TRAKA TOUCH LOCKERS USER GUIDE

UD0090

02/12/25

VERSION 6.6

CONTENTS

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

Internal

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**

1. INTRODUCING TRAKA

About Traka

Traka is the global leader in intelligent management solutions for keys and equipment. Our solutions help all types of organizations better control their important assets, improving productivity and accountability, and reducing risk in critical processes.

We continuously invest in the development of our technology to provide leading, innovative, secure and effective real-world solutions to the challenges that organizations face in managing keys and equipment, which have such a high impact on the way their organization is run. Our solutions are tailored to customer needs and requirements, providing the most value and impact on their business.

Traka is a global organization with local support, working to defined processes so that we are local when you need us and global when it counts.

Traka is part of **ASSA ABLOY Global Solutions**, dedicated to reimagining how people move through their world. Our expertise in customer journey mapping, innovation and service design leads to the invention of new security solutions that create value for our clients and exceptional experiences for end users.

Project Management

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.

Customer Support

Customer satisfaction is our top priority – at Traka we pride ourselves on building long term partnerships from the initial hardware installation, through the system software configuration and user training and finally in providing on-going customer support via our global help desks.

Maintenance Contracts

In the unlikely event that you do experience a problem with your Traka system, our dedicated customer support service, located in UK, US, EMEA and Oceania, operate a fast and efficient telephone service to assist you quickly in resolving any problems.

Training

Our training department provides a comprehensive range of courses to enhance your knowledge and skills with the aim that the courses give you the best qualifications for long term success in an environment a dynamic as the asset management industry.

2. TRAKA CONTACT DETAILS

Sales Website	**www.traka.com**
Sales Enquiries Email	**sales@traka.com**
Support Website	**support.traka.com**

Traka UK

Main Tel:	**+44 (0)1234 712345**
Support Tel:	**+44 (0)333 3553641**
Contact Email:	**info@traka.com**

Traka Europe

Main Tel:	**+44 (0)1234 712345**
Support Tel:	**+44 (0)1234 943900**
Contact Email	**eusupport@traka.com**

Traka Nordics

Main Tel:	**08 775 1090**
Support Tel:	**08 775 1099**
Contact Email:	**nordicinfo@traka.com**

Traka Iberia

Main Tel:	**+34 91 8676696**
Contact Email:	**info@traka.es**

Traka US

Main Tel:	**+1 877 34 87252**
Support Tel:	**+1 855 94 87252**
Contact Email:	**info@trakaUSA.com**

Traka Africa

Main Tel:	**+27 11 761 5000**
Contact Email:	**info@traka.co.za**

Traka Oceania

Main Tel:	**+61 1300 666 108**
Contact Email:	**enquiries@traka.com.au**

3. WHAT AND WHO IS THIS GUIDE FOR?

This User Guide has been prepared to assist you (the end user) with the operating basics of the Traka Touch System. Please keep this guide handy for those times when you need to remember how to **Add a user**, **Replace an Item** or simply refresh your memory on how to restrict access to a key in the user details form.

NOTE: **For information on the TrakaWEB please refer to either of the following guides UD0018 - TrakaWEB User Guide or UD0260 - TrakaWEB Version 4 User Guide, dependent on which version of TrakaWEB you are using.**

Access to documentation such as User Guides or Getting Started Guides can be accessed by scanning a QR code within the Administration screen at Traka Touch. This will take you directly to the Traka website. Alternatively, you can visit the website using the address: **www.traka.com/qr** as shown below.
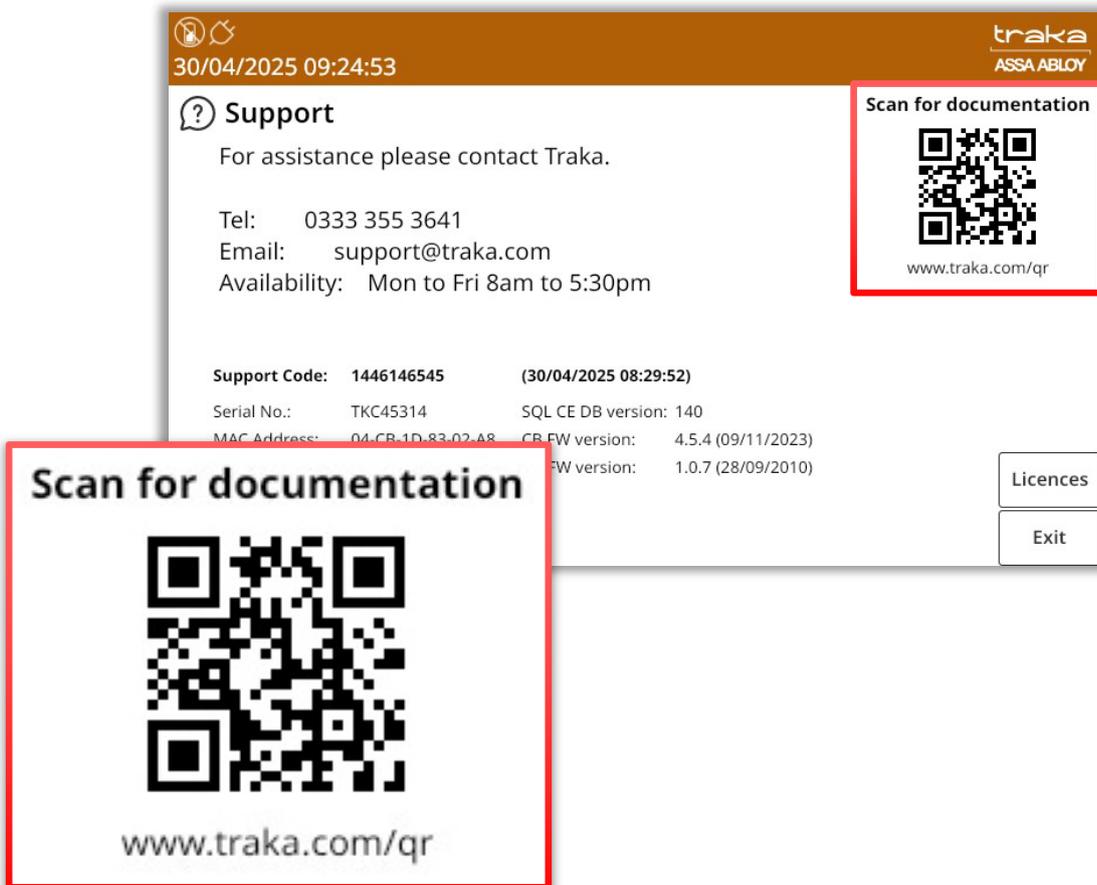
4. PRODUCT DETAILS

