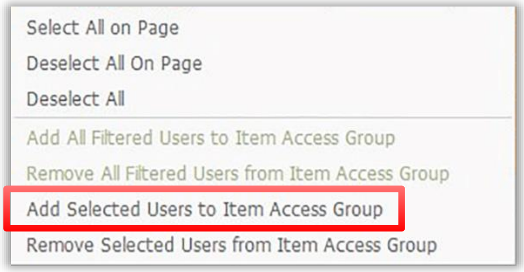
12. Now select the **Users** tab.

The **Users** tab will display a list of all the available users who have been granted access to the selected systems.

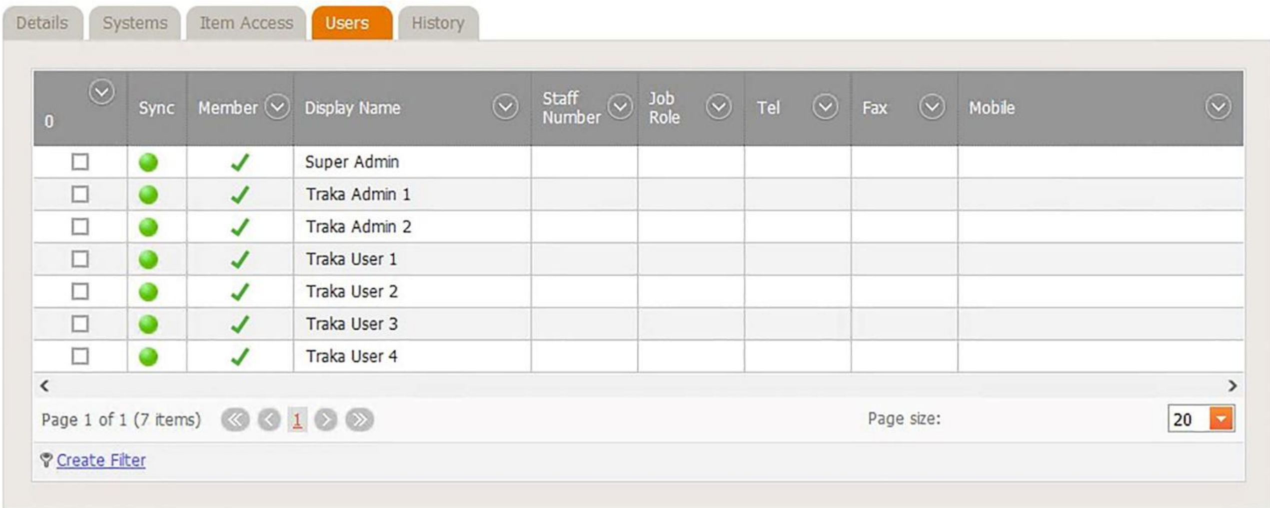
13. Select which users you wish to assign to the group.



14. Right click within the grid and select **Add Selected Users to Item Access Group.**



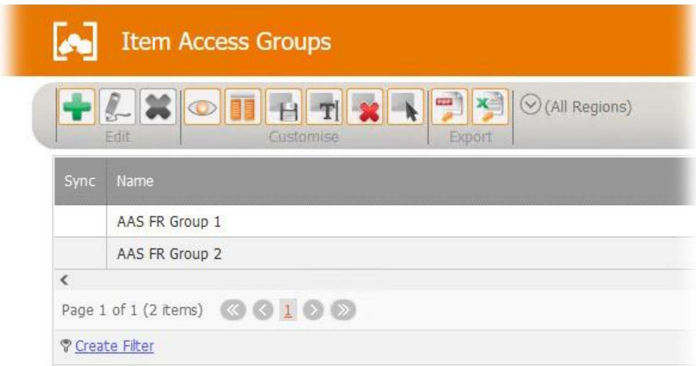
After confirmation, you will now see a green tick against the selected users indicating that they have now been added to the group.



15. Once completed, click on the **Save and Return** button.

Should you wish to make any changes to the Common Item Access Group, you may return to the **Item Access Groups** page and select the group you wish to edit and then click on the edit button. You will then be taken back through steps as shown above.

NOTE: If you have more items to which you wish to allow access to across multiple systems, they must each be assigned to a different Common Item Access Group as items can only be a member of a single group.



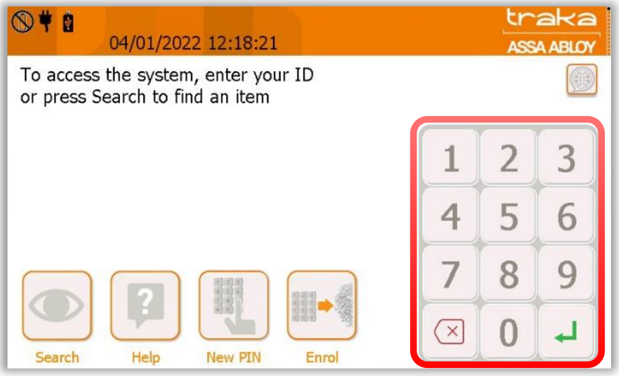
6.19.8 USING ALLOWANCE ACROSS SYSTEMS - (FIXED RETURN)

The following section describes the process of using Allowance Across Systems for Fixed Return systems. In this example, 2 systems have been configured to utilise the feature. 2 Common Item Access groups have been created with 4 items in each and divided across both systems. To demonstrate the functionality, the allowance on both groups has been set to 2.

A User is able to take up to the allowance for a group from just one of the systems or across both systems. For example, if group A consists of 2 items on System 1 and 2 items on System 2 then a user with access to the group could take one item from both systems or both items from just one of the systems. Once the allowance of 2 for that group has been met, they cannot remove any more items that belong to that group from either system.

6.19.9 TAKING & RETURNING ITEMS – NON-ADMIN USER - (FIXED RETURN)

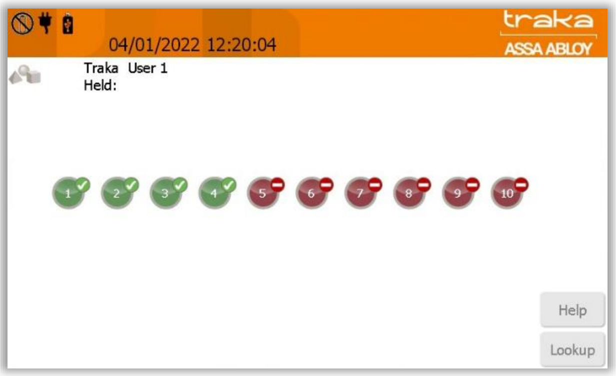
1. Log into system 1 using either keypad, card reader or fingerprint.



System #1

System #2

The door will now open, and the user will be able to remove available items according to their allowance. In the example below, 4 items are available based on the 2 Common Item Access Groups that the user has been assigned to.



System #1 **System #2**

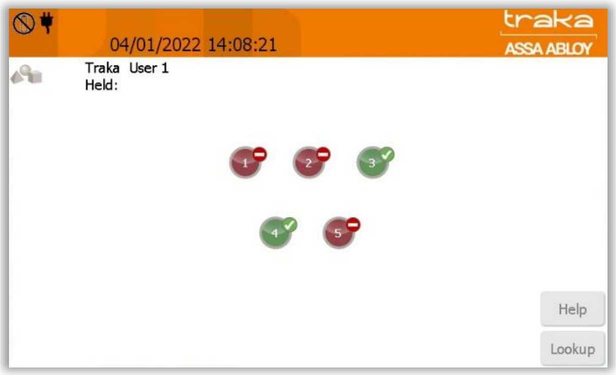
Based on this example, if the user had only been granted access to 1 Common Item Access Group, then only 2 items from both systems would be available as shown below.

System #1 **System #2**

NOTE: Once an item has been taken and the user closes the door, they will automatically be logged out.

Providing the user does not remove all their allocated items from System #1, they may log out and then log into System #2 and take items up to the group's allowance.

Once the user's item allowance for the Common Item Access Group on System #1 has been reached, the option to remove any more items from that group will not be available on either system. However, items from other Common Item Access Groups could still be available.



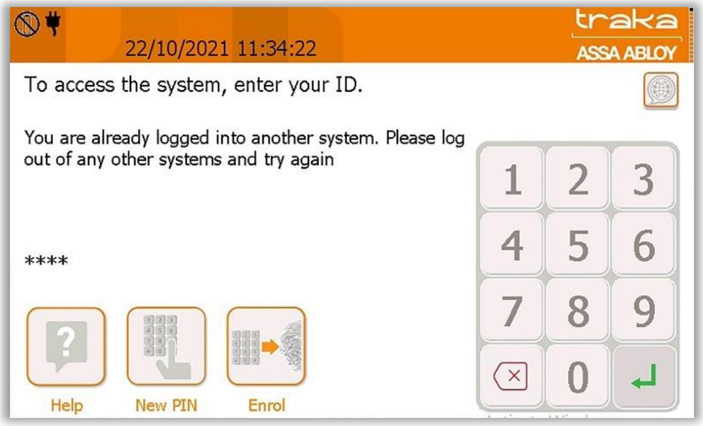
System #1 **System #2**

If a user removes all the available items from both Common Item Access Groups from System #1, there will be no more available items for other users to take from that system and the removed items will appear greyed out. However, they will still be able to take items from System #2 as required, until all available items from both groups in both systems have been taken.

System #1

System #2

NOTE: A non-admin user cannot log into more than 1 system at a time when Allowance Across Systems has been activated on that system. This does not apply to an admin user.

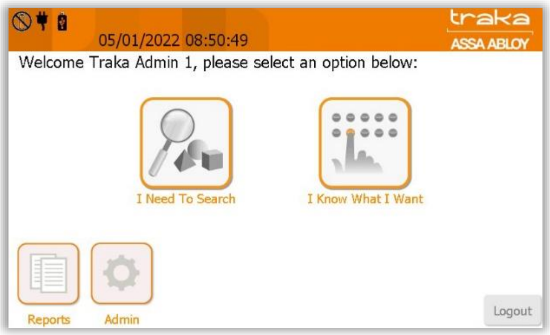


6.19.10 TAKING & RETURNING ITEMS – ADMIN USER (FIXED RETURN)

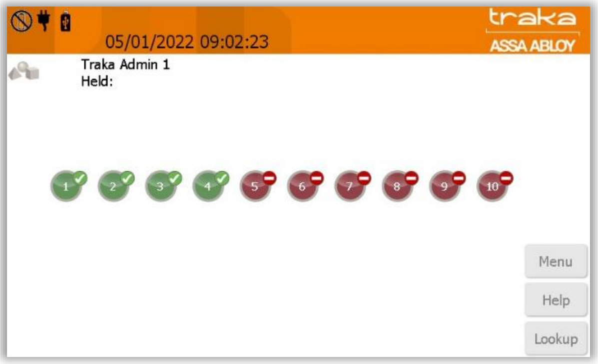
As an admin user, the same Allowance Across Systems rules will apply as a non-admin user. An admin user will however be able to perform admin activities in Traka Touch.

NOTE: The combinations for I Know What I Want or I Need To Search modes may be set in General Options on each system to determine the default Item release screens. The following examples are based around the I Know What I Want option.

1. Login to the system as an Admin User and select the required option for accessing items.



Once the door has opened, you will now be able to perform the same Allowance Across Systems activities as outlined in the previous section.



6.19.11 OVERRIDE OPTIONS - (FIXED RETURN)

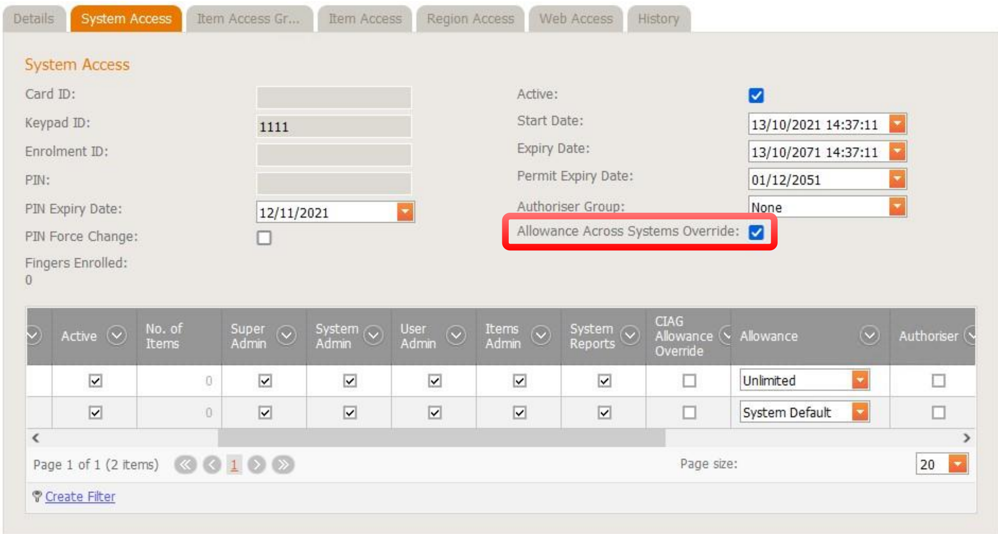
There are 2 separate override options available for Allowance Across Systems for Fixed Return in TrakaWEB which can be set individually.

The override option granted to a user will give them permission to remove all items from the relevant Common Item Access Groups. A Common Item Access Group created with Allowance Across Systems selected is subject to the Allowance Across Systems Override. Any other Common Item Access Group or Item Access Group on the same system will be unaffected by selecting this option. The option to enable the permission is performed in TrakaWEB.

Allowance Across Systems Override:

This option will allow access to all items in Allowance Across Systems Common Item Access groups on any of the relevant systems. It will not override the allowance limits on any other groups on those systems.

1. From the Users Page, select a User to whom you wish to grant the override permission and then navigate to the **Edit User** page.
2. Place a tick in the check box for **Allowance Across Systems Override.**

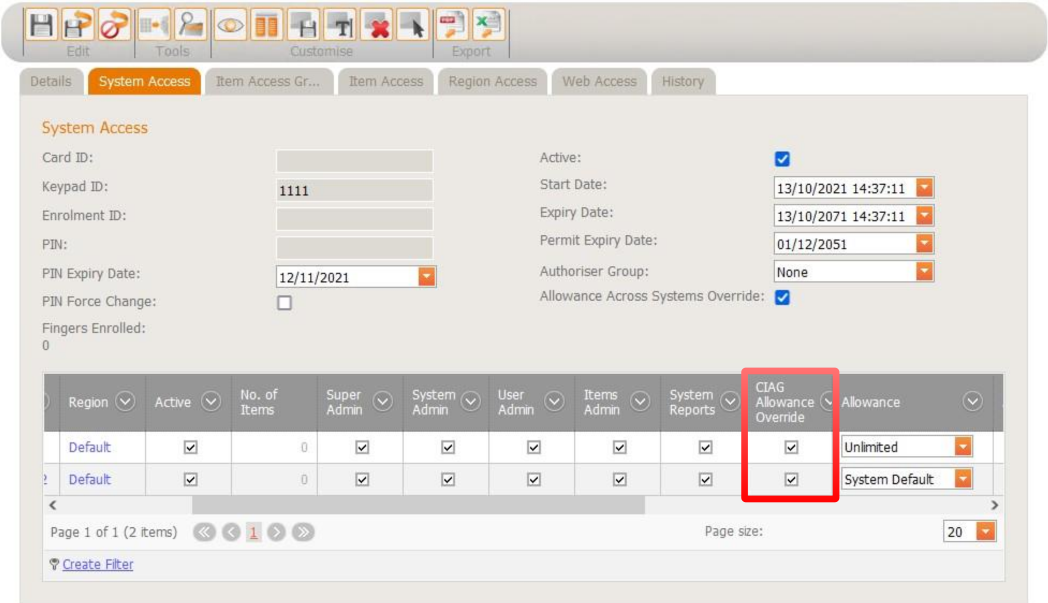


With the override permission enabled. The user will then be able to remove all the available items from across all systems.

CIAG Allowance Override:

This option removes the allowance limit for non-AAS Common Item Access Groups, so the user can now remove all items from their assigned groups.

From the System Access Grid, you can additionally choose to allocate a user with the **CIAG Allowance Override.** This will be applicable to non-AAS Common Item Access Groups on a specific system.



6.20 TRAKAWEB 16BIT SUPPORT

6.20.1 INTRODUCTION

For customers that already have a number of 8/16bit systems and want to purchase some additional Traka Touch systems, Traka is proposing to continue its development of TrakaWEB support for Traka Touch as well as support for 16bit systems.

6.20.2 FEATURES

6.20.2.1 CORE FEATURE SUPPORT

- TrakaWEB core functionality
- Support for 16bit Key Cabinets & Lockers (both non-RFID and RFID)
- Automatic event download (~30 seconds)
- Keypad ID, Card Reader support
- Access Levels as used on Traka32 will be converted to the equivalent Item Access in TrakaWEB
- Regions support
- Notifications (although notification rules will not automatically be imported)
- Integration via IEv2 only (LTTPS & RTUS not supported)
- Key Cabinet & Locker Fixed Return only initially
- Locking, non-locking, LED support Key Cabinet Receptor Strips
- No door, Single door, and Multi-door Key Cabinets supported
- FIFO on Lockers
- Item allowance (although Item allowance per access level not supported)
- Item & User Curfews. Relative curfews are limited to 24 hours on 16bit

6.20.2.2 NEW 16BIT FEATURES

- Sagem Biometrics enrolment at 16bit Systems will be implemented at the system using the Enrolment PIN method through TrakaWEB as available on Traka Touch
- iFob Setup for FR & RRSS will be implemented on 16bit via an Admin menu

6.20.2.3 UNSUPPORTED FEATURES

The following Communications features will not be supported:

- 8bit systems
- Serial and RS485 communications/protocol
- TCP/IP IPv6
- TCP/IP AES256 Encryption
- TACLS

6.20.3 PREREQUISITES

The following requirements must be met to allow 16bit support for TrakaWEB:

- The latest version of Traka32
- Requires 16bit systems with firmware version 4.00.12 or above for compatibility with TrakaWEB
- If a system is operating on an earlier software or firmware version, it will need to be upgraded to the versions above before migrating to TrakaWEB
- 8bit systems will need to be upgraded to 16bit first
- TCP/IP only will be supported. Systems using RS232 or RS485 will have to be upgraded with a Lantronix Xport or UDS2100
- The latest version of TrakaWEB

6.20.4 LIMITATIONS FOR 16BIT SYSTEMS

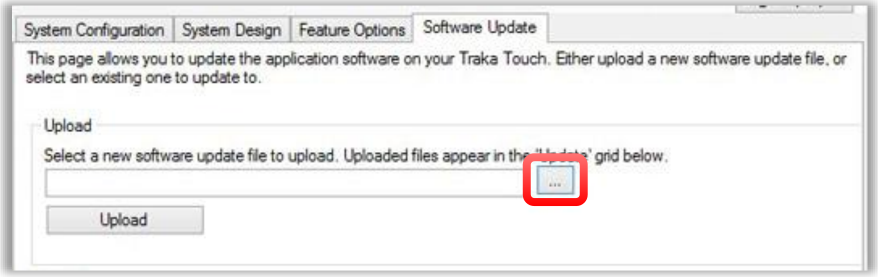
- 16bit Systems have a 70-character limit for descriptions
- Display names are limited to 17 characters
- Pin numbers have a 6-digit limit
- Simultaneous Keypad ID and Card ID is not supported
- Secondary PIN Support will remain limited on 16bit compared to Touch. E.g., multiple length PIN, PIN expiry, force PIN change on next login will not be supported on 16bit but only on Touch
- Authorisers are supported to a limited extent. To read more on that, refer to the Enable the use of X-System & X-iFob Authorisation on 16bit Systems section in this document
- New features available on Touch will not be supported on 16bit

6.20.5 16BIT FIRMWARE UPGRADE USING THE ADMIN APP

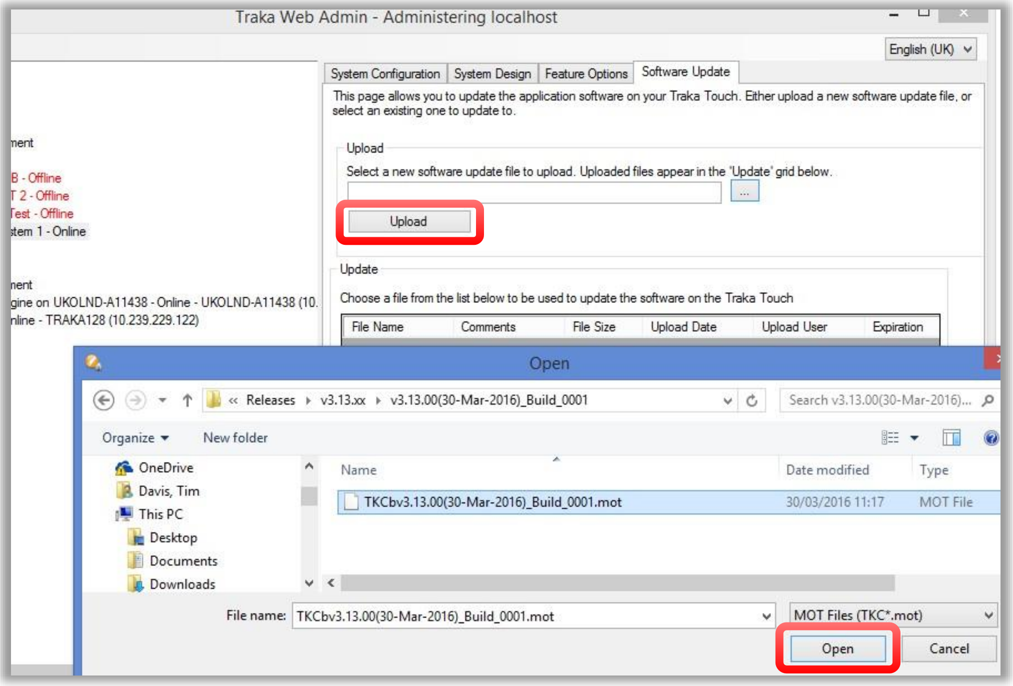
The process of upgrading the Firmware on a 16bit system using the Admin App is almost identical to the Traka Touch Application upgrade.

1. Within the Admin App, select the system you wish to upgrade the firmware to and then click on the **Software Update** tab.

2. Click on the button to the right of the grid as shown below. If the firmware version you require appears in the list, skip ahead to step 5.

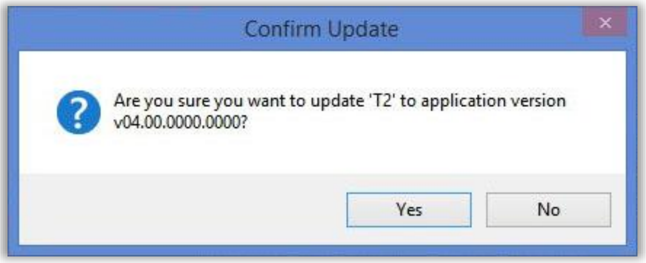


3. Navigate to the Firmware file to be uploaded and click on **Open**. The selected file will appear in the grid. Click on **Upload**.



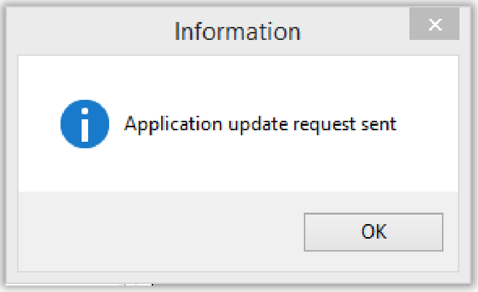
Clicking on upload will initiate the sending of the file to the database via the business engine.

4. Once the file has been uploaded, it will appear in the list.
5. Click on the row and then click on **Update System.**



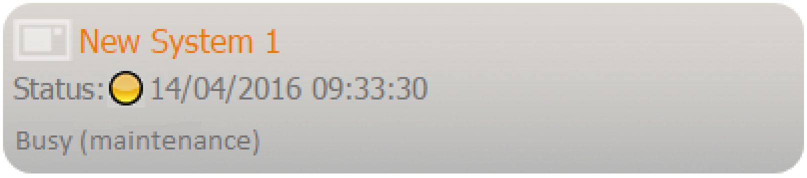
TrakaWEB will decide whether the new firmware requires a Full Upload after the upgrade process has completed. If you wish to force a Full Upload after the upgrade, see section 5.7 or 5.8.

6. Click the **OK** button to continue.



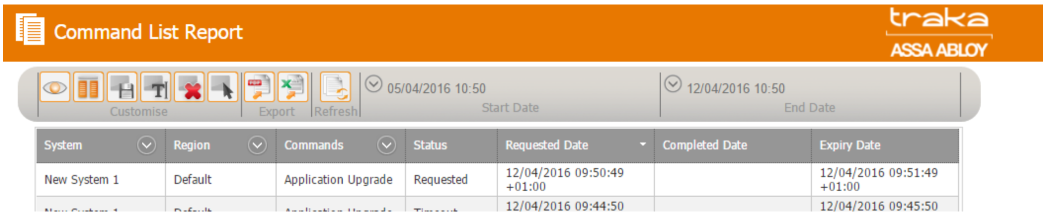
When the process begins, it can be viewed in the Admin App.

NOTE: The system will be unavailable during the upgrade process. The System View will show that the System is 'Busy'.



The Command List Report will also show progress of the upgrade.

1. Open the Command List Report in the Diagnostics report section. Each command can be expanded by clicking on the **+** sign to show the detailed Command Progress events that occurred during the Command processing at the system.



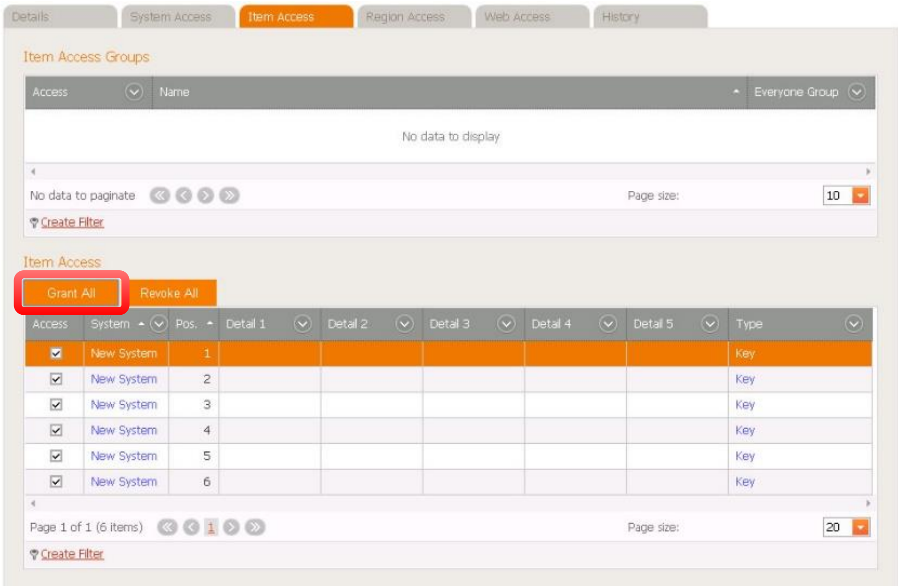
NOTE: The actual firmware upgrade process is the same as used by Traka32.

6.20.6 ITEM ACCESS

Before any items can be removed from the system, their access must be assigned to a user.

1. In TrakaWEB, select the User icon from the Navigation Toolbar.

2. At the Users' page, select the user you wish to edit or alternatively, double click on the username.
3. At the Edit User page, click on the **Item Access** tab.
4. The Item Access page will show all the items that can be allocated to that user. In the access column, select to assign individual items to the user or click on **Grant All** to assign all the items.



5. When the selection of items has been completed, click on Save to continue.

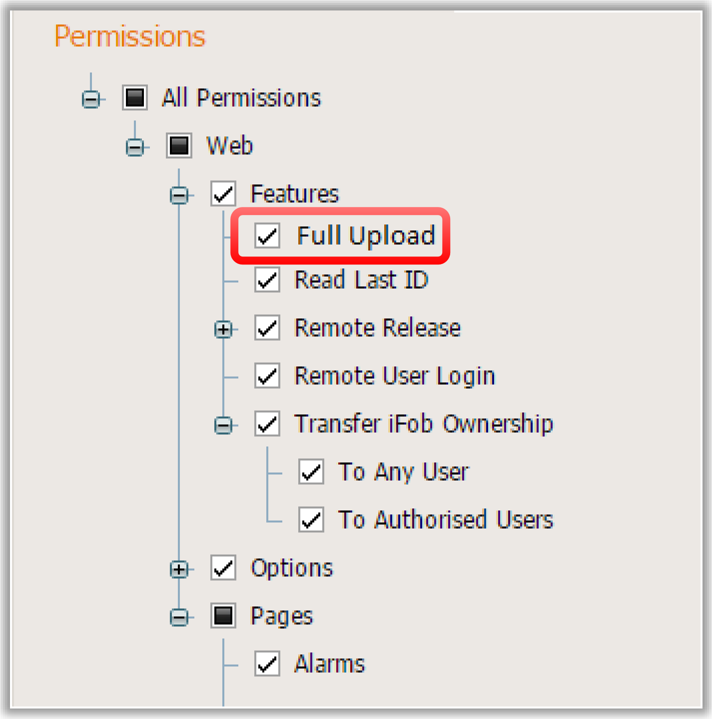
The user will now be able to remove items from the system using their Keypad ID, Swipe Card or Fingerprint.

6.20.7 PERFORMING A FULL UPLOAD FROM THE WEB CLIENT

NOTE: Only a user with appropriate permissions will be able to perform this task.

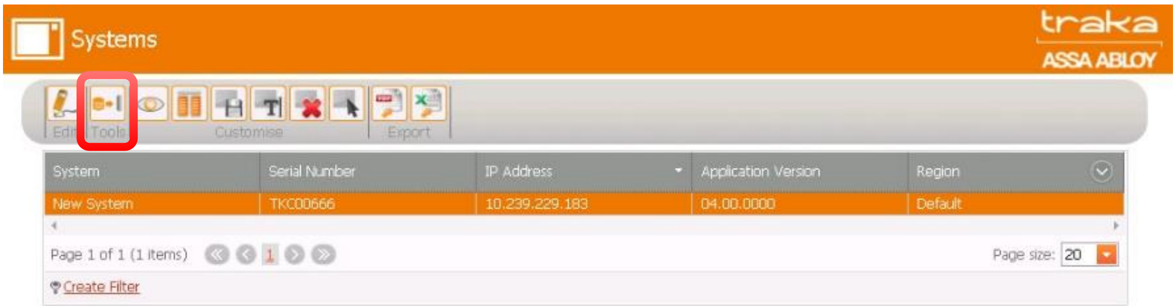
1. From The Navigation Toolbar, select **Software Permissions Groups**.

2. From the chosen Permissions list, click the check box next to **Full Upload.**



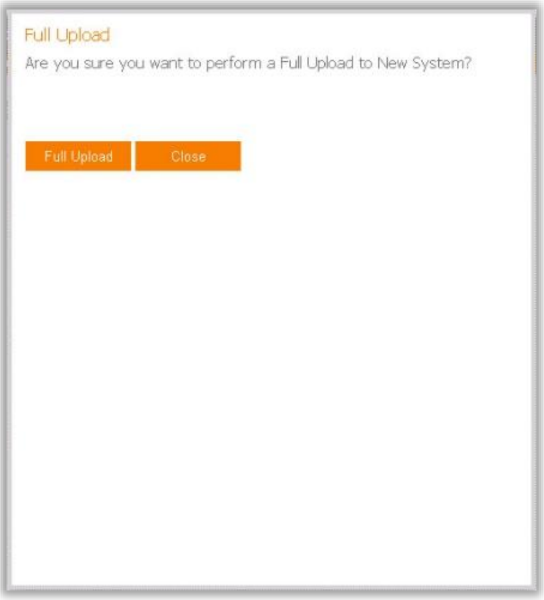
NOTE: For more information on using and assigning Permissions, refer to section 3.6.5 – Software Permissions Groups.

3. To perform a Full Upload on a 16bit system from TrakaWEB Client, select the system in the grid and click the **Full Upload** button.

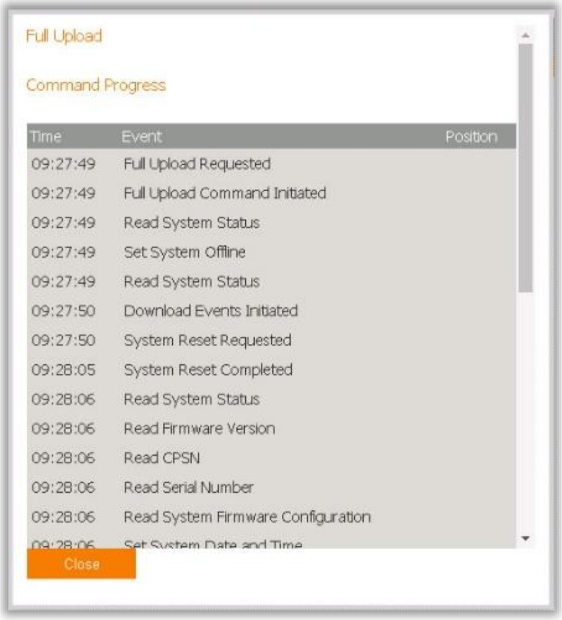


NOTE: This function will only be effective on a 16bit system.

4. At the next confirmation window, click on **Full Upload** to continue.

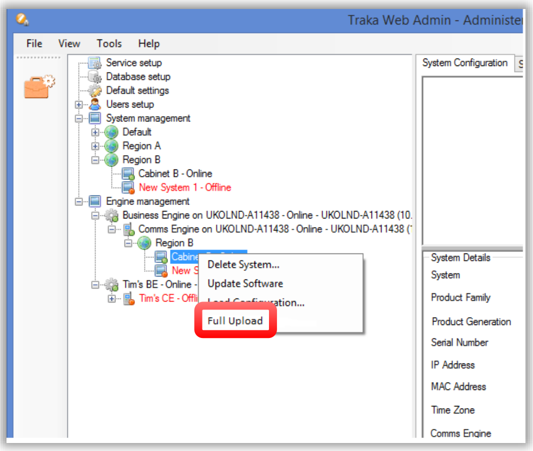


5. The command progress window will be displayed once the Full Upload is complete, click on **Close** to continue.

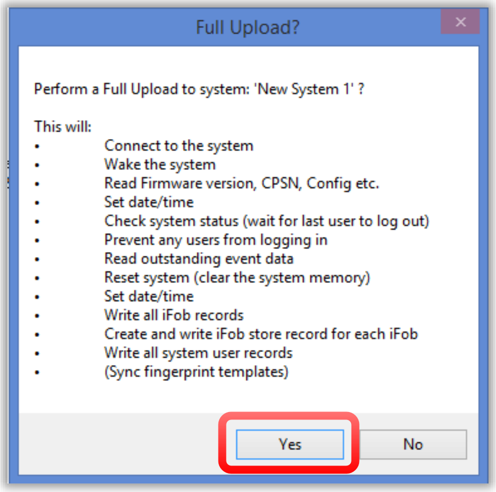


6.20.8 PERFORMING A FULL UPLOAD FROM THE ADMINISTRATION APPLICATION

1. From within the Admin App, right click on the 16bit system and select the **Full Upload** option.



2. At the next window, click **Yes** to confirm the Full Upload.



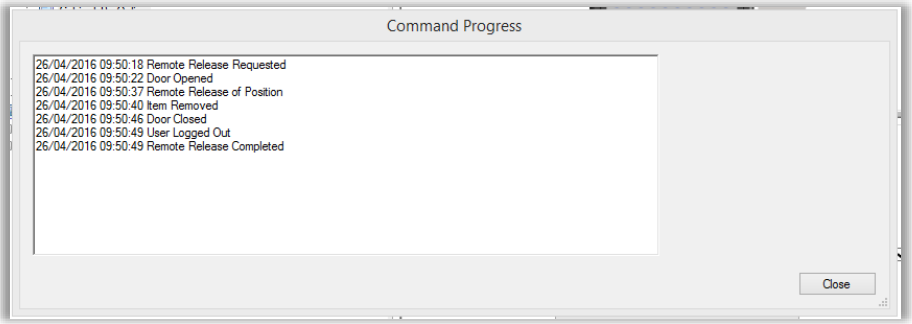
NOTE: If the system is in use at the time the Full Upload command is given, the system will wait for the user to logout before beginning the process.