NOTE: **Please ensure that the correct installation procedures have been utilised and the product is safely secured.**

4.1 ELECTRICAL RATING

Power supply: Input: 100-240V AC 50/60Hz 35W Max

Battery backup: DC12V 7Ah

NOTE: **These values are not inclusive of charging.**

4.2 ENVIRONMENTAL RATING

Operating temp: Ambient, for indoor use only (-5°C to +40°C at 95% non-condensing relative humidity).

4.3 APPROVALS & COMPLIANCE LEVEL

4.3.1 PRODUCT COMPLIANCE

UK – UKCA

Europe – CE

USA – MET NRTL, FCC

Canada – MET NRTL, ICES

4.3.2 BUSINESS COMPLIANCE

Quality – ISO9001

Environmental – ISO14001

Information Security – ISO27001

NOTE: **USB memory sticks should be formatted to FAT32 and not NTFS when used in a Traka Touch system, as NTFS is not supported by the Windows CE operating system used.**

NOTE: **Files should be located on the root of the USB memory stick and not in sub folders. This is to ensure that the Traka Touch software is able to locate them.**

NOTE: **If the USB memory stick has any metal attachments, remove them or reposition them to prevent them making contact with any metalwork on the system and risking a short circuit.**

The type of system will determine which USB port will be used. Some Locker systems will require access to the Touch PCB located behind the control panel door using a master key.

If you require further assistance, please contact Traka Technical Support using the information at the end of this document.

Internal

5. TRAKA TOUCH LOCKER DETAILS AND DIAGRAMS

Traka Touch Lockers are designed around each customer's individual requirements. Therefore, each locker system is different and will vary in size, compartment numbering, colour etc. The diagrams below are examples to show the different types of Locker System available.

5.1 TRAKA TOUCH TABLET LOCKER

The Traka Touch Tablet Locker System is available in 10, 20 or 30 compartment versions. It is designed to store all Tablet types and is available with RFID or non-RFID tagging.

These lockers are now available in two variants: original Touch Tablet Locker is equipped with a Resistive Touch Screen and the iMX28 Control Board. A newer version with a Capacitive Touch Screen is equipped with the iMX6 Control Board. For clarity, whenever there are Capacitive Touch Screen models discussed in this guide and their features are different from standard Touch lockers, distinction between the two models is always indicated.

Extension Systems are also available whereby additional Tablet Lockers can be connected back to a single Control Panel.

Each compartment provides the option for charging. It is important to return the Tablet to the locker in same orientation from which it was removed so that the charging lead may be attached in the correct location.

Figure 1 – Traka Touch Tablet Locker (left) and Traka Touch Capacitive Screen Tablet Locker (right)

5.2 TRAKA TOUCH PERSONNEL LOCKER

The Traka Touch Personnel Locker System is available in a range of sizes, with each Locker Stack containing 3, 5 or 8 compartments. It is also available with charging or non-charging capability.

The Control Locker Stack utilises one of the doors and compartments for the Touch screen and Control electronics.

Additional Systems can be added connecting back to a single Control Panel.

This locker range also includes Sound Masking Locker (SML).

5.3   TRAKA TOUCH MODULAR LOCKER

Modular locker solutions allow for operation as a standalone system or can be managed by TrakaWEB for the ultimate administrative control.

As with our other intelligent locker systems, protected items are only available to authorized users, and a complete audit trail is captured for all user activity. This means your assets are secure, and your users are always accountable for the items they access.

With a range of compartment sizes, charging options, access methods and complete integration, Traka's modular lockers provide the ultimate solution in asset management. These systems provide flexibility for various types of assets and are useful when multiple types of different assets need to be managed together.

5.4   TRAKA TOUCH LAPTOP LOCKER

The Traka Touch Laptop Locker System is available in 10 or 15 compartment versions with RFID or non-RFID tagging capability.