NOTE: If the system is performing AutoComms when the Full Upload command is given, it will be cancelled at the earliest point that is safe to do so.

NOTE: Once the Full Upload process starts, the system will prevent any users from logging in.

A Command Progress window will now appear. The upload process can take several minutes to complete.

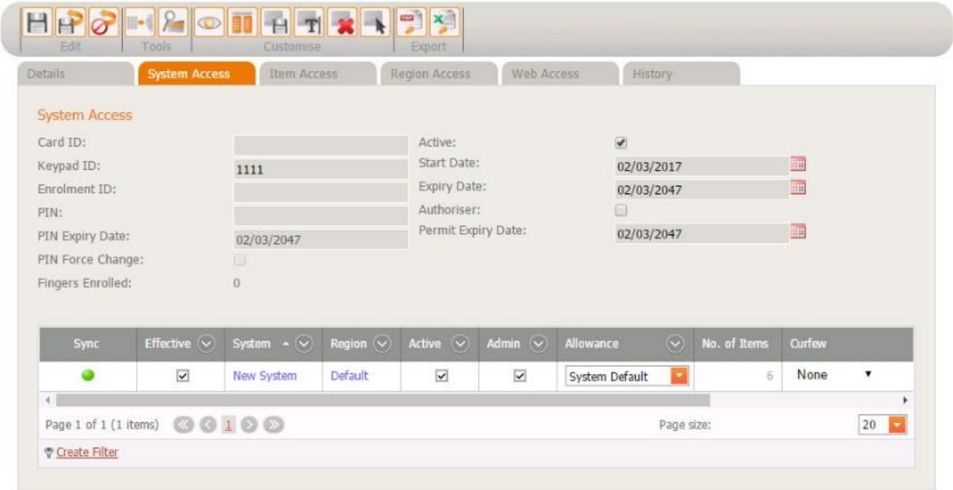
3. Once the Full Upload has completed, click on the **Close** button.



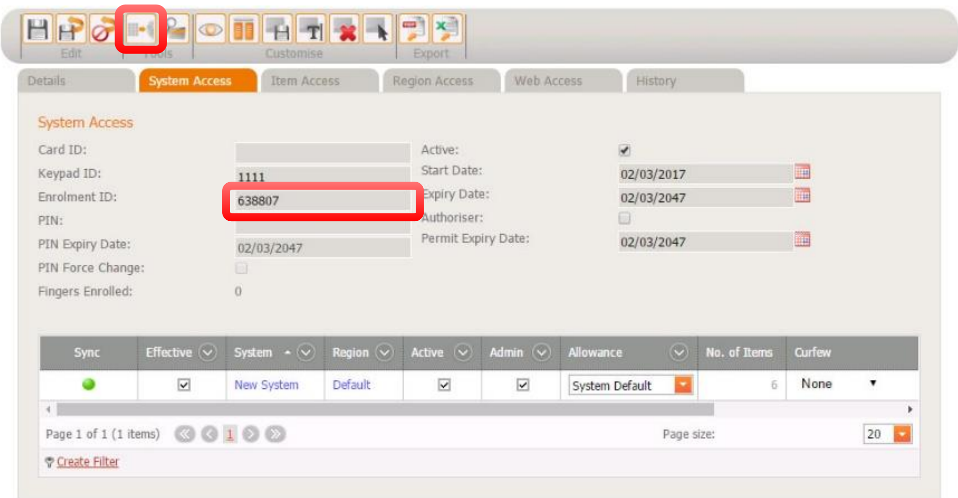
6.20.9 ENROL A BIOMETRIC TEMPLATE ON A 16BIT SYSTEM

Users with User Edit Permissions can allocate an enrolment ID to other users. The Enrolment ID is a 6-digit number, which can be created manually or randomly. A user can then access the system with their enrolment ID to enrol their fingerprint.

1. Select the user you wish to grant an enrolment ID to and select the **System Access** tab within the Edit User page.



2. The Enrolment ID can be entered either manually into the blank field or by clicking on the **Random Enrolment ID** button. Once completed, click on the Save button to continue.



3. At the 16bit System, press the **0** button on the keypad. The screen will display the following message:

4. Enter the 6-digit Enrolment ID followed by the **#** key.

If the 6-digit enrolment number is valid, the following screen will be displayed:

5. Press the **#** key on the keypad and then follow the on-screen instructions for enrolling a fingerprint using the biometric reader.

Once completed, the following screen will be displayed:

NOTE: To access the system, the user first presses the # key and then places their finger on the reader.

6.20.10 SYNCHRONISING AND DOWNLOADING EVENTS WITH THE 16BIT SYSTEM

The Comms Engine will ensure that the 16bit system is kept updated by performing the following processes every 30 seconds:

- Making sure that the system is online and ready
- Making sure that the Firmware Version number is compatible
- Making sure that the Date & Time is set correctly
- Making sure that the CPSN has not changed
- Reading new events from the System
- Sending the changed User records to the system
- Sending the changed iFob records to the system
- Sending the changed User Biometric templates to the System

There will be certain constraints placed upon some of the data sent to the 16bit systems compared with Traka Touch. These include:

- iFobs and Items allocated to a 16bit System will have their descriptions limited to a maximum of 70 characters when edited in TrakaWEB. If an iFob/Item is moved from a Traka Touch system to a 16bit System, the description will be truncated if it exceeds 70 characters.
- If you have one or more 16bit Systems in your database, the maximum allowable length of the User Display Name field is 17 characters. If the Display Name Override tick box is not ticked and the automatically generated name is longer than 17 characters, it will be recalculated before being sent.
- Pin numbers will be limited to 6 digits.
- Due to the fact that 16bit systems store a unique key that will remain identical across all 16bit systems, there can be no more than 65,535 users active across all 16bit systems at any one time. TrakaWEB will allocate a unique key that will remain identical across all 16bit systems. Traka Touch is not affected by this limitation.

6.20.11 USING A TRAKAWEB KEYPAD ID/CARD ID WITH OPTIONAL PIN ON 16BIT SYSTEMS

16-bit Cabinets support identifying users with either a card reader or the numeric keypad. This is determined by the Reader configuration supplied by the Traka Technical Support Department.

Similarly, TrakaWEB supports a Card ID and a Keypad ID, which can be entered in the user System Access tab on the Edit User page. The main difference is that TrakaWEB will support having users with both simultaneously and can be configured for both systems with readers and systems without readers.

The following rules will apply.

16bit Firmware with Card Reader Enabled without 'Card and/or PIN' Option

Fields in TrakaWEB

- Keypad ID is not used
- If the 16bit System has a Card Reader configured, TrakaWEB maps the Card ID field to the **Primary ID Field**
- TrakaWEB maps the PIN field to the **Secondary ID Field.** (The system will only prompt for the Secondary PIN if it is supplied)

Behaviour at Cabinet

- **Card ID only:** System will accept Card without a Keypad ID
- **Card ID & PIN:** System will accept Card and prompt for PIN

16bit Firmware with Keypad Only Configuration

NOTE: The 'Card and/or PIN' option is not designed to be used with keypad only systems.

Fields in TrakaWEB

- The Keypad ID is the Primary PIN
- The Card ID field is not used
- The PIN field is used for Secondary PIN (This is optional – The system will only prompt for Secondary PIN if supplied)

Behaviour at Cabinet

- **Keypad ID only:** System will accept Keypad ID
- **Keypad ID and PIN:** System will accept Keypad ID and prompt for PIN

16bit Firmware with Card Reader & 'Card and/or PIN' options

WARNING: If switching the 'Card and/or PIN' option on or off on an existing system, a full sync must be carried out to ensure that the correct data is synchronised with the system.

NOTE: There is no option available on 16bit to enforce both Card *and* PIN if the keypad ID is not supplied.

Fields in TrakaWEB

- Keypad ID is optionally used for Primary PIN
- Card ID Field is used for Cards
- PIN Field is optionally used for Secondary PIN

Behaviour at Cabinet

- **Card ID Only:** System will accept Card without a Keypad ID
- **Keypad ID Only:** System will accept Card without a Keypad ID
- **PIN Only:** Not Supported
- **Card ID and Keypad ID supplied**
    - System will accept Card *and* Keypad ID *or*
    - System will just accept Keypad ID only
- **Card ID and PIN supplied**
    - System will accept Card *and* PIN

NOTE: The user will not be able to access the system with just their PIN.

NOTE: This underlying "User requires Card *and* PIN to access Cabinet" flag would be set in this case.

- **Card ID and Keypad ID and PIN supplied**

NOTE: This is not a valid combination for 16bit and so would behave just like a Card ID and Keypad ID being supplied. I.e., The PIN will be ignored.

6.20.12 16-BIT SYSTEM SUPPORT FOR ALL CARD READERS AND INTERFACES UNDER TRAKA32

As all of the Card-Reader configuration and data is handled solely within the 16-bit firmware, TrakaWEB will support all of the current and foreseeable Card-Reader and hardware interfaces.

Card-reader configuration settings which are contained within the 16bit configuration file are always sent unchanged to the 16bit system.

6.20.13 10-WAY RECEPTOR STRIPS SUPPORTED BY THE CURRENT 16BIT FIRMWARE

The available options are as follows:

- 10-way only
- Locking
- Non-Locking
- Mixed Locking and Non-Locking

NOTE: The 16bit firmware will only support a single consecutive group of Non-Locking strips anywhere in the cabinet.

6.20.14 16BIT ABSOLUTE OR RELATIVE ITEM AND USER CURFEW FEATURE

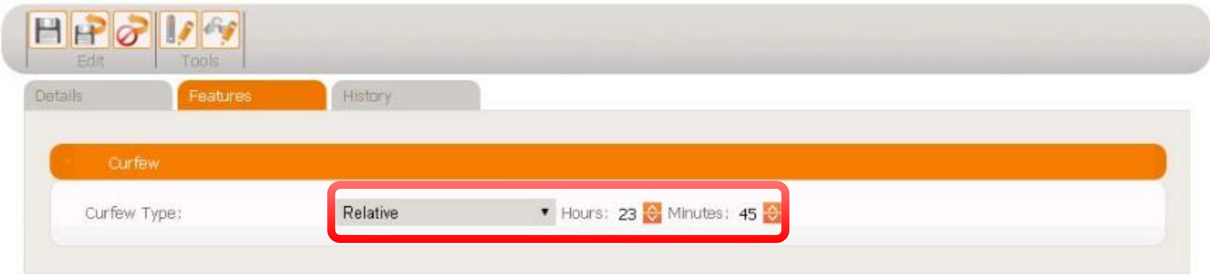
This section explains the functionality of Absolute and Relative Curfews on a 16bit System. It also explains the differences between Curfews on 16bit and Traka Touch systems.

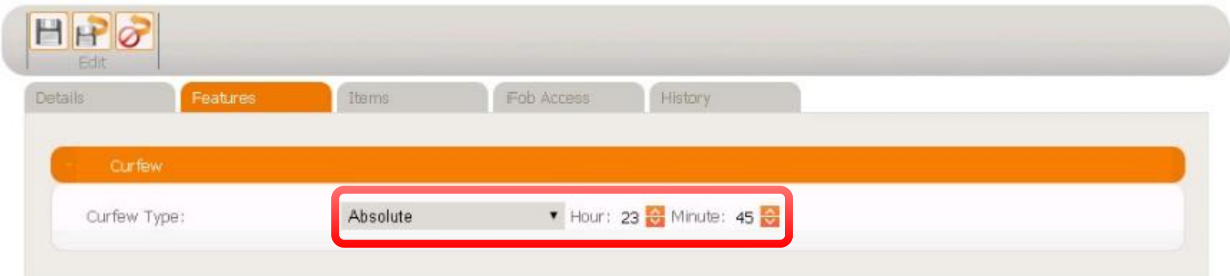
This feature will use the existing 16bit firmware iFob and User Curfew feature.

NOTE: For a complete guide to Traka Touch Curfews, refer to Section 3.11

6.20.14.1 IFOB CURFEW

When editing an iFob from a 16bit system, the settings will only allow up to 24 hours for a Relative Curfew and 23 hours and 45 minutes for an Absolute Curfew, both in 15-minute increments.

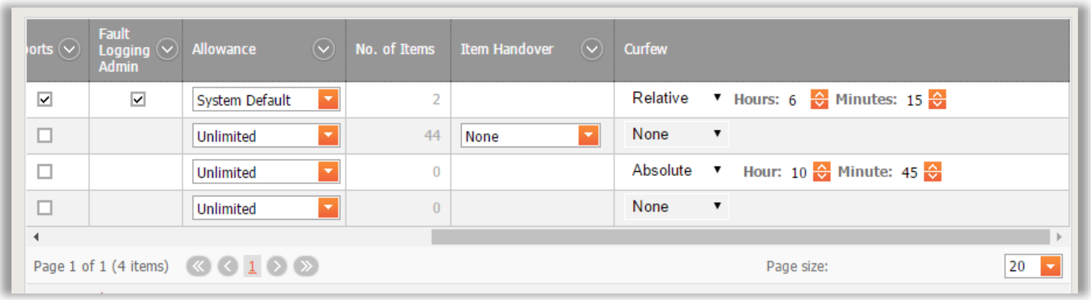




When editing an iFob from a Traka Touch system, the settings will allow up to 365 days, 23 hours and 59 minutes for a Relative Curfew and up to 23 hours and 59 minutes for an Absolute Curfew.

6.20.14.2 USER CURFEW

Like iFob Curfews, User Curfews are set on a 'per-system' basis and so for 16bit systems, the Absolute Curfew is limited to 23 hours and 45 minutes and a Relative Curfew is limited to 24 hours in 15-minute increments as shown below.



For a Traka Touch system, like iFob Curfews, User Curfews are set on a 'per-system' basis. A Relative curfew can be set for 365 days, 23 hours and 59 minutes and up to 23 hours and 59 minutes for an Absolute Curfew.

NOTE: Traka Touch Curfews are not limited to 15-minute increments. If, for example an iFob with a Curfew is set for 05:20 on a Traka Touch system and is returned to a 16bit system, the time will be rounded down to 05:15.

NOTE: Relative Curfews on Traka Touch can be set for up to 356 days, 23 hours and 59 minutes. Relative Curfews on a 16-bit system have 23 hours and 45 minutes. Any days will be set to zero at a 16-bit system if a curfew was set on a Traka Touch system for over a day.

6.20.15 REMOTE RELEASE AN ITEM TO AN AUTHORISED OR ANONYMOUS USER

This will use the existing Remote Release Toolbar function on the TrakaWEB System Viewer. For more information, refer to **section 3.2.3.1**

6.20.16 USE 'REMOTE USER LOGIN' TO LOGIN A USER TO A 16BIT SYSTEM

This will use the existing Remote User Login toolbar function on the TrakaWEB System Viewer. For more information, refer to **section 3.2.3.2**

6.20.17 READ THE LAST CARD ID PRESENTED TO A 16BIT SYSTEM WITHIN A USER RECORD

This will use the existing Read Last ID Toolbar function on the Edit User page. For more information, refer to **section 3.3.2**

6.20.18 TRANSFER THE OWNERSHIP OF AN ITEM FROM ONE USER TO ANOTHER

This will use the existing Transfer Ownership Toolbar function from the TrakaWEB System Viewer. Refer to **Section 3.2.3.3**

6.20.19 USE 16BIT FIRMWARE ONLY FEATURES

These Firmware only features will affect cabinet operation but have no operational effect within TrakaWEB.

The Firmware Only Features are as follows:

- Fixed Return to a Single System (FRSS)
- Key Cabinet with Single Door
- Key Cabinet with Multiple Doors (Extension Cabinets)
- Key Cabinet Open all Doors on Login
- Key Cabinet without a Door
- Receptor Tri-Colour LEDs
- Receptor Button Release
- 16bit Keypad Release

- 16bit Description Release
- 16bit Key Cabinet Auto Release Multiple Items
- Anti Passback
- CAN Gateway
- Non-RFID Rotation Auto Allocation

6.20.20 ENABLE THE USE OF X-SYSTEM & X-IFOB AUTHORISATION ON 16BIT SYSTEMS

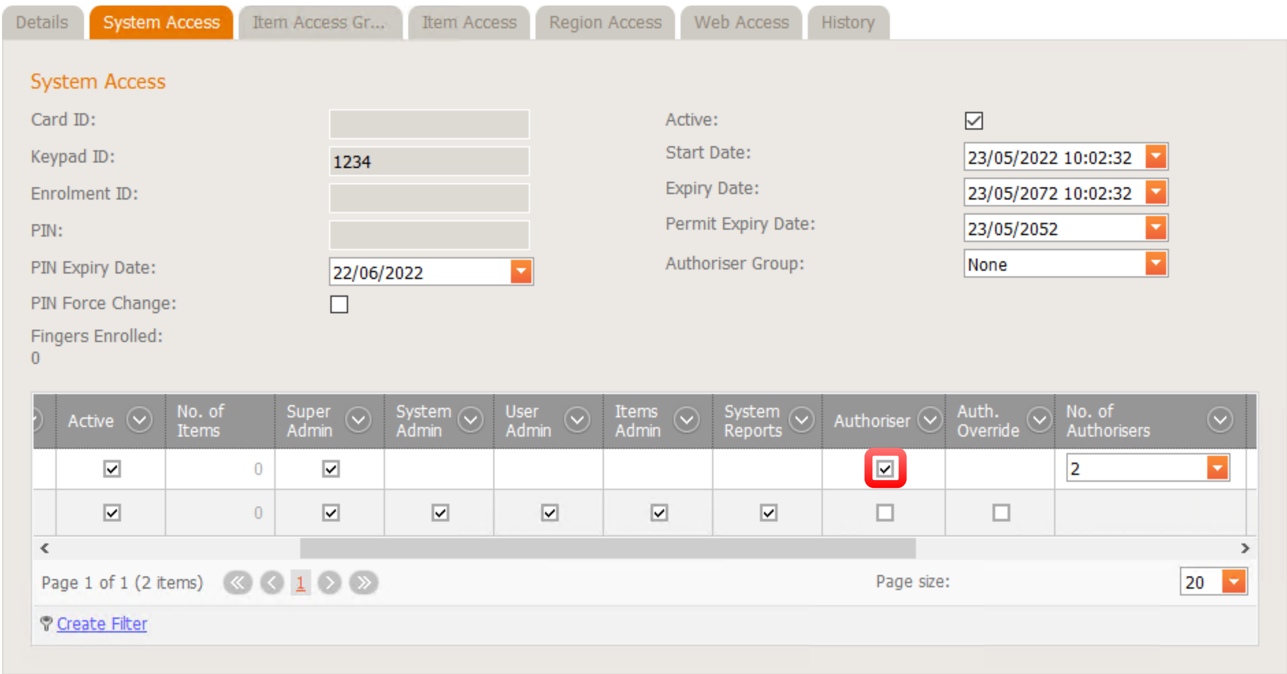
NOTE: This must first be enabled within the configuration setup before it can be used. A config can be created for either X-iFob or X-System Authorisers, or both.

NOTE: Traka Touch will only support iFob Authorisation and not System/User Authorisation.

NOTE: iFobs on 16bit systems will only be able to have the 'Authorisers' set to a maximum of 2, whereas Traka Touch will allow up to 3.

The Item Authoriser enables a user to become an Authoriser to other users and allows the user to override the Item Authorisation feature. This will allow them to take items without requiring authorisation.

1. Select the user that will be set up as an Authoriser.
2. At the System Access page check the box in the Authoriser column for the 16bit system in your network and then click the Save button.

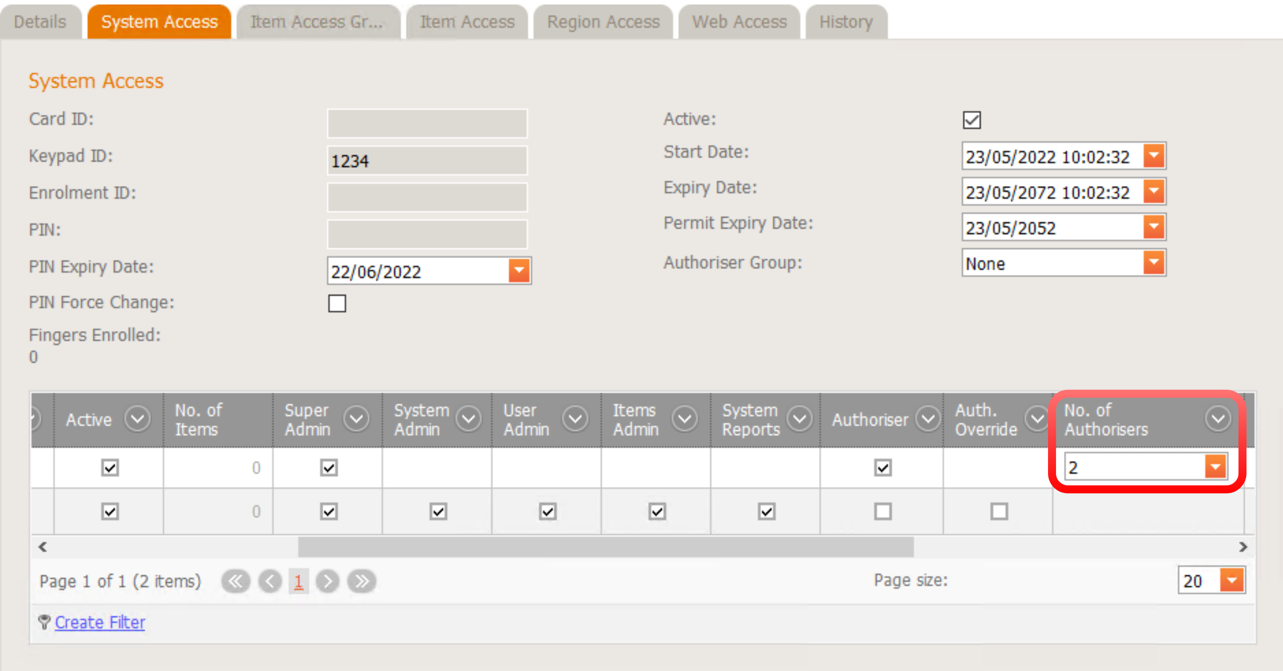


NOTE: Authorisers can be nominated on 16bit systems and they will be able to authorise non-authorisers. However, when an Authoriser user logs in, the system will allow them to authorise themselves (the function of "Denying Single Access Authoriser Access" from Traka32 is not supported on 16bit systems connected to TrakaWEB). As a result, the functionality works as follows:

- **If the system or iFob authorisation is set to 1, the system will release the iFob automatically**
- **If the system or iFob authorisation is set to 2, the system will require only one more Authoriser to confirm the iFob removal.**

6.20.21 SYSTEM AUTHORISATION

1. In TrakaWEB, select the user that will be required to have authorisation to access the 16bit system.
2. At the System Access page, select the number of Authorisers that will be required from the drop-down menu and then click the save button.

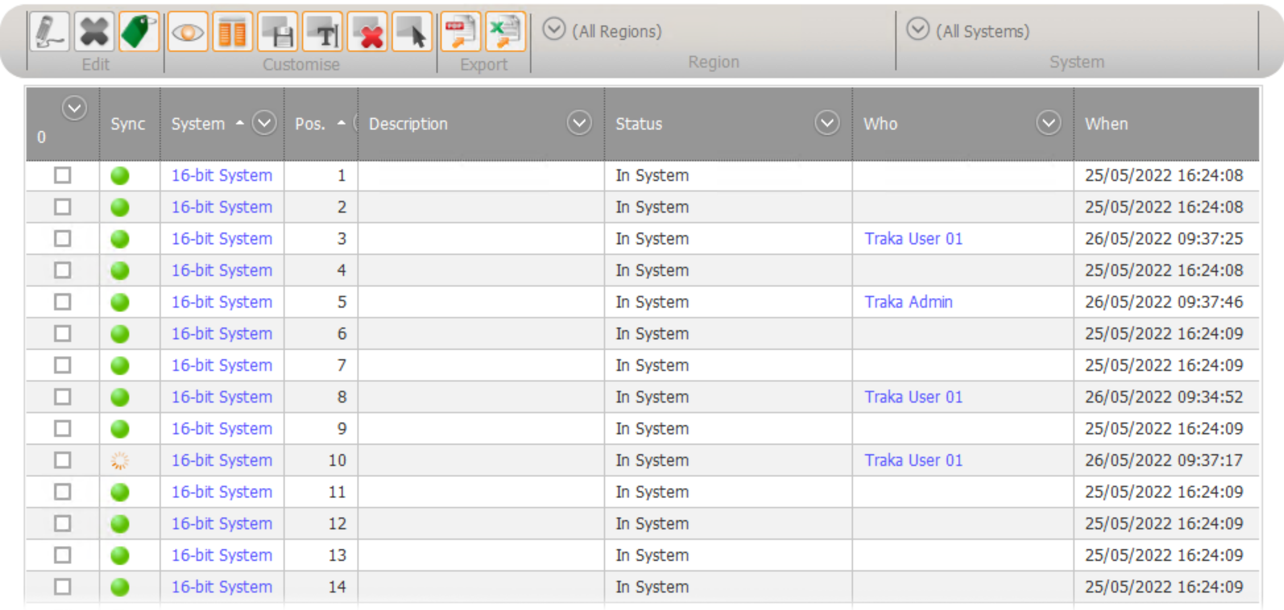


When the user attempts to access the 16bit System using keypad, swipe card or fingerprint, an authorised user will be prompted to identify themselves first, before the system can be accessed.

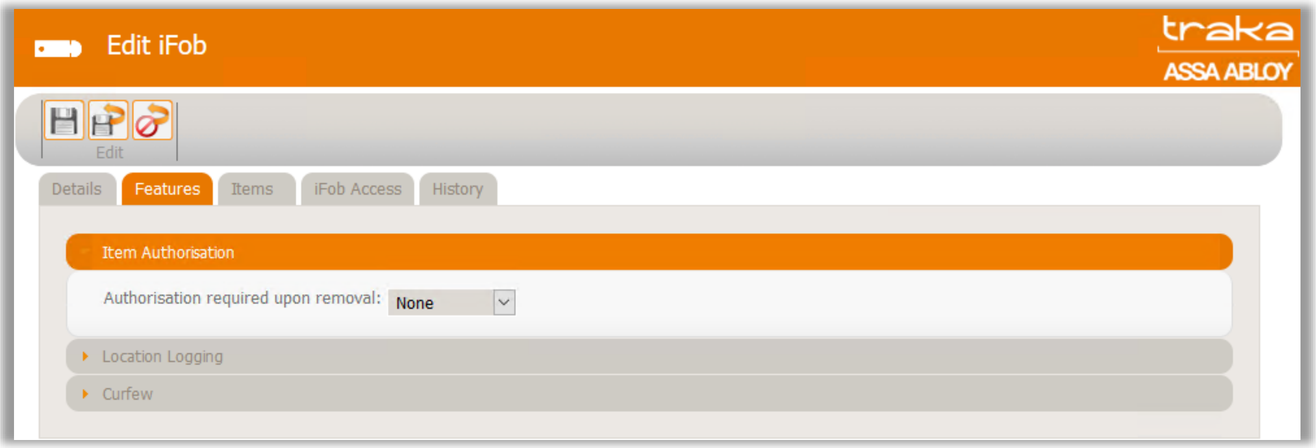
6.20.21.1 IFOB AUTHORISATION

1. Select the iFobs icon from the Navigation Toolbar.

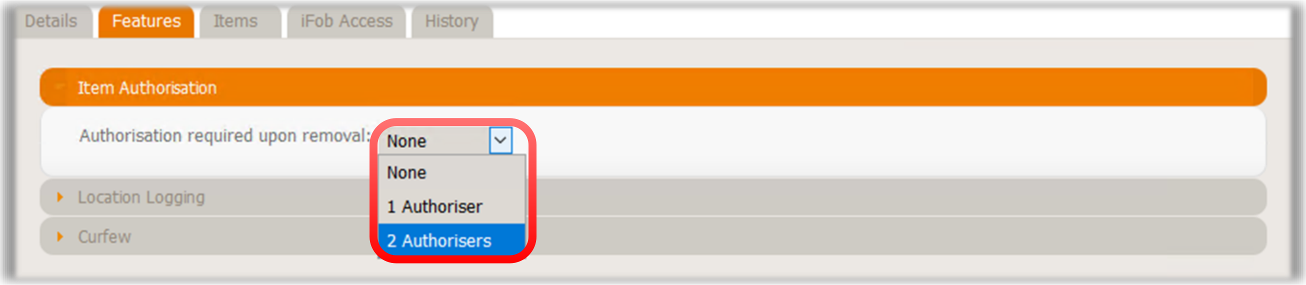
2. Double click on the iFob that will require the Authorisation permission to be added to it.



3. At the Edit iFob page, navigate to the Features tab and expand the Item Authorisation option.



4. Select the number of Authorisers from the drop-down menu, then click the Save button.



When a user who requires iFob Authorisation attempts to remove the iFob from the system using keypad, swipe card or fingerprint, an Authoriser will be prompted to identify themselves at the system first, before the iFob can be removed.

6.20.22 LOCATION LOGGING (BAY LOGGING)

NOTE: This section covers Location Logging using TrakaWEB with a 16bit System. For information regarding its functionality with Traka Touch, refer to section 4.7 – Fuel, Distance & Location Logging.

Location Logging or **Bay Logging** as it is also referred to, will allow users to record the current location of an asset.

Every time a user returns an iFob they will be prompted to enter a location. The user can use the keypad like a mobile phone keypad to enter letters and numbers to make up a location description.

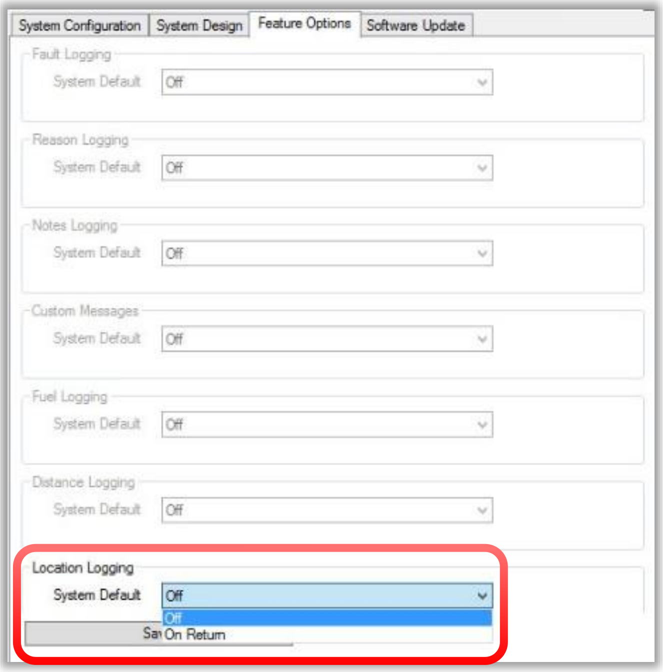
NOTE: The location description is limited to 5 characters.

The location can be looked up at any time using the Lookup Facility. For more information on this facility, refer to the Traka32 User Guide. Event reports will also be generated and can be accessed through the Reports page in TrakaWEB.

NOTE: Location Logging will only be available if the firmware of the selected system has the 'Bay Logging' configuration option enabled. If the Bay Logging option is enabled in the firmware, it is possible to enable/disable the option on any iFob in TrakaWEB and change the default option value for all iFobs in the TrakaWEB Admin Application.

6.20.22.1 ENABLING THE OPTION

1. The Admin Application is used to set the default option to on or off for all items in that system. An administrator who has the appropriate access to the Admin Application will need to select the desired system and navigate to the **Feature Options** tab. Once selection has been completed, Click **Save**.

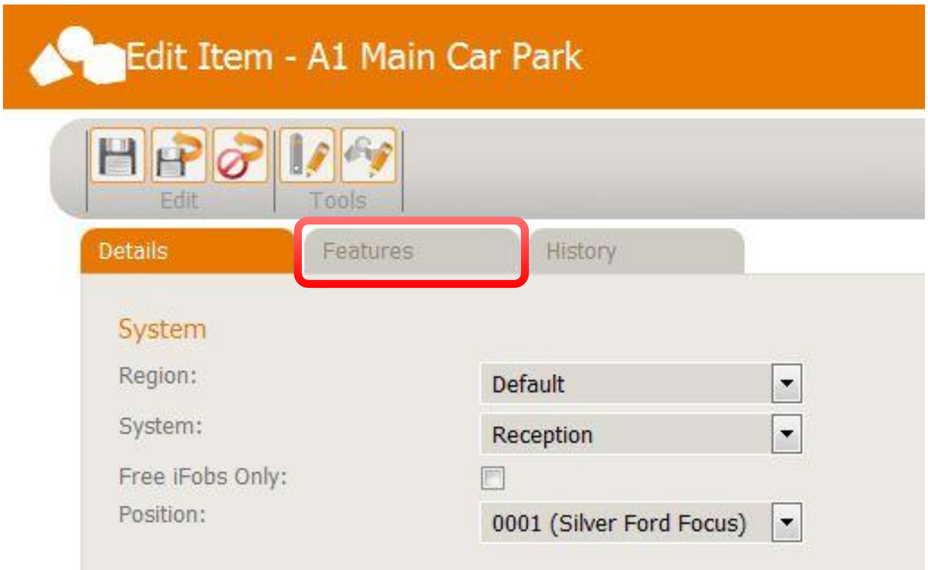


NOTE: Enabling the feature in TrakaWEB Admin will set all items in the system to have the feature active.

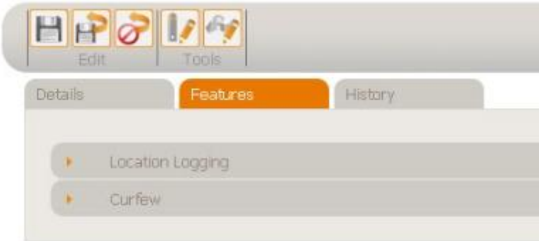
Alternatively, the feature can be activated within TrakaWEB through the **Features** tab.

2. From the System Viewer, select **Edit Item**.

3. At the next window, select the **Features** tab.



Within the **Features** tab, you will see a list of all the Feature Options that are available.



NOTE: If you choose to enable the feature through TrakaWEB, it will only be available on the current selected item. Depending on how many items you wish to have the feature enabled upon, it may be more time efficient to enable it in TrakaWEB Admin and then disable it on any items you don't want it enabled upon in TrakaWEB. If however, you have many items and only wish the feature to be enabled on a few, it will be more time efficient to enable it on those items in TrakaWEB.

With the feature enabled, TrakaWEB will display the Current Location if one has previously been entered at the system.

6.20.22.2 REMOVING AN ITEM

When a User removes an item from the 16bit system, the screen will display the last location of the vehicle for that particular slot.

6.20.22.3 RETURNING AN ITEM

When a User returns an item to the 16bit system, they will be required to enter details of the vehicles current location followed by pressing the **#** key.

As well as using the Lookup facility through the 16bit system, the location information can be viewed through TrakaWEB in a number of ways.

- The System Viewer
- The Current Location on the Features page
- Viewing the Current Location Report

NOTE: An Exception report will be generated if a user does not enter a location. This will also be reflected in the Item Activity tab on the System Viewer page.

NOTE: For more information on Location Reports, refer to Section 4.7.1.6 – Reports, within the Fuel, Distance & Location section of this document.

6.20.23 NON-RFID AUTO ALLOCATION SUPPORT

16Bit systems include a feature for lockers which will auto-allocate locker compartments. This feature is now supported by TrakaWEB. This is similar to a Personnel Locker whereby a non-RFID equipped locker system can be used to store a users' items over a period of time as required.