These lockers are now available in two variants: original Touch Laptop Locker is equipped with a Resistive Touch Screen and the iMX28 Control Board. A newer version with a Capacitive Touch Screen is equipped with the iMX6 Control Board. For clarity, whenever there are Capacitive Touch Screen models discussed in this guide and their features are different from standard Touch lockers, distinction between the two models is always indicated.

Each compartment provides the option for charging. It is important to return the laptop to the locker in same orientation from which it was removed so that the charging lead may be attached in the correct location.

Additional Laptop Lockers can be installed alongside the main Laptop Locker System allowing up to 100 compartments to be added to a single Control Panel.

Figure 2 – Traka Touch Laptop Locker (left) and Traka Touch Capacitive Screen Laptop Locker (right)

Internal

5.5   TRAKA TOUCH SMARTPHONE LOCKER

The Traka Touch smartphone Locker is available with 20 or 30 compartments with RFID or non-RFID tagging capability.

These lockers are now available in two variants: original Touch Smartphone Locker is equipped with a Resistive Touch Screen and the iMX28 Control Board. A newer version with a Capacitive Touch Screen is equipped with the iMX6 Control Board. For clarity, whenever there are Capacitive Touch Screen models discussed in this guide and their features are different from standard Touch lockers, distinction between the two models is always indicated.

Each locker compartment also provides the option for charging. The user must return the smartphone to the locker in the same orientation from which it was removed to enable the charging lead to be attached in the correct location. Access to the locker is available with the option of HID reader or biometrics.

Additional Smartphone Lockers can be installed alongside the main Locker System, connecting back to a single control panel.

Figure 3 – Traka Touch Smartphone Locker (left) and Traka Touch Capacitive Screen Smartphone Locker (right)

5.6   TRAKA TOUCH ASSET MASTER LOCKER

Asset Master retail and distribution lockers offer an ideal solution for securing, managing and auditing your retail and distribution barcode scanners, printers and other equipment types.

Available in three compartment sizes and with a range of charging, RFID asset identification and access control options, Asset Master lockers offer a flexible and scalable solution to meet your solution needs.

The charging and RFID options will cater to a wide range of applications. Our unique iFob receptors enable items to be secured and managed when the asset is stored externally to the locker.

With three compartment sizes, these systems provide flexibility for various assets, such as radios, scanners, medical equipment, or firearms. They are helpful when multiple types of assets need to be managed together.

This locker range also includes Medicine Dispensing Locker (MDL).

5.7 TRAKA TOUCH LARGE FORMAT LOCKER

Specially designed for your assets and your facility, Traka's large format lockers offer a customized solution for managing a large inventory of assets.

Even with large inventories of critical assets, companies can easily track, store and manage inventory with our software-controlled locker systems. Whether you have hundreds of identical assets to track or an inventory with dozens of different sized items, Traka can engineer a large-scale solution that works for your business.

These systems offer the same accountability, control and efficiency as our other intelligent lockers, but the locker compartments are built to the exact specifications of your unique assets, and to the scale necessary to make sure every item is intelligently managed.

5.8 TRAKA FLEXIBLE ASSET DETECTION LOCKER

NOTE: This product will be released at the start of 2026.

A new Locker solution for a range of equipment such as retail scanners without charging cradles, laptops and tablets:

- New Patent pending UHF RFID Antenna
- Improved usability
- Reduced cost and complexity
- New Industrial Design
- Range consolidation
- Improved manufacturability
- Improved installation and serviceability
- Improved portability

It will allow the retail scanners without charging cradles, laptops and potentially tablets to be placed more liberally in the compartment. This will significantly reduce the need for expensive custom bracketry/inserts to position and contain the equipment and thus improves the overall customer experience.

This will help to future proof the solution by making customer laptop upgrades/changes seamless and by eliminating laptop costs and complexity.

5.9   TRAKA AESTHETIC LOCKER KIT

NOTE: This product will be released at the start of 2026.

The Aesthetic Locker Kit enables Traka's intelligent locker technology to be fitted or retrofitted into locally sourced locker shells. This hybrid solution addresses the need for secure, aesthetically pleasing, and sustainable locker systems, whilst creating the ability for mechanical locker manufacturers to improve their offering by upgrading their capabilities to electronic, centrally controllable lockers.
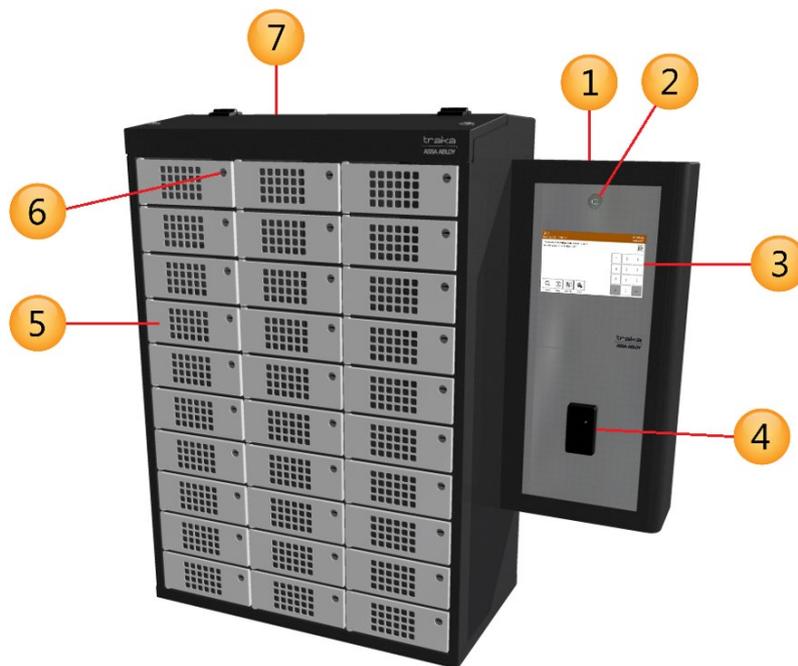
5.10   LOCKER DIAGRAM