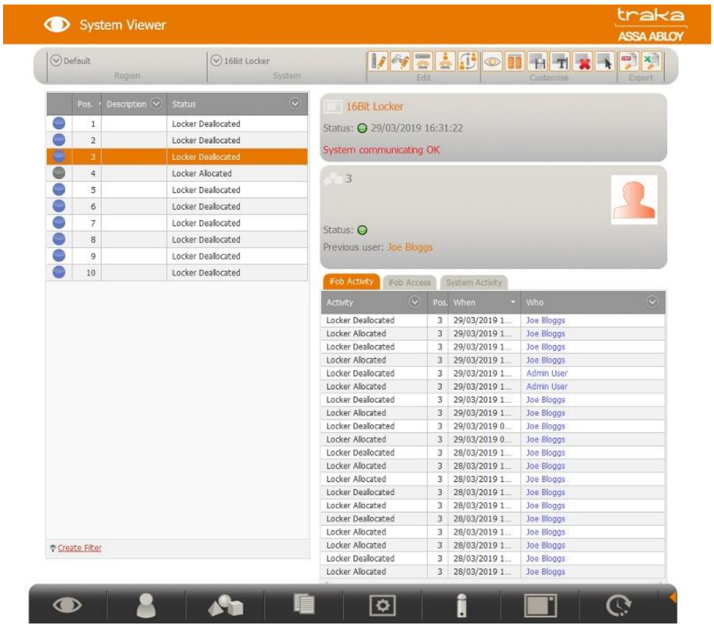
When a user accesses the system, a vacant compartment is made available to the user. Should they choose to, they can select another vacant compartment.

Two different statuses are created for each position in the locker depending on whether that particular compartment is occupied or unoccupied.

For an allocated compartment, the icon within TrakaWEB will be displayed by a grey icon.

For a deallocated compartment, the icon within TrakaWEB will be displayed by a blue icon.

A typical example of the TrakaWEB System Viewer with allocated and deallocated locker compartments is shown below.



Two new events are generated in the event of an allocation/deallocation:

Locker Allocated Event

The Locker compartment now contains a users' items. This event is generated by receiving a 'Locker Occupied' event from the 16Bit system.

Locker Deallocated Event

The Locker compartment is now vacant and once again available. This event is generated by receiving a 'Locker Unoccupied' event from the 16Bit system.

6.20.2416 BIT FIRST IN/FIRST OUT (FIFO) ON TRAKAWEB - OVERVIEW

Although Traka 16bit systems were designed to run using Traka32 software, TrakaWEB does offer limited support for them. On a 16bit locker, the asset manager works like a combination of FIFO & AFIFO. It will allow a user to hold multiple items at once, however they will only be able to take or return the items one at a time. The CIAG allowance feature is not supported by TrakaWEB when using a 16bit system. 16bit systems will need to have a firmware version of 4.0.12 or above for compatibility.

For more in-depth information on 16bit FIFO on TrakaWEB, please refer to **UD0232 – TrakaWEB FIFO and Advanced FIFO User Guide.**

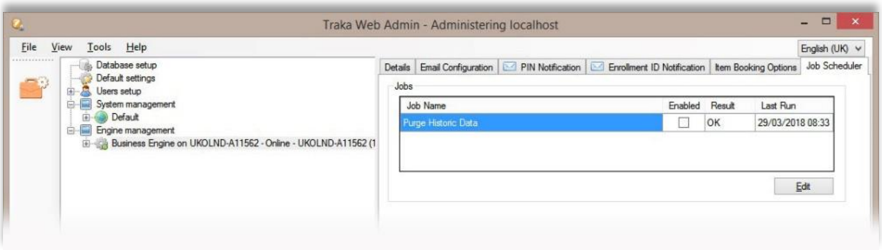
7. TRAKAWEB ADMIN JOB SCHEDULER

NOTE: As of TrakaWEB version 3.3.0, the TrakaWEB Admin Job Scheduler replaces the requirement for the TrakaWEB Database Purge Batch File – TD0103. Users of previous versions of TrakaWEB should still refer to this.

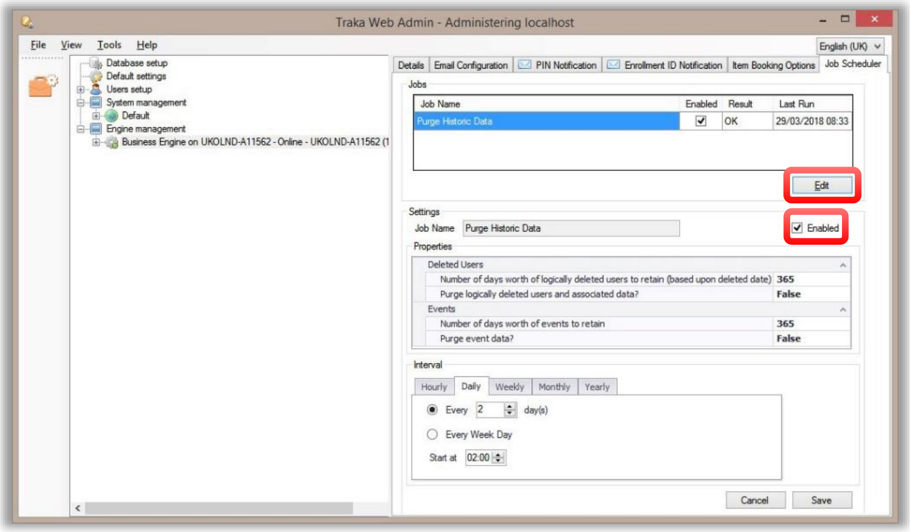
Within the TrakaWEB Admin App, it is possible to configure a Job Scheduler. This will make it possible to clear data from the system at specific times, which can be enabled by the System Administrator.

The tab for the job scheduler is located by selecting the Business Engine. By default each job schedule will be disabled.

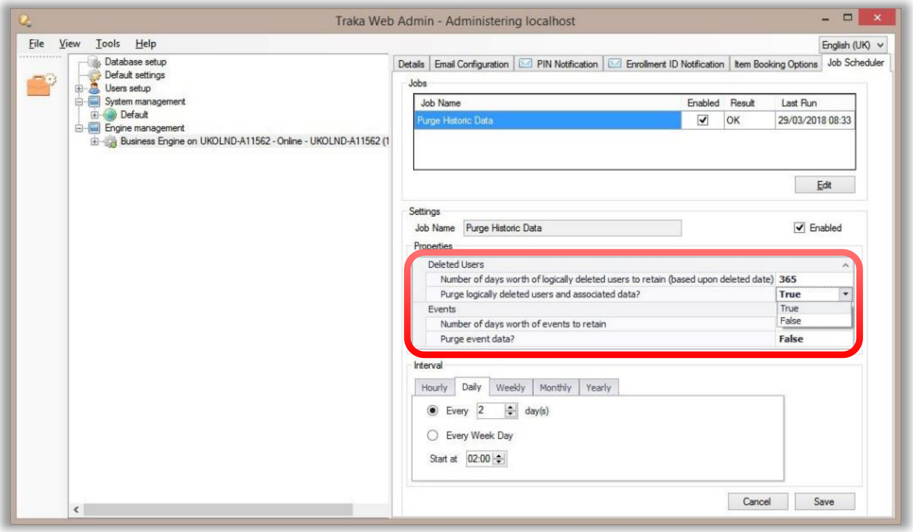
1. Select the **Business Engine** followed by the **Job Scheduler** tab.



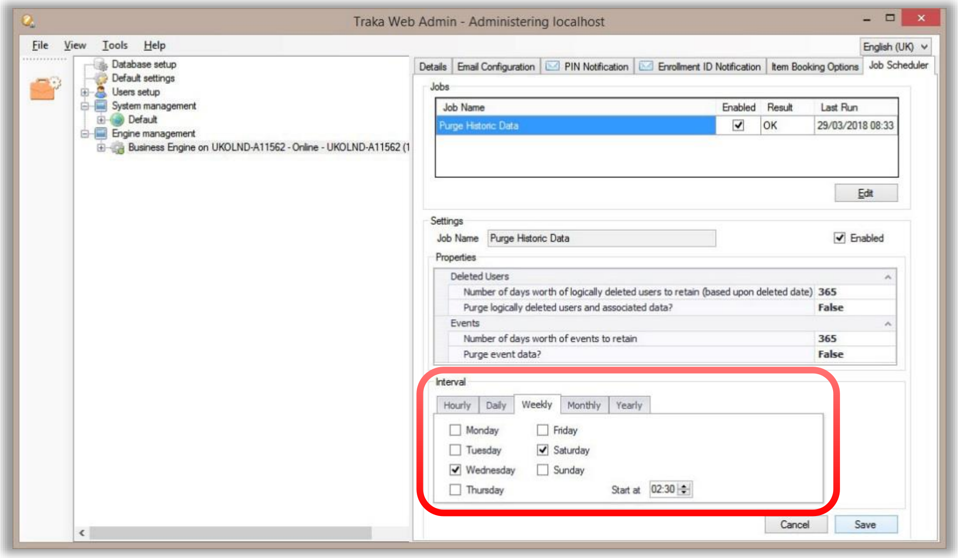
2. Clicking on the **Edit** button will allow you to change the parameters for the selected Jobs. Placing a tick in the **Enabled** checkbox will enable the jobs in the list.



3. Within the Properties box, change the setting to **True** to enable the parameter.



4. The lower box will allow you to change the interval for when you wish the Schedule to be run.



5. Once complete, click the **Save** button.

8. TWDI – TRAKAWEB DATA IMPORT

The TWDI process describes the procedure for migrating database information such as Items, Item Access Groups and Users from an existing Traka32 system or a manually created database into TrakaWEB as required.

The database is exported from Traka32 into an Excel Spreadsheet which can then be imported to TrakaWEB via the Admin App. Unfortunately, it is not possible to migrate all of the database information such as Access Schedules and RRMS.

It is recommended that the Traka32 database is backed up before proceeding to export the database and the 16-bit system is only disconnected after the export process is completed.

For more information on TWDI please refer to **TD0155 – TrakaWEB Data Import & Traka32 Data Export Procedure**

For your assistance with the Traka32 Data Export/TrakaWEB Data Import procedure, please refer to **TV0052 – Traka32 Data Export_TrakaWEB Data Import Online Help Tool.**

9. DISABLE & CLEAR AUTOFILL INFORMATION

9.1 OVERVIEW

If the autofill options have not been disabled in your web-browser, the Username and Password information will be displayed when you next access the login screen. This section will show you how to disable the autofill options in some of the more popular web-browsers to prevent this information from being unintentionally saved or used in your browser.

The web-browsers covered in this section include:

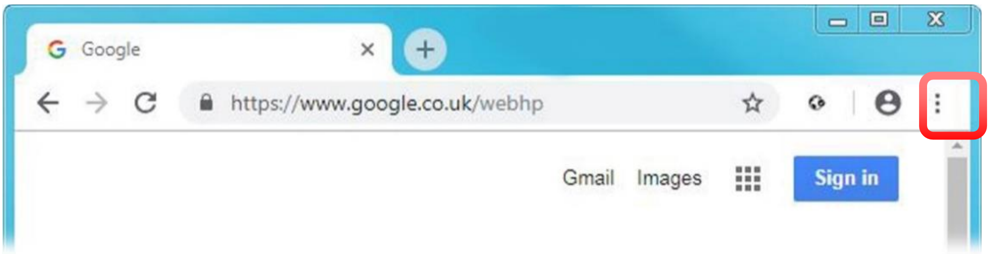
- Google Chrome
- Firefox
- Internet Explorer
- Safari

9.2 GOOGLE CHROME

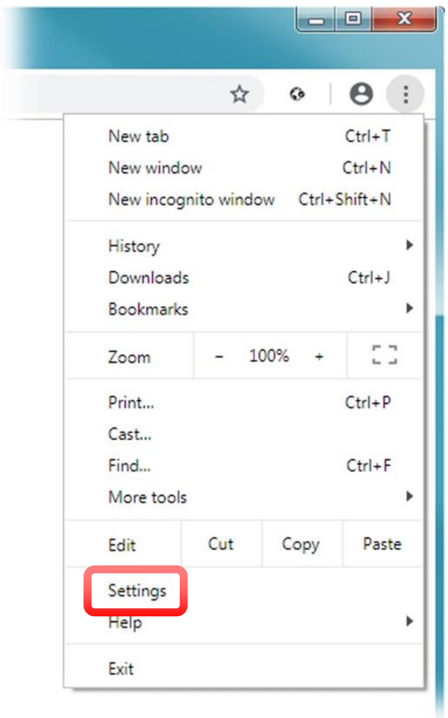
When using Google Chrome it is recommended that you disable autofill data and also clear the browsing data.

9.2.1 DISABLING AUTOFILL

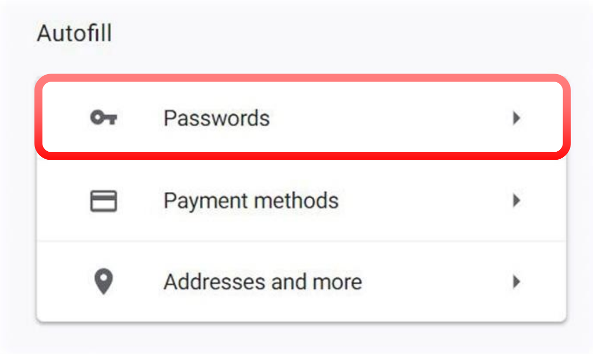
5. Click on the Chrome menu icon.



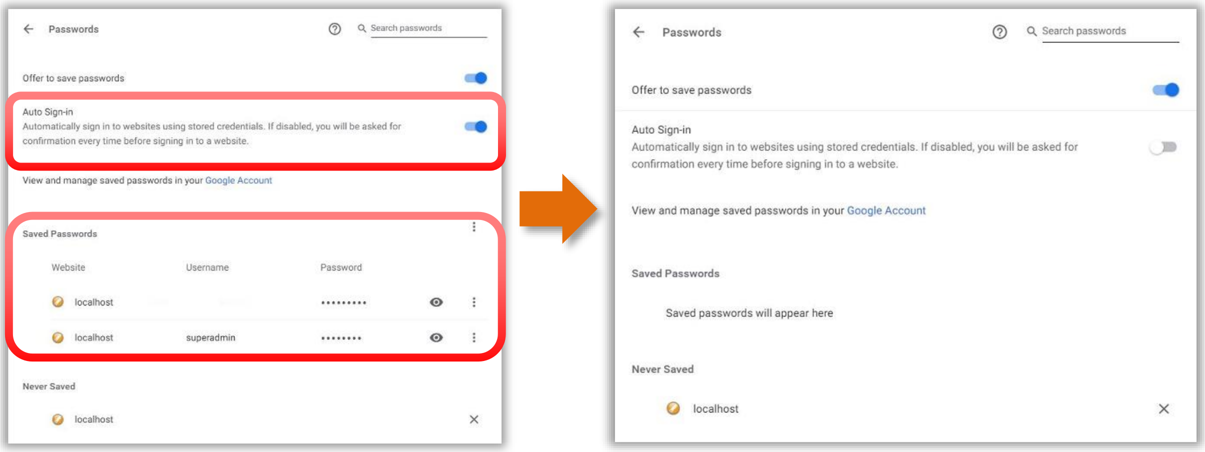
6. From the menu, select **Settings**.



7. At the next screen locate the **Autofill** section and select the **Passwords** option.

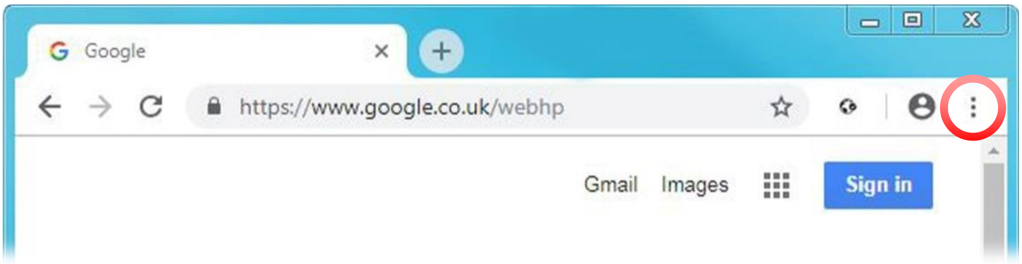


8. The next window will allow you to disable the **Auto Sign-in** option and also enable you to remove any existing saved passwords.

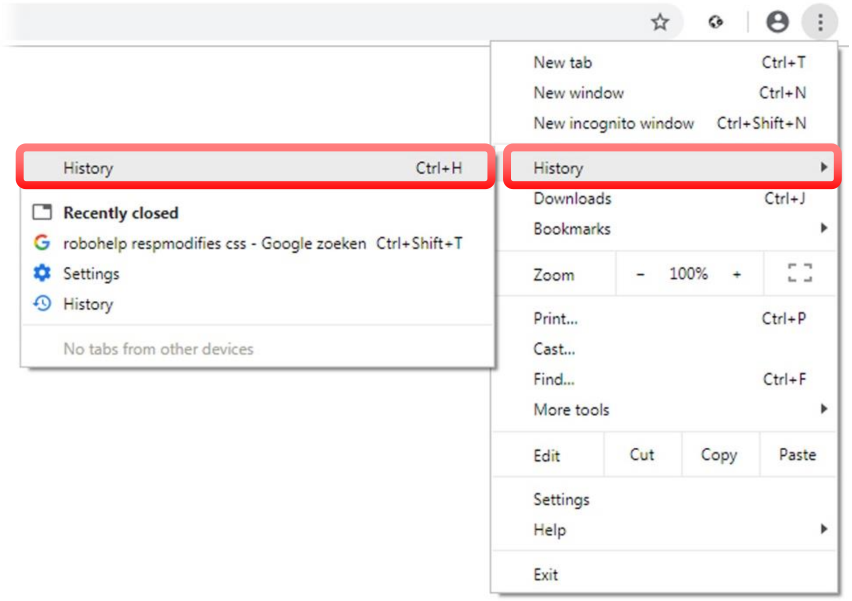


9.2.2 CLEARING AUTOFILL DATA

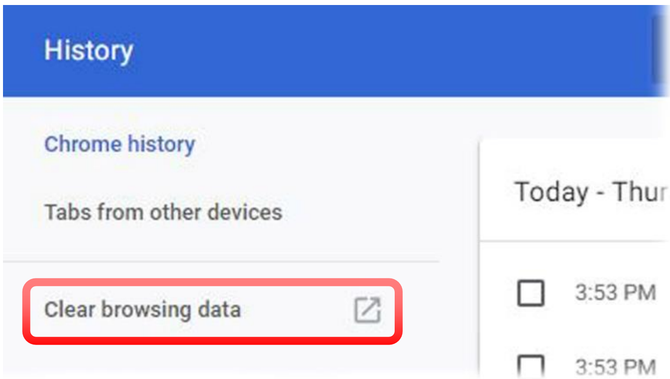
4. Click on the Chrome menu icon.



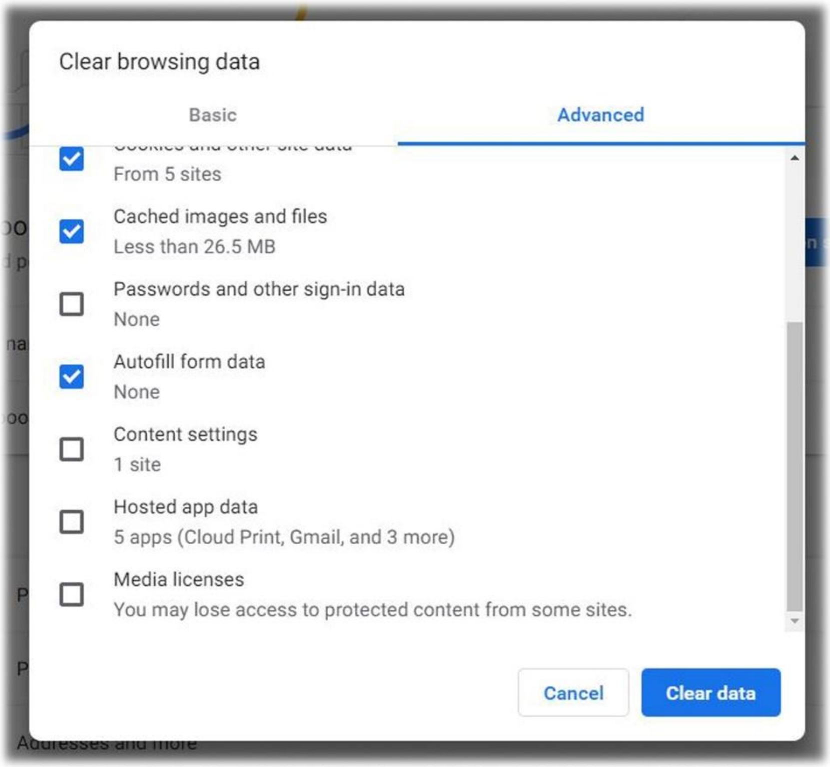
5. From the menu select the **History** option to expand the properties window and then select **History** from the list.



6. At the next window select the **Clear Browsing Data** option.



7. A new window will now appear. Select the **Advanced** tab, ensuring that the option for **Autofill Form Data** check-box is selected and then click on **Clear Data.** The browsing data will now be cleared.



Alternatively, you can press CTRL+SHIFT+DEL on your keyboard and bypass steps 1-4.

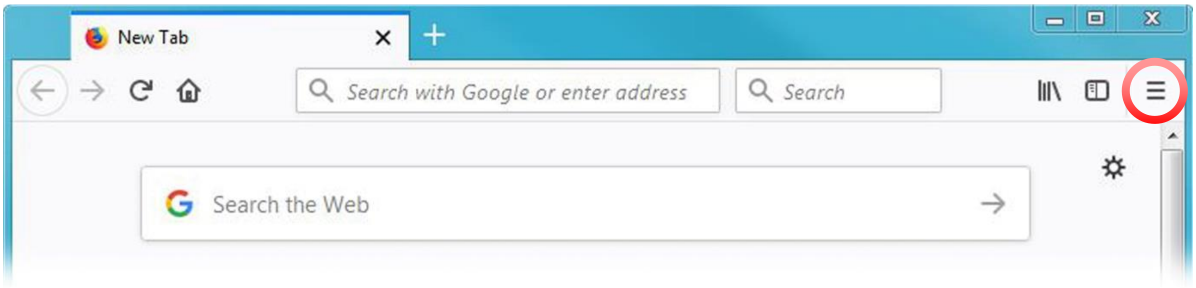
NOTE: Depending on how often your browsing history is cleared, this process may take some time.

9.3 FIREFOX

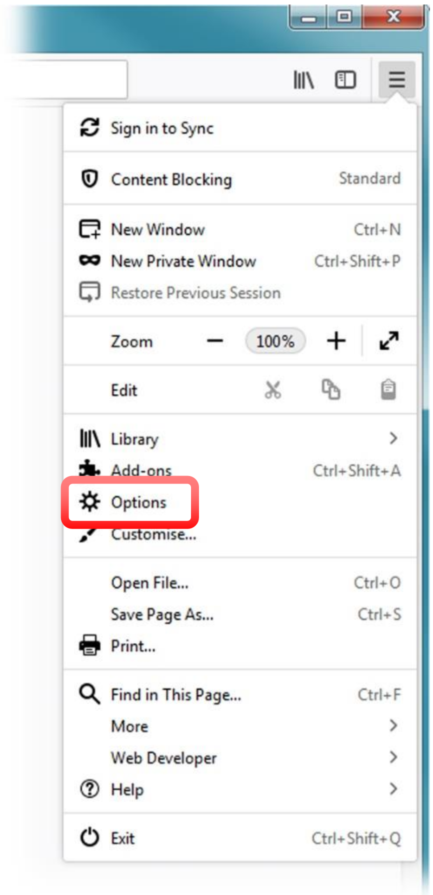
When using Firefox, it is recommended that you disable autofill data and clear the browsing data.

9.3.1 DISABLING AUTOFILL DATA

3. Click on the Firefox menu icon.

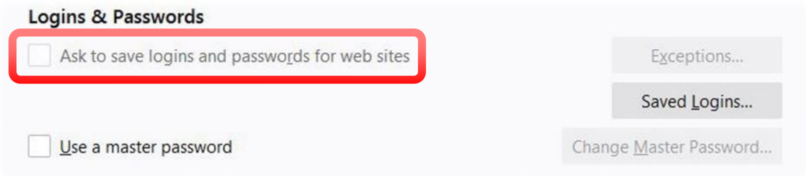


2. From the menu, select **Options.**



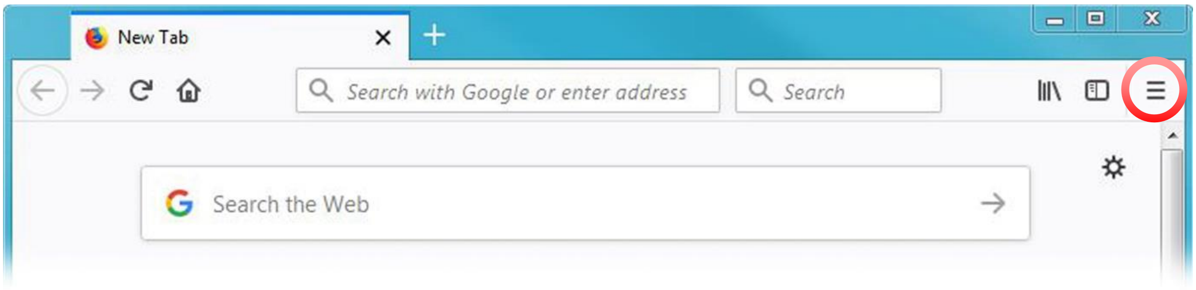
3. At the next screen under the **General** section, select **Privacy & Security.**

4. Scroll down to the **Logins & Passwords** section and uncheck the **Ask to save logins and passwords for web sites** check box.

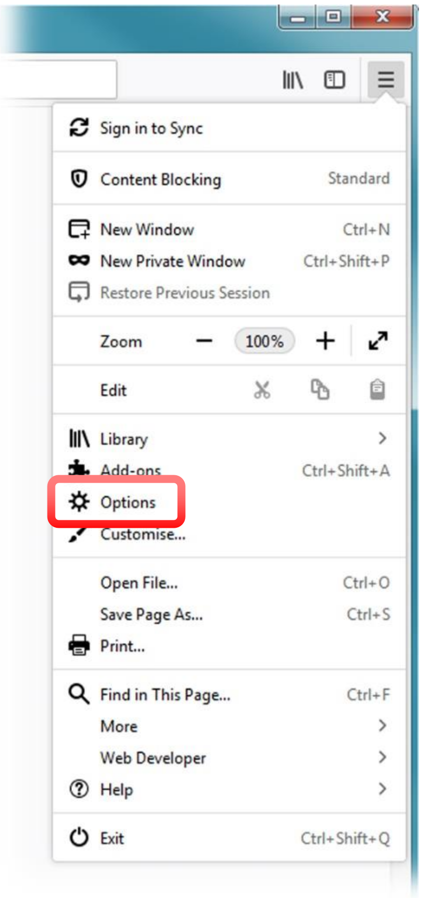


9.3.2 CLEARING AUTOFILL DATA

1. Click on the Firefox menu icon.

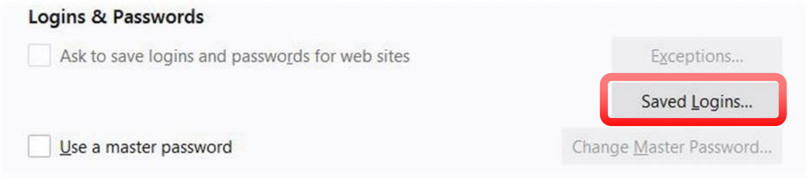


2. From the menu, select **Options.**

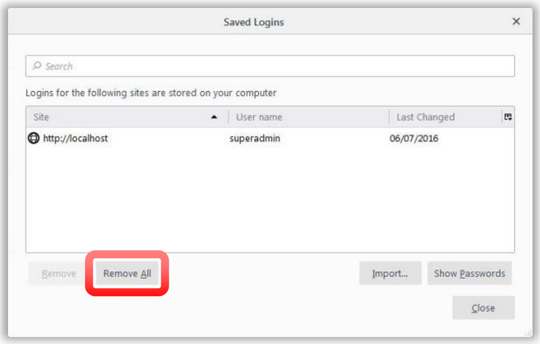


3. At the next screen under the **General** section, select **Privacy & Security.**

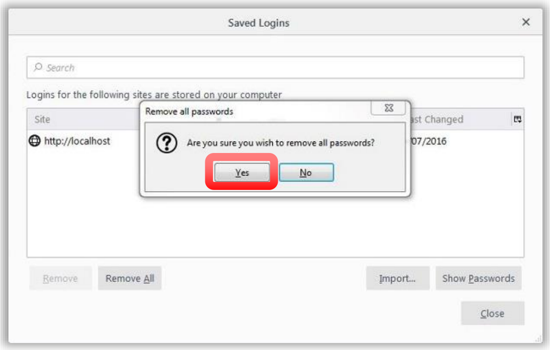
4. Scroll down to the **Logins & Passwords** section and click on the **Saved Logins** button.



5. A new window will open displaying all the saved passwords. Click on the **Remove All** button.



6. A message will appear asking you to confirm the removal process. Click on **Yes** to continue.



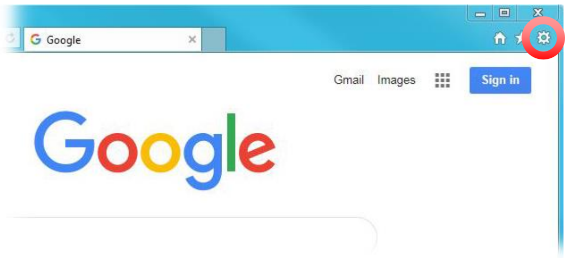
All passwords will then be removed from your browser and you may then close the window.

9.4 INTERNET EXPLORER

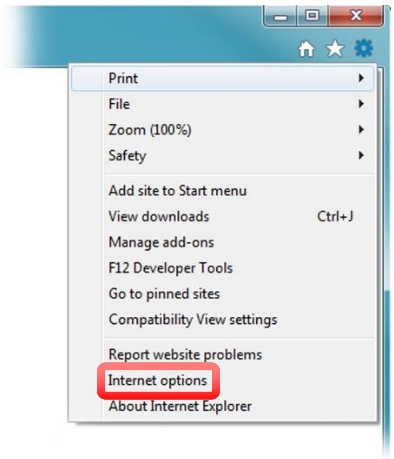
When using Internet Explorer, it is recommended that you disable autofill data and clear the browsing data.

9.4.1 DISABLING AUTOFILL DATA

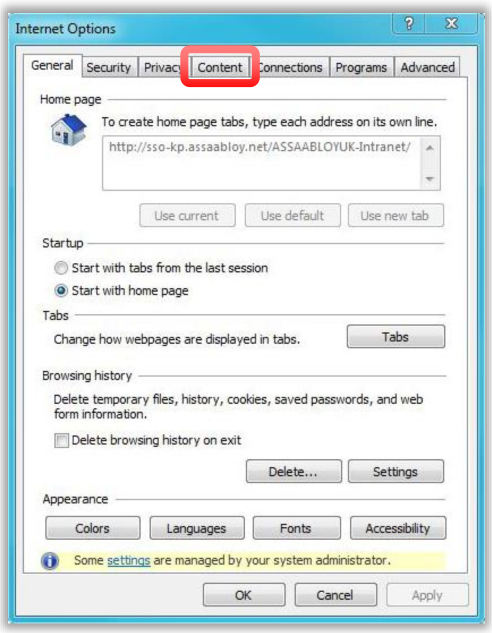
1. In the Internet Explorer browser, click on the Tools menu icon.



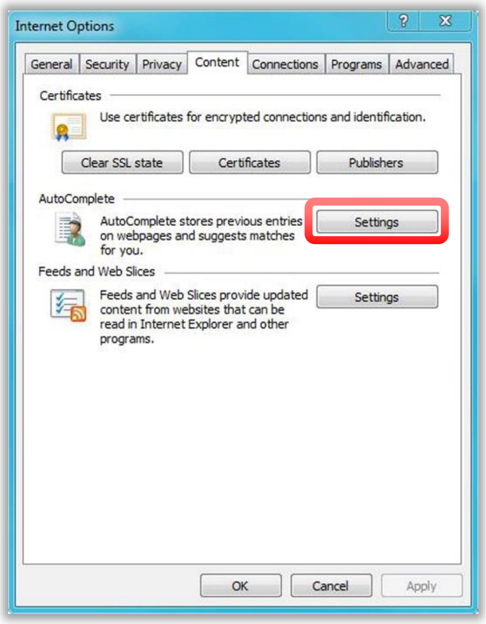
2. From the drop-down menu, select **Internet Options.**



3. A new window will now appear, select the **Content** tab from the top row.



4. Within the **AutoComplete** section, click on **Settings.**

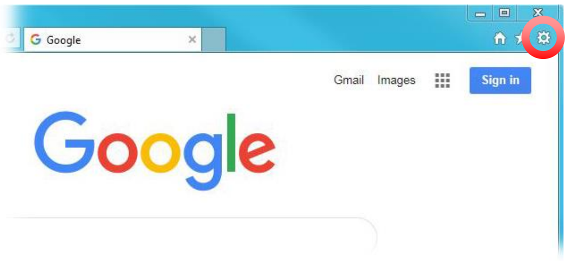


5. If checked, uncheck the **Forms** and **User names and passwords on forms** check boxes and then click on **OK** to close the window.

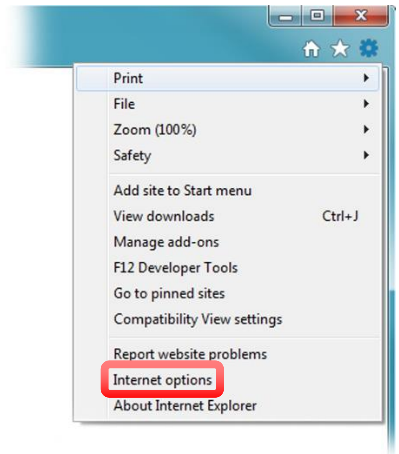
6. Click on **OK** to close the **Internet Options** window.

9.4.2 CLEARING AUTOFILL DATA

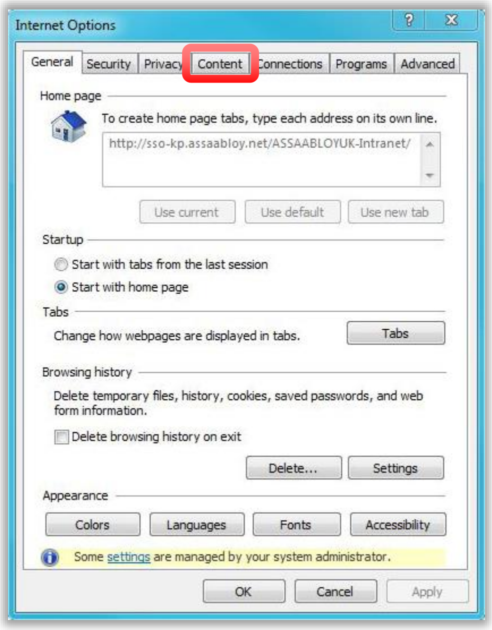
1. In the Internet Explorer browser, click on the Tools menu icon.