5.10.1 LOCKER DIAGRAM KEY

1. **Control Pod**
   Incorporates the Touch Display and Card/Biometrics Reader (if applicable) as well as the Cam Lock providing access to the systems electronics.

2. **Pod Cam Lock**
   This cam lock provides access to the cabinet's electronics during servicing and maintenance. 2 keys are supplied with your Traka system. We ask that you **do not** keep these keys in any locker compartments. In case of system failure, they will be required to gain access to the electronics.

3. **Touch Screen**
   The Touch sensitive LCD works as a user-friendly interface for our embedded application. The numeric keypad, alphabetic keyboard and receptor buttons are incorporated into this easy to use 7" LCD.

4. **Card/Proximity Reader/Biometrics Reader (optional)**
   Traka supports a wide range of access devices. The primary job of any access device is to identify the user to the Traka system. Once the system knows who you are, it can grant or deny access to specific items accordingly.

5. **Compartments**
   Traka Lockers can have different sized doors depending on shape and size of the item the locker is managing. You can also have a mixture of small and large compartments in the same locker system.

6. **Manual Door Override**
   Every compartment is fitted with an electromechanical lock. However, each lock also can also be manually opened with a key in the case of an emergency. 2 manual override keys are supplied with your Traka Locker system. We ask that you do not keep these keys in any locker compartments. In case of system failure, they will be required to gain access to the locker compartments.

7. **Access Cover**
   The Access Cover is a hinged lid that covers the Locker Interface PCBs and the compartment wiring. The cover is locked on both sides with two Cam Locks, and you will be provided with 2 keys, we ask that you do not keep these keys in any locker compartments. In case of system failure, they will be required to gain access to the electronics.

6. OVERVIEW

The Traka Touch system uses touch screen technology for an easy, user-friendly interface. The Traka Touch does not require the use of a stylus or any other navigation device, to use the system simply select the desired buttons with your finger.

6.1   TRAKAWEB

Traka Touch systems are designed to operate as independent standalone systems; however, there also exists an optional web-based solution called TrakaWEB. The TrakaWEB application allows Traka Touch systems to be managed from a platform such as a phone, tablet device or a PC, capable of running a browser.

It has been built to provide simple administration, quick links to actions such as remote release and easy access to summary reports and events.

## 6.2   THE TOUCH SCREEN

6.2.1   SCREEN SAVER
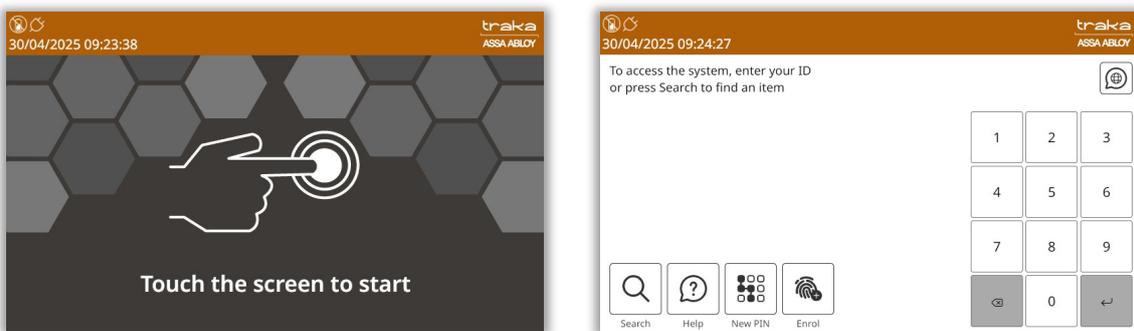
If the Traka Touch system is not used for a user definable period, then the system will go into 'idle' mode. To use the system again simply press anywhere on the touch screen or swipe your card to wake the system up.

It is possible to select the languages to be included in the scrolling screensaver. If this is required, please contact Traka to request a configuration file.

6.2.2 ITEM AVAILABILITY SCREEN SAVER

It is possible to display available items within the Traka Touch system on the screen saver as demonstrated in the image below. This option can be turned on/off within the General Administration page or via a configuration file. See the 'General Options' section for further information.