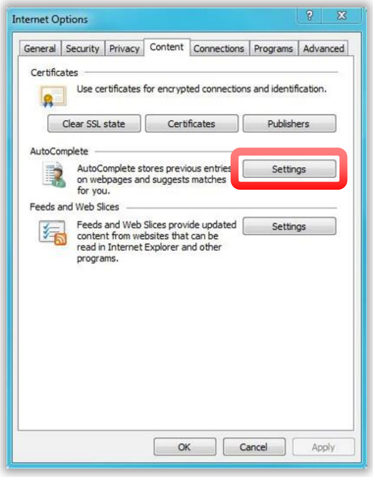
2. From the drop-down menu, select **Internet Options.**



3. A new window will now appear, select the **Content** tab from the top row.

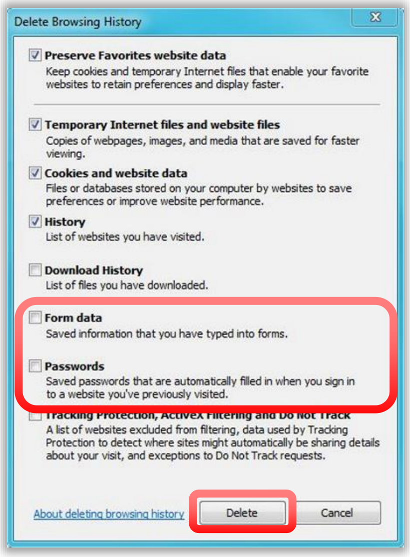


4. Within the **AutoComplete** section, click on **Settings.**



5. Click on the **Delete Auto Complete history…** button at the bottom of the window.

6. If checked, uncheck the **Form Data** and **Passwords** check boxes and then click the **Delete** button.



7. Click **OK** to close the **Auto Complete** window.
8. Click **OK** to close the **Internet Options** window.

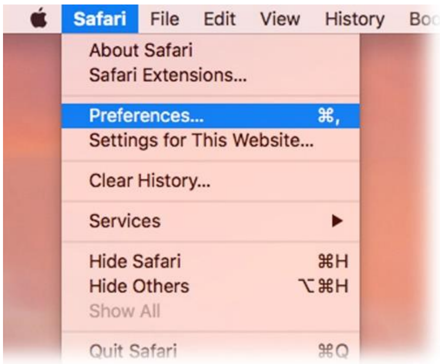
NOTE: Depending on how often you clear your browsing history, this process can take some time to complete.

9.5 SAFARI

When using Safari, it is recommended that you disable autofill data and clear the browsing data.

9.5.1 DISABLING AUTOFILL DATA

1. With the Safari browser open, select **Safari** from the top of the screen and select **Preferences.**

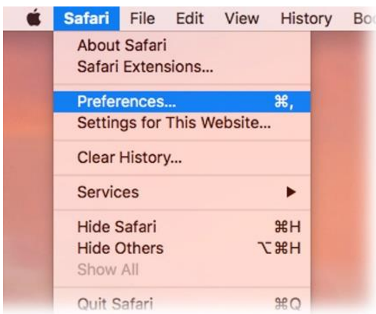


2. A new window will open. Select the **Autofill** tab and if checked, select the **Using information from my contacts** and **Other Forms** check boxes to deselect them.

3. Once completed, close the window.

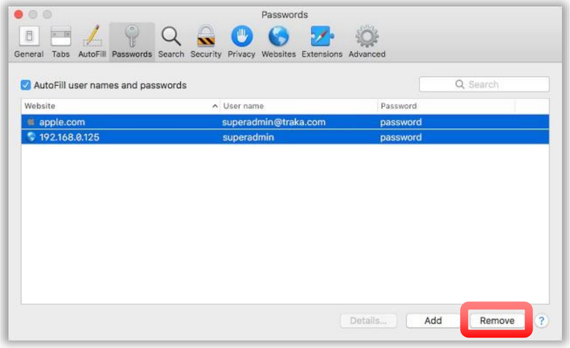
9.5.2 CLEARING AUTOFILL DATA

1. With the Safari browser open, select **Safari** from the top of the screen and then select **Preferences.**



2. A new window will open. Select the **Autofill** tab and if checked, select the **Using information from my contacts** and **Other Forms** check boxes to deselect them.

3. Within the **Passwords** window, select any specific passwords that require clearing and then click on the **Remove** button. Once complete, close the window.



For more information about managing usernames and passwords with Safari, refer to the Apple website: https://support.apple.com/guide/safari/use-autofill-ibrw1103/mac

10. SUPPORT LOG FILES

Should you be required to access or provide your Support Log Files, they are stored as text documents and can be located here:

Traka Business Engine Support Logs:

C:\Program Files (x86)\Traka Limited\Traka Business Engine Service\Support

Traka Communication Engine Support Logs:

C:\Program Files (x86)\Traka Limited\Traka Comms Engine Service\Support

TrakaWEB Admin Support Logs:

C:\Program Files (x86)\Traka Limited\Traka Web Admin\Support

IIS (Web Front End) Support Logs:

C:\inetpub\wwwroot\TrakaWeb\App_Data\Support\Logs

11. TECHNICAL SUPPORT

If you need to contact Traka/distributor for technical support:

From the top of TrakaWEB, select the Info icon to bring up the information window.

Technical Support Information

Telephone: **0333 355 3641**

International Telephone: **+(0)44 333 355 3641**

Email: **support@traka.com**

12. END USER LICENCE AGREEMENT – SOFTWARE

The Software supplied under this End User Licence Agreement (EULA) shall be subject to the following terms and conditions:

1. Definitions

“Applicable Law” means any: (i) law including any statute, statutory instrument, bye-law, order, regulation, directive, treaty, decree, decision (as referred to in Article 288 of the Treaty on the Functioning of the European Union) (including any judgment, order or decision of any court, regulator or tribunal); (ii) rule, policy, guidance or recommendation issued by any governmental, statutory or regulatory body; and/or (iii) industry code of conduct or guideline in force from time to time which relates to this EULA and/or the Hardware.

“Commercial Terms” means any legally binding document relating to the sale or supply of the Hardware to the Customer or dealing with the subject matter of this EULA, including under which payment is made for the Hardware by the Customer.

"Company" means ASSA ABLOY Global Solutions UK Ltd trading as Traka and shall include the Company's successors and assigns.

"Customer" means the person, firm or company with whom this EULA is made.

“Data Protection Laws” means all Applicable Laws relating to data protection, the processing of personal data and privacy, including: (i) the Data Protection Act 1998; (ii) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679; and (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and references to “Data Processor”, “Data Subjects”, “Personal Data”, “Process”, “Processed”, “Processing” “Processor” and “Supervisory Authority” have the meanings set out in, and will be interpreted in accordance with, such Applicable Laws.

“Documentation” means materials such as manuals, user guides or similar materials associated with or related to the Hardware.

"Embedded Software" means all software including firmware on or embedded in the Hardware at the date of manufacture together with any updates or newer versions made available by the Company from time to time.

“Hardware” means the product acquired from the Company or its authorised partner, including all Embedded Software and Documentation.

“Intellectual Property Rights” means all intellectual and industrial property rights of any kind whatsoever including, but not limited to, patents, supplementary protection certificates, registered trademarks, unregistered trademarks, rights in know-how, registered designs, models, unregistered design rights, rights to prevent passing off or unfair competition and copyright (whether in drawings, plans, specifications, designs and computer software or otherwise), database rights, topography rights, any rights in any invention, discovery or process and applications for and rights to apply for any of the foregoing, in each case in the United Kingdom and all other countries in the world and together with all renewals, extensions, continuations, divisions reissues, re-examinations and substitutions.

“Supplier” means the entity from which the Hardware was purchased by the Customer being the Company or one of its authorised partners.

“Warranty Period” means the 12 months following the date of sale by the Company of the Hardware to which the Embedded Software relates.

2. Licence

2.1 In consideration of the payment of the price for the Hardware to the Company or its authorised partner, the Company hereby grants a perpetual, non-exclusive, non-transferable licence for the use of the Embedded Software solely for use with the Hardware.

2.2 By installing and/or operating the Hardware, the Customer agrees to the terms of this EULA.

3. Patents, Designs and Copyright

The Embedded Software is licensed, not sold, to the Customer by the Company for use only under the terms of this EULA. The Company and its licensors retain all proprietary interests and rights in and over the Embedded Software and reserve all rights not expressly granted to the Customer under this EULA including all Intellectual Property Rights which shall remain the exclusive property of the Company or its licensors.

4. Restrictions

4.1 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to disclose the contents or code of the Embedded Software to any third party. The Customer may take such copies of the Embedded Software as is necessary for the purpose of back-up security and agrees that all copies shall be kept confidential and subject to the terms of this EULA.

4.2 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to lease, rent, sub-license, loan, sell or otherwise redistribute the whole or any part of the Embedded Software. The Customer may, however, rent, lease or sell the Hardware, provided that: (a) any rental, leasing or sale must include the Hardware and all of the Embedded Software, including all its component parts, original media, printed materials and this EULA; (b) the Customer does not retain any copies of the Embedded Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the Hardware reads and agrees to accept the terms and conditions of this EULA.

4.3 The Customer agrees not to modify, disassemble, reverse engineer, derive the source code of, decrypt, create derivative works or decompile the whole or any part of the Embedded Software nor attempt to do so save to the extent expressly permitted by law.

4.4 The Customer will not attempt to ascertain or list the source programs or source code relating to the Embedded Software.

4.5 The Customer will notify the Company as soon as it becomes aware of any unauthorised use of the Embedded Software by any person.

5. Warranty

5.1 The Company believes that to the best of its knowledge the Embedded Software has been thoroughly tested for freedom from arithmetic or logical defects in the Embedded Software and that it will function and perform substantially in accordance with the functions described in the Documentation.

5.2 If at any time during the Warranty Period, the Customer becomes aware of a breach of the warranty at Clause 5.1, the Customer will:

5.2.1 promptly notify the Supplier of any defect which it believes to exist, such notice to be given prior to the expiry of the Warranty Period, with all details and information which may assist in diagnosing and correcting the defect; and

5.2.2 provide any facilities, information and assistance which the Supplier may reasonably request to aid the diagnosis of the alleged defect and co-operate with the Supplier in these activities.

5.3 If the Supplier is unable to ascertain or correct the defect with the Embedded Software as notified by the Customer in accordance with Clause 5.2, the Supplier (if not the Company) shall notify the Company.

5.4 The Company reserves the right to charge the Customer at its prevailing rates for any effort expended in tracing apparent defects which prove not to be defects covered under this Clause 5.

5.5 In the event of a proven breach of the warranty in Clause 5.1 during the Warranty Period, the Supplier (or Company (as the case may be)) will either:

5.5.1 repair, or at its option replace, the Embedded Software (or the relevant part of it); or

5.5.2 correct the Documentation to reflect the proper performance of the Software where it is determined by the Company (acting reasonably) that the Software is functioning correctly but is not properly described in the Documentation.

5.6 The repair or replacement of the Embedded Software under Clause 5.5 will not be available to the Customer if:

5.6.1 the defect in the Embedded Software is attributable to failure or breakdown or interference of any third party, or software or hardware not supplied subject to this EULA;

5.6.2 the Customer is in breach of this EULA;

5.6.3 the Customer fails to operate the Hardware properly or fails to follow the instructions or recommendations of the Company as set out in the Documentation with respect to the Embedded Software;

5.6.4 the Customer interferes with, modifies, or fails to secure the Embedded Software otherwise than in accordance with the terms of this EULA;

6. Training

Other than the supply of the Documentation included with the Embedded Software, no training is provided by the Company unless otherwise agreed by the Customer and the Company.

7. Limit of Liability

7.1 Subject to Clause 7.2 and 7.3, the Company's maximum aggregate liability in connection with this EULA or the use of the Embedded Software will be limited to the lower of:

7.1.1 any applicable limitation of liability set out in the Commercial Terms; or

7.1.2 £100,000 or 100% of the price paid for the Hardware, whichever is lower.

7.2 Subject to Clause 7.3, the Company accepts no liability for any:

7.2.1 loss of business, loss of revenue, loss of profits, loss of goodwill, loss of use, loss of data or loss of any economic liability; or

7.2.2 indirect or consequential losses, however caused, arising in connection with this EULA or the use of the Embedded Software.

7.3 The Company makes no attempt to exclude liability relating to or arising from death or personal injury caused by the Company's negligence or the negligence of any employee, agent or contractor of the Company or liability for fraud or fraudulent misrepresentation, or for any other liability for which it would be unlawful to exclude or limit liability.

8. Disposal

The Customer undertakes that, upon the cessation of the use of the Hardware for whatever cause, or upon termination of this EULA, it will promptly destroy all known copies of the Embedded Software on any media other than the copy embedded in the Hardware and, if required by the Company, certify that this has been done.

9. Force Majeure

Neither party shall be liable for failure to perform its obligations under this EULA if such failure results from circumstance beyond the party's control.

10. Termination

Either party shall have the right to terminate this EULA if the other party is in material or persistent breach of this EULA and fails to rectify such breach within 30 days of receipt of notification thereof in writing, from the injured party, or if a right to terminate the relevant Commercial Terms has arisen. Termination shall not affect any other rights of the injured party.

11. Consequences of Termination

Upon termination of this EULA all rights and licences granted to the Customer under this EULA will cease immediately.

12. Communications and Notices

12.1 All communications or notices that the Customer is required to provide to the Company under this EULA shall be sent to the following address:

Traka – ASSA ABLOY
30 Stilebrook Road, Olney,
Milton Keynes, MK46 5EA, United Kingdom

or such other address of which the Company makes the Customer aware from time to time.

12.2 Any notice given in accordance with Clause 12.1 will be deemed to have been served:

12.2.1 if delivered to or left at the Company's address, at the time the notice is delivered to or left; or

12.2.2 if delivered by pre-paid first class post or mail delivery service providing proof of delivery, at 9:00am on the second Business Day after the date of posting.

13. Assignment

Except as expressly set out in this EULA or as permitted by law, the Customer will not be permitted to assign, transfer, charge, hold on trust for any person or deal in any other manner with any of its rights under this EULA without the prior written consent of the Company.

14. Waiver

A delay in exercising or failure to exercise a right or remedy under or in connection with this EULA will not constitute a waiver of, or prevent or restrict future exercise of, that or any other right or remedy, nor will the single or partial exercise of a right or remedy prevent or restrict the further exercise of that or any other right or remedy.

15. Severance

If any term of this EULA is found by any court or body or authority of competent jurisdiction to be illegal, unlawful, void or unenforceable, such term will be deemed to be severed from this EULA and this will not affect the remainder of this EULA which will continue in full force and effect.

16. Rights of Third Parties

The parties do not intend that any term of this EULA will be enforceable under the Contracts (Rights of Third Parties) Act 1999 by any person.

17. Law

17.1 This EULA (and any non-contractual obligations arising out of or in connection with it) is governed by the laws of England and Wales and the parties submit to the jurisdiction of the Courts of England and Wales.

Data Protection Laws

17.2 The Customer acknowledges that for the purposes of the Data Protection Laws, to the extent any Personal Data is involved in its use of the Hardware and Embedded Software, the Customer will be the Data Controller in respect of such Personal Data.

17.3 In limited circumstances, the Company may have access to data stored on the Hardware which may include user names or other Personal Data relating to the Customer's employees or authorized users ("Agreement Personal Data") where such access is required in order to provide support under the Warranty or any hardware maintenance agreement entered into by the Customer and the Company. The Customer authorises the Company to Process Agreement Personal Data during the term of this EULA as a Data Processor for the purposes of performing its obligations under this EULA only.

17.4 The Customer authorises the Company to appoint sub-processors of Agreement Personal Data and agrees to the use of the Company's existing sub-processors of Agreement Personal Data (each an "Authorised Sub-Processor").

17.5 The Customer shall:

17.5.1 comply with the Data Protection Laws;

17.5.2 ensure that only the Personal Data that the Company requires in order to perform its obligations under this EULA will be disclosed to, shared with and/or accessible by the Company; and

17.5.3 obtain all necessary consents and/or provide all fair processing notices required under the Data Protection Laws to enable the Company to lawfully receive, store, disclose and/or use all Agreement Personal Data (whether by itself or Authorised Sub-Processors) for the purpose of performing its obligations and exercising its rights under this EULA and as otherwise agreed by the parties from time to time.

17.6 The Company:

17.6.1 may appoint Authorised Sub-Processors in connection with the performance of its obligation under this EULA; and

17.6.2 shall provide notification of changes to Authorised Sub-Processors of Agreement Personal Data to the Customer at least 14 calendar days in advance to provide the Customer with the opportunity to object to the change. The Customer shall be deemed to accept the change if an objection is not received within 10 calendar days of notification. If an objection is received then the parties will work together in good faith to achieve an agreed outcome and any Authorised Sub-Processors appointed shall be appointed on terms the same as this EULA and the Company shall remain liable for the acts and omissions of such Authorised Sub-Processors.

17.7 The Company warrants that, if acting as a Data Processor, it shall:

17.7.1 Process the Agreement Personal Data only for the purpose of performing its obligations under this EULA and on such documented instructions received from the Customer from time to time as are reasonable, necessary and relevant to enable each party to perform its obligations under this EULA, save where required by Applicable Law and in such case the Company shall notify the Customer of the nature and extent of the Applicable Laws preventing such Processing (unless to do so would itself be a contravention of any Applicable Law); and

17.7.2 put in place appropriate technical and organisational security measures to the standard required under the Data Protection Law ("Security Measures") and shall provide reasonable assistance with any privacy impact assessment(s) that may be required of the Company under the Data Protection Laws which relate to the Processing of Agreement Personal Data under this Agreement.

17.8 From the 25 May 2018, the Company warrants that, if acting as a Data Processor, it shall:

17.8.1 notify the Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed ("Data Security Breach"). Where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay;

17.8.2 except to Authorised Sub-Processors, not disclose the Agreement Personal Data to a third party save as required for the performance of its obligations under this EULA, as otherwise provided under this EULA, or as required by Applicable Law;

17.8.3 notify the Customer without undue delay of any notice or communication from the Supervisory Authority which relates directly to the Processing of Agreement Personal Data;

17.8.4 ensure that any individual authorised to Process Agreement Personal Data on behalf of the Customer is subject to appropriate statutory or contractual obligation of confidentiality;

17.8.5 will upon reasonable notice, no more than once in any one calendar year, subject to appropriate confidentiality agreements being entered into, make available to the Customer all reasonable information relating to the Processing of Agreement Personal Data necessary to demonstrate compliance with the obligations set out in this EULA to the extent such information is not already available to the Customer; and allow for and contribute to one audit in any one calendar year, including inspection, conducted by the Customer or another auditor mandated by the Customer to that same extent solely to the extent relevant to the Processing of Agreement Personal Data;

17.8.6 to the extent required by Data Protection Laws, notify and provide reasonable assistance to the Customer on receiving any:

17.8.6.1 complaint by a Data Subject in respect of their Personal Data contained in the Agreement Personal Data or any request received from a Data Subject to have access to his Personal Data (or to exercise any other right(s) afforded to him under the Data Protection Laws) as contained in the Agreement Personal Data (including by appropriate technical and organisational measures, insofar as this is possible);

17.8.6.2 notice or communication from the Supervisory Authority which relates to the processing of Agreement Personal Data;

17.8.7 to the extent required by Data Protection Laws, reasonably assist the Customer in:

17.8.7.1 taking measures to address any Data Security Breach; and

17.8.7.2 conducting privacy impact assessments of any Processing operations and consulting with any applicable Supervisory Authority;

17.8.8 only share Agreement Personal Data with the Authorised Sub-Processors to carry out the services provided that, to the extent the Authorised Sub-Processor is located outside the UK or the European Union, the Company will implement measures to ensure an adequate level of protection for the rights and freedoms of the relevant individuals in relation to the transfer of any Personal Data, except to the extent that the transfer is (i) to a country that the European Commission has recognised as providing adequate protection for such transfer from time to time and/or (ii) otherwise expressly permitted by Data Protection Laws.

17.9 At the option of the Customer, the Company shall securely delete or return to the Customer all Agreement Personal Data promptly following termination of this EULA and shall securely delete any remaining copies.

18. Entire Agreement

18.1 Subject to Clause 18.2, the parties agree that these terms and conditions (together with any Commercial Terms) represent the entire agreement between the parties relating to the licence of the Embedded Software, and that no statements or representations made by either party have been relied on by the other in agreeing to enter into the EULA and the parties shall have no remedy in respect of any such statement or representation which is not set out in this EULA.

18.2 Unless otherwise specified in the Commercial Terms, if the Customer also enters into a hardware maintenance agreement with the Company then the Customer’s rights and obligations under Clause 5.5 and Clauses 17.2-17.9 (inclusive) will apply for the duration of the relevant hardware maintenance agreement by changing only those things which require to be changed in order to retain the meaning of those Clauses.

NOTE: v3.1 of this EULA, published on 1/Oct/2022 reflects the new legal entity, ASSA ABLOY Global Solutions UK Ltd, and contains no other changes from v3 published in 2018.

13. END USER LICENCE AGREEMENT – EMBEDDED SOFTWARE

The Embedded Software supplied under this End User Licence Agreement (EULA) shall be subject to the following terms and conditions:

1. Definitions

“Applicable Law” means any: (i) law including any statute, statutory instrument, bye-law, order, regulation, directive, treaty, decree, decision (as referred to in Article 288 of the Treaty on the Functioning of the European Union) (including any judgment, order or decision of any court, regulator or tribunal); (ii) rule, policy, guidance or recommendation issued by any governmental, statutory or regulatory body; and/or (iii) industry code of conduct or guideline in force from time to time which relates to this EULA and/or the Hardware.

“Commercial Terms” means any legally binding document relating to the sale or supply of the Hardware to the Customer or dealing with the subject matter of this EULA, including under which payment is made for the Hardware by the Customer.

"Company" means ASSA ABLOY Global Solutions UK Ltd trading as Traka and shall include the Company's successors and assigns.

"Customer" means the person, firm or company with whom this EULA is made.

“Data Protection Laws” means all Applicable Laws relating to data protection, the processing of personal data and privacy, including: (i) the Data Protection Act 1998; (ii) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679; and (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and references to “Data Processor”, “Data Subjects”, “Personal Data”, “Process”, “Processed”, “Processing” “Processor” and “Supervisory Authority” have the meanings set out in, and will be interpreted in accordance with, such Applicable Laws.

“Documentation” means materials such as manuals, user guides or similar materials associated with or related to the Hardware.

"Embedded Software" means all software including firmware on or embedded in the Hardware at the date of manufacture together with any updates or newer versions made available by the Company from time to time.

“Hardware” means the product acquired from the Company or its authorised partner, including all Embedded Software and Documentation.

“Intellectual Property Rights” means all intellectual and industrial property rights of any kind whatsoever including, but not limited to, patents, supplementary protection certificates, registered trademarks, unregistered trademarks, rights in know-how, registered designs, models, unregistered design rights, rights to prevent passing off or unfair competition and copyright (whether in drawings, plans, specifications, designs and computer software or otherwise), database rights, topography rights, any rights in any invention, discovery or process and applications for and rights to apply for any of the foregoing, in each case in the United Kingdom and all other countries in the world and together with all renewals, extensions, continuations, divisions reissues, re-examinations and substitutions.

“Supplier” means the entity from which the Hardware was purchased by the Customer being the Company or one of its authorised partners.

“Warranty Period” means the 12 months following the date of sale by the Company of the Hardware to which the Embedded Software relates.

2. Licence

2.1 In consideration of the payment of the price for the Hardware to the Company or its authorised partner, the Company hereby grants a perpetual, non-exclusive, non-transferable licence for the use of the Embedded Software solely for use with the Hardware.

2.2 By installing and/or operating the Hardware, the Customer agrees to the terms of this EULA.

3. Patents, Designs and Copyright

The Embedded Software is licensed, not sold, to the Customer by the Company for use only under the terms of this EULA. The Company and its licensors retain all proprietary interests and rights in and over the Embedded Software and reserve all rights not expressly granted to the Customer under this EULA including all Intellectual Property Rights which shall remain the exclusive property of the Company or its licensors.

4. Restrictions

4.1 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to disclose the contents or code of the Embedded Software to any third party. The Customer may take such copies of the Embedded Software as is necessary for the purpose of back-up security and agrees that all copies shall be kept confidential and subject to the terms of this EULA.

4.2 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to lease, rent, sub-license, loan, sell or otherwise redistribute the whole or any part of the Embedded Software. The Customer may, however, rent, lease or sell the Hardware, provided that: (a) any rental, leasing or sale must include the Hardware and all of the Embedded Software, including all its component parts, original media, printed materials and this EULA; (b) the Customer does not retain any copies of the Embedded Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the Hardware reads and agrees to accept the terms and conditions of this EULA.

4.3 The Customer agrees not to modify, disassemble, reverse engineer, derive the source code of, decrypt, create derivative works or decompile the whole or any part of the Embedded Software nor attempt to do so save to the extent expressly permitted by law.

4.4 The Customer will not attempt to ascertain or list the source programs or source code relating to the Embedded Software.

4.5 The Customer will notify the Company as soon as it becomes aware of any unauthorised use of the Embedded Software by any person.

5. Warranty

5.1 The Company believes that to the best of its knowledge the Embedded Software has been thoroughly tested for freedom from arithmetic or logical defects in the Embedded Software and that it will function and perform substantially in accordance with the functions described in the Documentation.

5.2 If at any time during the Warranty Period, the Customer becomes aware of a breach of the warranty at Clause 5.1, the Customer will:

5.2.1 promptly notify the Supplier of any defect which it believes to exist, such notice to be given prior to the expiry of the Warranty Period, with all details and information which may assist in diagnosing and correcting the defect; and

5.2.2 provide any facilities, information and assistance which the Supplier may reasonably request to aid the diagnosis of the alleged defect and co-operate with the Supplier in these activities.

5.3 If the Supplier is unable to ascertain or correct the defect with the Embedded Software as notified by the Customer in accordance with Clause 5.2, the Supplier (if not the Company) shall notify the Company.

5.4 The Company reserves the right to charge the Customer at its prevailing rates for any effort expended in tracing apparent defects which prove not to be defects covered under this Clause 5.

5.5 In the event of a proven breach of the warranty in Clause 5.1 during the Warranty Period, the Supplier (or Company (as the case may be)) will either:

5.5.1 repair, or at its option replace, the Embedded Software (or the relevant part of it); or

5.5.2 correct the Documentation to reflect the proper performance of the Software where it is determined by the Company (acting reasonably) that the Software is functioning correctly but is not properly described in the Documentation.

5.6 The repair or replacement of the Embedded Software under Clause 5.5 will not be available to the Customer if:

5.6.1 the defect in the Embedded Software is attributable to failure or breakdown or interference of any third party, or software or hardware not supplied subject to this EULA;

5.6.2 the Customer is in breach of this EULA;

5.6.3 the Customer fails to operate the Hardware properly or fails to follow the instructions or recommendations of the Company as set out in the Documentation with respect to the Embedded Software;

5.6.4 the Customer interferes with, modifies, or fails to secure the Embedded Software otherwise than in accordance with the terms of this EULA;

6. Training

Other than the supply of the Documentation included with the Embedded Software, no training is provided by the Company unless otherwise agreed by the Customer and the Company.

7. Limit of Liability

7.1 Subject to Clause 7.2 and 7.3, the Company's maximum aggregate liability in connection with this EULA or the use of the Embedded Software will be limited to the lower of:

7.1.1 any applicable limitation of liability set out in the Commercial Terms; or

7.1.2 £100,000 or 100% of the price paid for the Hardware, whichever is lower.

7.2 Subject to Clause 7.3, the Company accepts no liability for any:

7.2.1 loss of business, loss of revenue, loss of profits, loss of goodwill, loss of use, loss of data or loss of any economic liability; or

7.2.2 indirect or consequential losses, however caused, arising in connection with this EULA or the use of the Embedded Software.

7.3 The Company makes no attempt to exclude liability relating to or arising from death or personal injury caused by the Company's negligence or the negligence of any employee, agent or contractor of the Company or liability for fraud or fraudulent misrepresentation, or for any other liability for which it would be unlawful to exclude or limit liability.

8. Disposal

The Customer undertakes that, upon the cessation of the use of the Hardware for whatever cause, or upon termination of this EULA, it will promptly destroy all known copies of the Embedded Software on any media other than the copy embedded in the Hardware and, if required by the Company, certify that this has been done.

9. Force Majeure

Neither party shall be liable for failure to perform its obligations under this EULA if such failure results from circumstance beyond the party's control.

10. Termination

Either party shall have the right to terminate this EULA if the other party is in material or persistent breach of this EULA and fails to rectify such breach within 30 days of receipt of notification thereof in writing, from the injured party, or if a right to terminate the relevant Commercial Terms has arisen. Termination shall not affect any other rights of the injured party.

11. Consequences of Termination

Upon termination of this EULA all rights and licences granted to the Customer under this EULA will cease immediately.

12. Communications and Notices

12.1 All communications or notices that the Customer is required to provide to the Company under this EULA shall be sent to the following address:

Traka – ASSA ABLOY
30 Stilebrook Road, Olney,
Milton Keynes, MK46 5EA, United Kingdom

or such other address of which the Company makes the Customer aware from time to time.

12.2 Any notice given in accordance with Clause 12.1 will be deemed to have been served:

12.2.1 if delivered to or left at the Company's address, at the time the notice is delivered to or left; or

12.2.2 if delivered by pre-paid first class post or mail delivery service providing proof of delivery, at 9:00am on the second Business Day after the date of posting.

13. Assignment

Except as expressly set out in this EULA or as permitted by law, the Customer will not be permitted to assign, transfer, charge, hold on trust for any person or deal in any other manner with any of its rights under this EULA without the prior written consent of the Company.

14. Waiver

A delay in exercising or failure to exercise a right or remedy under or in connection with this EULA will not constitute a waiver of, or prevent or restrict future exercise of, that or any other right or remedy, nor will the single or partial exercise of a right or remedy prevent or restrict the further exercise of that or any other right or remedy.

15. Severance

If any term of this EULA is found by any court or body or authority of competent jurisdiction to be illegal, unlawful, void or unenforceable, such term will be deemed to be severed from this EULA and this will not affect the remainder of this EULA which will continue in full force and effect.

16. Rights of Third Parties

The parties do not intend that any term of this EULA will be enforceable under the Contracts (Rights of Third Parties) Act 1999 by any person.

17. Law

17.1 This EULA (and any non-contractual obligations arising out of or in connection with it) is governed by the laws of England and Wales and the parties submit to the jurisdiction of the Courts of England and Wales.

Data Protection Laws

17.2 The Customer acknowledges that for the purposes of the Data Protection Laws, to the extent any Personal Data is involved in its use of the Hardware and Embedded Software, the Customer will be the Data Controller in respect of such Personal Data.

17.3 In limited circumstances, the Company may have access to data stored on the Hardware which may include user names or other Personal Data relating to the Customer's employees or authorized users ("Agreement Personal Data") where such access is required in order to provide support under the Warranty or any hardware maintenance agreement entered into by the Customer and the Company. The Customer authorises the Company to Process Agreement Personal Data during the term of this EULA as a Data Processor for the purposes of performing its obligations under this EULA only.

17.4 The Customer authorises the Company to appoint sub-processors of Agreement Personal Data and agrees to the use of the Company's existing sub-processors of Agreement Personal Data (each an "Authorised Sub-Processor").

17.5 The Customer shall:

17.5.1 comply with the Data Protection Laws;

17.5.2 ensure that only the Personal Data that the Company requires in order to perform its obligations under this EULA will be disclosed to, shared with and/or accessible by the Company; and

17.5.3 obtain all necessary consents and/or provide all fair processing notices required under the Data Protection Laws to enable the Company to lawfully receive, store, disclose and/or use all Agreement Personal Data (whether by itself or Authorised Sub-Processors) for the purpose of performing its obligations and exercising its rights under this EULA and as otherwise agreed by the parties from time to time.

17.6 The Company:

17.6.1 may appoint Authorised Sub-Processors in connection with the performance of its obligation under this EULA; and

17.6.2 shall provide notification of changes to Authorised Sub-Processors of Agreement Personal Data to the Customer at least 14 calendar days in advance to provide the Customer with the opportunity to object to the change. The Customer shall be deemed to accept the change if an objection is not received within 10 calendar days of notification. If an objection is received then the parties will work together in good faith to achieve an agreed outcome and any Authorised Sub-Processors appointed shall be appointed on terms the same as this EULA and the Company shall remain liable for the acts and omissions of such Authorised Sub-Processors.

17.7 The Company warrants that, if acting as a Data Processor, it shall:

17.7.1 Process the Agreement Personal Data only for the purpose of performing its obligations under this EULA and on such documented instructions received from the Customer from time to time as are reasonable, necessary and relevant to enable each party to perform its obligations under this EULA, save where required by Applicable Law and in such case the Company shall notify the Customer of the nature and extent of the Applicable Laws preventing such Processing (unless to do so would itself be a contravention of any Applicable Law); and

17.7.2 put in place appropriate technical and organisational security measures to the standard required under the Data Protection Law ("Security Measures") and shall provide reasonable assistance with any privacy impact assessment(s) that may be required of the Company under the Data Protection Laws which relate to the Processing of Agreement Personal Data under this Agreement.

17.8 From the 25 May 2018, the Company warrants that, if acting as a Data Processor, it shall:

17.8.1 notify the Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed ("Data Security Breach"). Where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay;

17.8.2 except to Authorised Sub-Processors, not disclose the Agreement Personal Data to a third party save as required for the performance of its obligations under this EULA, as otherwise provided under this EULA, or as required by Applicable Law;

17.8.3 notify the Customer without undue delay of any notice or communication from the Supervisory Authority which relates directly to the Processing of Agreement Personal Data;

17.8.4 ensure that any individual authorised to Process Agreement Personal Data on behalf of the Customer is subject to appropriate statutory or contractual obligation of confidentiality;

17.8.5 will upon reasonable notice, no more than once in any one calendar year, subject to appropriate confidentiality agreements being entered into, make available to the Customer all reasonable information relating to the Processing of Agreement Personal Data necessary to demonstrate compliance with the obligations set out in this EULA to the extent such information is not already available to the Customer; and allow for and contribute to one audit in any one calendar year, including inspection, conducted by the Customer or another auditor mandated by the Customer to that same extent solely to the extent relevant to the Processing of Agreement Personal Data;

17.8.6 to the extent required by Data Protection Laws, notify and provide reasonable assistance to the Customer on receiving any:

17.8.6.1 complaint by a Data Subject in respect of their Personal Data contained in the Agreement Personal Data or any request received from a Data Subject to have access to his Personal Data (or to exercise any other right(s) afforded to him under the Data Protection Laws) as contained in the Agreement Personal Data (including by appropriate technical and organisational measures, insofar as this is possible);

17.8.6.2 notice or communication from the Supervisory Authority which relates to the processing of Agreement Personal Data;

17.8.7 to the extent required by Data Protection Laws, reasonably assist the Customer in:

17.8.7.1 taking measures to address any Data Security Breach; and

17.8.7.2 conducting privacy impact assessments of any Processing operations and consulting with any applicable Supervisory Authority;

17.8.8 only share Agreement Personal Data with the Authorised Sub-Processors to carry out the services provided that, to the extent the Authorised Sub-Processor is located outside the UK or the European Union, the Company will implement measures to ensure an adequate level of protection for the rights and freedoms of the relevant individuals in relation to the transfer of any Personal Data, except to the extent that the transfer is (i) to a country that the European Commission has recognised as providing adequate protection for such transfer from time to time and/or (ii) otherwise expressly permitted by Data Protection Laws.

17.9 At the option of the Customer, the Company shall securely delete or return to the Customer all Agreement Personal Data promptly following termination of this EULA and shall securely delete any remaining copies.

18. Entire Agreement

18.1 Subject to Clause 18.2, the parties agree that these terms and conditions (together with any Commercial Terms) represent the entire agreement between the parties relating to the licence of the Embedded Software, and that no statements or representations made by either party have been relied on by the other in agreeing to enter into the EULA and the parties shall have no remedy in respect of any such statement or representation which is not set out in this EULA.

18.2 Unless otherwise specified in the Commercial Terms, if the Customer also enters into a hardware maintenance agreement with the Company then the Customer's rights and obligations under Clause 5.5 and Clauses 17.2-17.9 (inclusive) will apply for the duration of the relevant hardware maintenance agreement by changing only those things which require to be changed in order to retain the meaning of those Clauses.

NOTE: v3.1 of this EULA, published on 1/Oct/2022 reflects the new legal entity, ASSA ABLOY Global Solutions UK Ltd, and contains no other changes from v3 published in 2018.