Internal
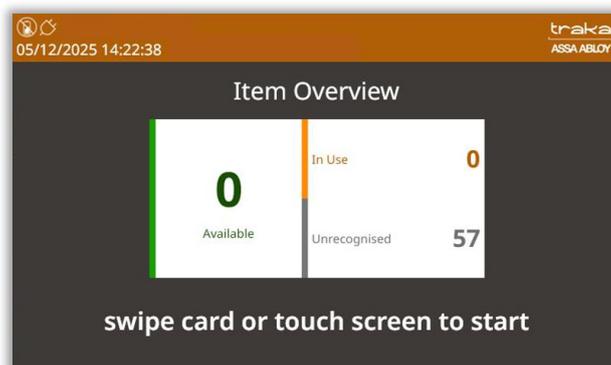
6.2.3 TOUCH COMMANDS

Click – Selecting an onscreen button then immediately releasing will activate it.

Click & Hold – Selecting and holding certain buttons will scroll through menus and various options.

Scroll – Swiping up and down on a list will scroll through the various options.

6.2.4 TOP BAR ICONS

Certain icons will be displayed in the top bar of the Touch system to indicate the current status of the system.

Mains Power Connected – This icon will be present as long as the system is connected to mains power.

USB Memory Stick Inserted – This icon indicates that there is currently a USB stick in the system.

Battery Full – This icon will be displayed when the backup battery is full.

Battery Low – The battery low icon will only appear when the backup battery is low.

Battery Critical – The battery critical icon will only appear when the backup battery is about to run out.

No Battery Connected – This icon appears when the system does not have a backup battery connected.

Alert – This icon will be displayed when the system has an alert message showing in the top bar, see the example below.

Database Backup Failed!
28/02/2023 09:04:24

If your system has an alert and you are unsure what to do, please use the back page of this document to contact support.

7. TYPES OF IDENTIFICATION

The way in which you access the system depends upon the type of identification device fitted, e.g., biometrics reader, card reader or simply a Keypad ID. In addition to a user's primary means of identification, a user may also be given a Secondary PIN providing extra security. Depending on your system configuration, identifying yourself to the system can be accomplished in several ways.

Any Traka Touch system, including those equipped with a biometric (finger) reader, is capable of being fully operated by users without the use of biometric data. Users therefore have a genuine choice about giving consent for their biometric (finger) data to be held and used within the system for this purpose, or not. A user who chooses not to give consent for their biometric (finger) data to be used to identify themself to the Traka Touch system is able to use a Keypad ID (as described below).

7.1   OTHER TYPES OF IDENTIFICATION

Other types of identification are also supported; these include iButton/Dallas Keys or an OSDP (Open Supervised Device Protocol) card reader interface. The minimum app and software requirement for these devices is Traka Touch 2.4.0 and TrakaWEB 3.5.0. For more information, please contact Traka.

NOTE: If this is the first time the system is being used, an Admin user will need to be created. Refer to the 'Users' section for more information.

7.1.1   KEYPAD ID ONLY ACCESS

1. **Touch** the screen to bring the system out of idle mode.

2. **Enter** your Keypad ID and press ⏎ (enter).

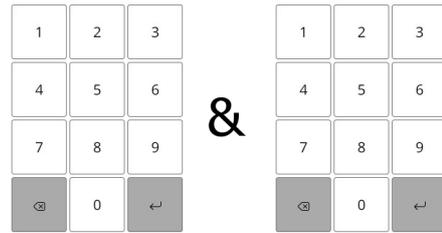3. **Verify** your username on the touch screen.

If required, a config file can be generated by Traka to enable an Alphanumeric Keypad ID and PIN. If this option has been enabled, a different login button will be presented at the login screen and a keyboard will be presented when clicked.

Internal
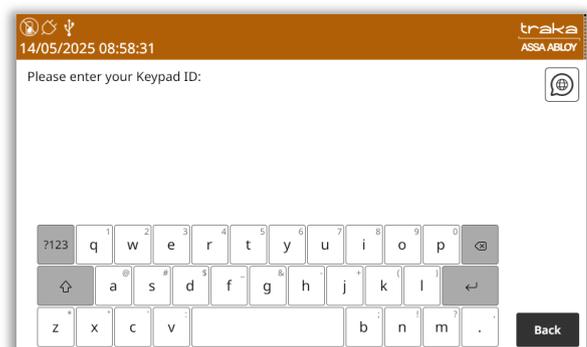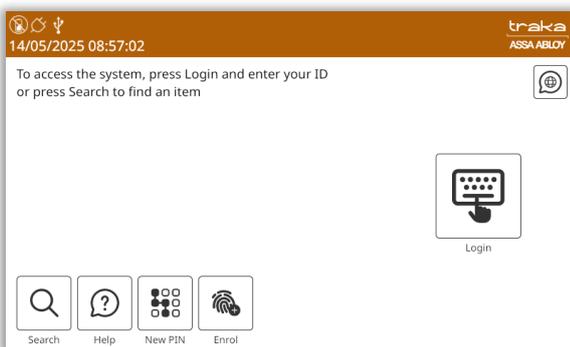
7.1.2   KEYPAD AND PIN ACCESS

1. **Touch** the screen to bring the system out of idle mode.

2. **Enter** your Keypad ID and press ⌨.

3. **Enter** your PIN and press ⌨.
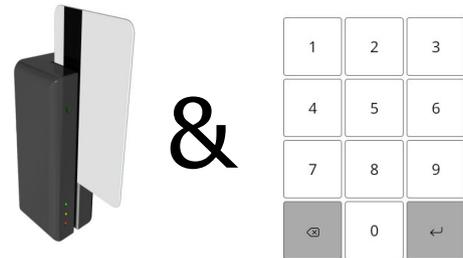
4. **Verify** your username on the touch screen.

7.1.3   CREDENTIAL ID ONLY ACCESS

1. **Swipe** or present your card/token to the reader.
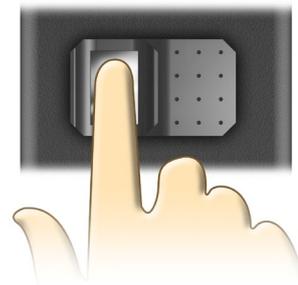
2. **Verify** your username on the touch screen.

7.1.4   CREDENTIAL ID AND PIN ACCESS

1. **Touch** the screen to bring the system out of idle mode.

2. **Swipe** or present your card/token to the reader.

3. **Enter** your PIN and press ⌨.

4. **Verify** your username on the touch screen.

7.1.5   FINGERPRINT ACCESS

1. **Touch** the screen to bring the system out of idle mode.

2. The reader will illuminate red. **Place** your finger on the reader.

3. **Verify** your username on the touch screen.

7.1.6 FINGERPRINT AND PIN ACCESS

1. **Touch** the screen to bring the system out of idle mode.

2. The reader will illuminate red. **Place** your finger on the reader.

3. **Enter** your PIN and press ↵
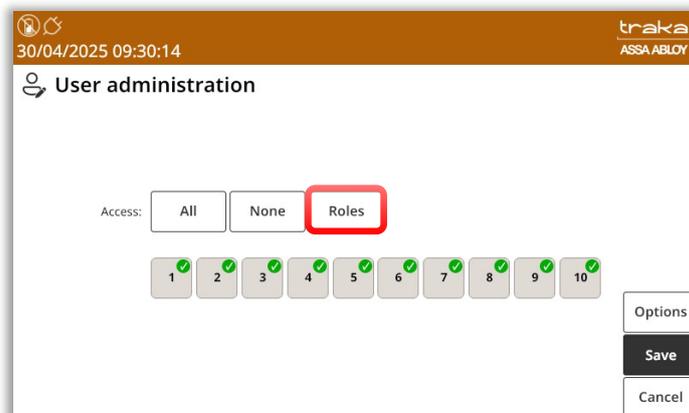
4. **Verify** your username at the touch screen.

1	2	3
4	5	6
7	8	9
⌫	0	↵
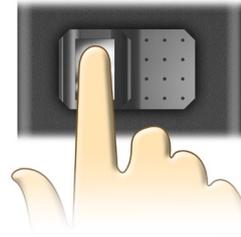
NOTE: There is an event within Traka Touch called 'Duress via PIN +/-1'. This is triggered to notify a duress situation. After a user has accessed the system either by Credential ID or fingerprint, they must input their PIN number + or - 1 digit of their actual PIN number to activate the event. For example, a PIN number, 2222 would be either 2223 or 2221.

7.2 GRANULAR USER PERMISSIONS

Below are examples of what users with different user roles will see when they log in. By default, each system is set up to work in a specific way when releasing items. The Traka default is known as 'I Know What I Want Mode'. This can be changed at any time by an administrator, for more information please review the **Item Release Screen** section. The examples below show users assigned with roles but no items.

An admin role can be assigned to a user to further restrict what Admin functions a Traka Touch Administrator can access when they are logged into the Traka Touch system. The Roles are assigned within the User Administration screen by selecting the Roles button.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

Admin roles can be selected individually from the User Roles list. They may also be assigned from the system access grid in TrakaWEB. For more information, please refer to **UD0018 – TrakaWEB User Guide or UD0260 - TrakaWEB Version 4 User Guide**.
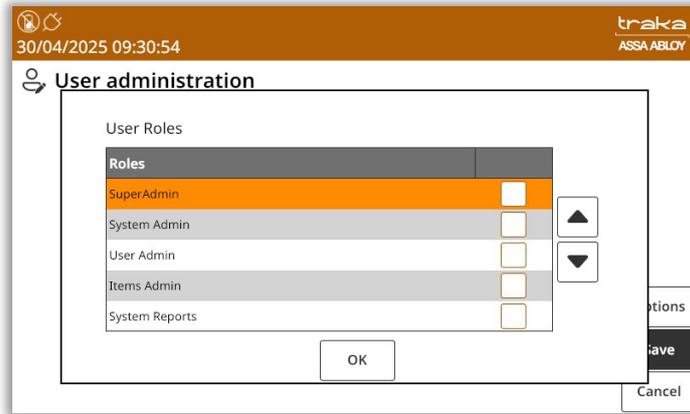
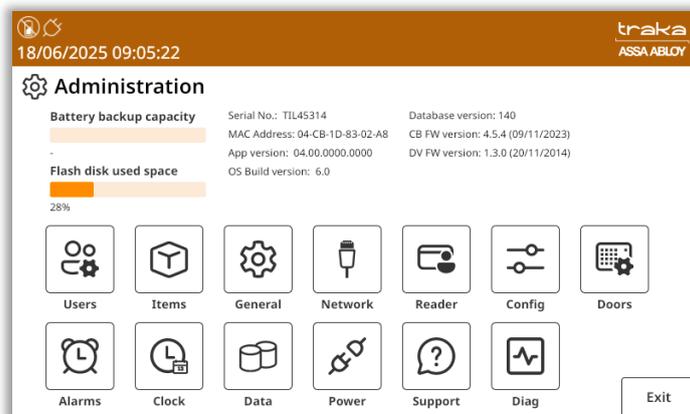**NOTE: Roles not applicable to Traka Touch may only be assigned from TrakaWEB, these will include many of the cost option override features.**
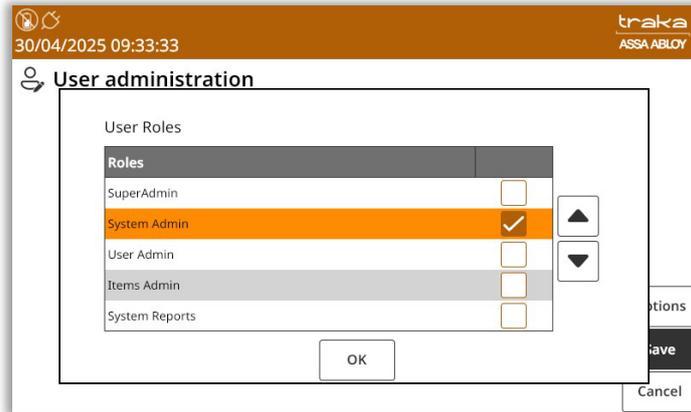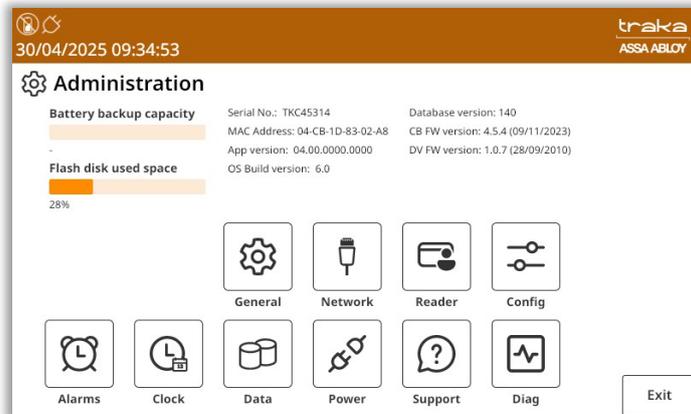
Super Admin Role
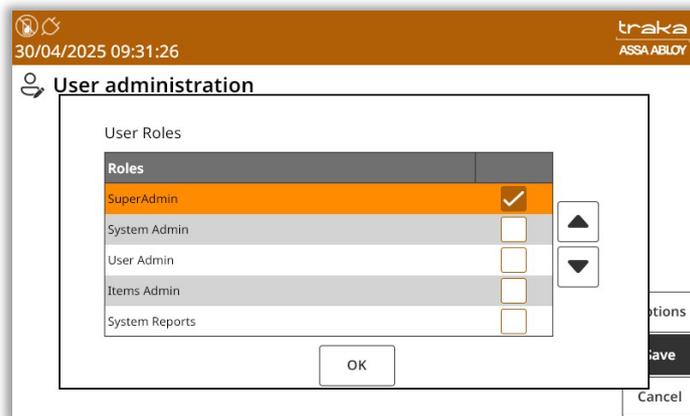
The Super Admin role will grant/revoke the user with all the Admin roles regardless of any of them being selected or deselected.
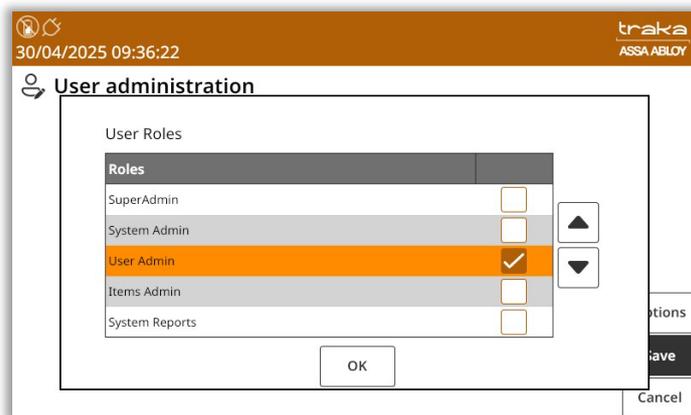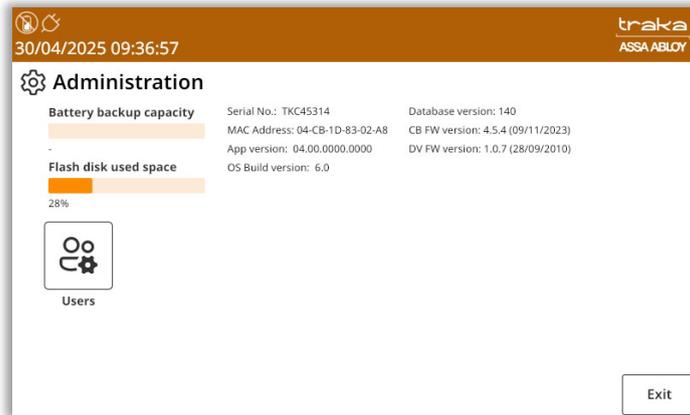
System Admin Only Role

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 enable the ability to edit user records.
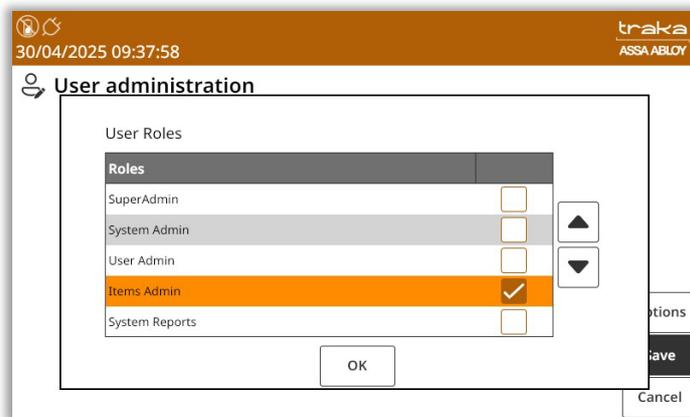

User Admin Only Role

Internal

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.
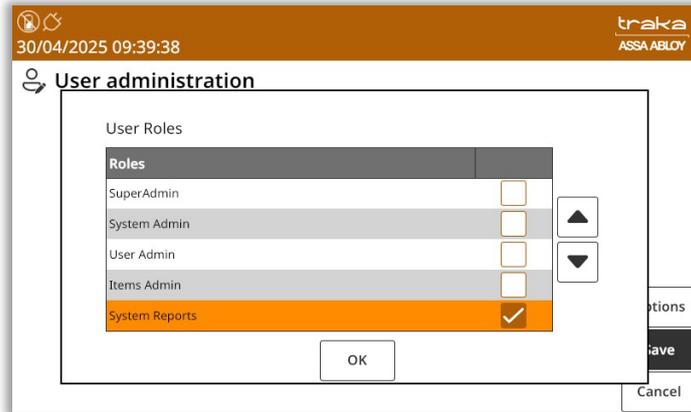

Items Admin Only Role

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.

Internal
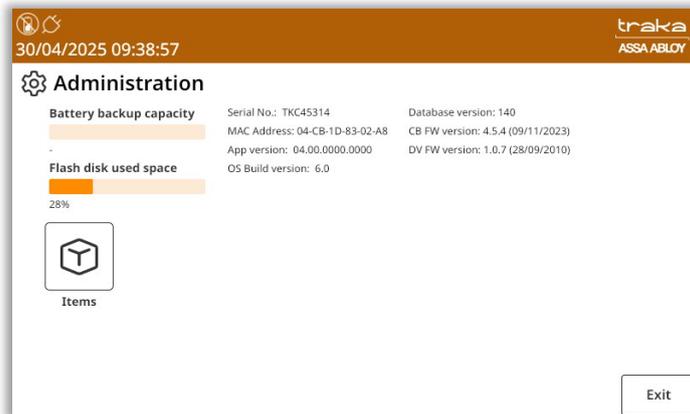
System Reports Only

Selecting this option will allow the user to view & run reports at the Traka Touch system.
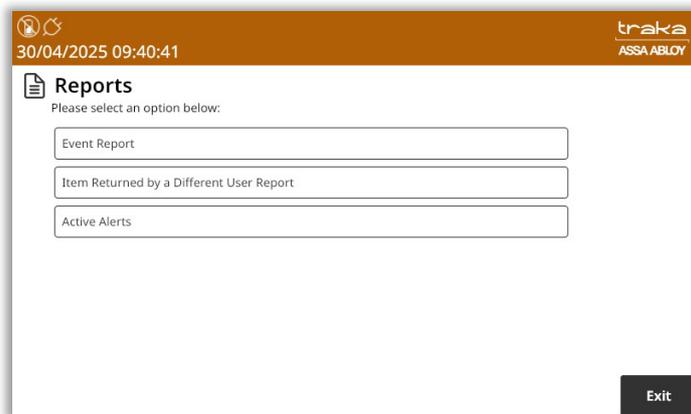
Users with Item Only Permissions

Users without admin or reports permissions will only have access to the system items. The system will take them straight to the item selection screen on login.

Internal

Users with System Admin & Items

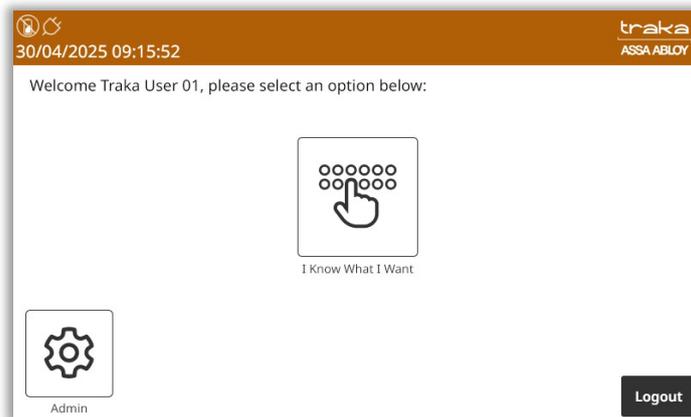Users with the System Admin & Items permissions will be given the choice of selecting the **I Know What I Want** button or accessing the System Admin menu.
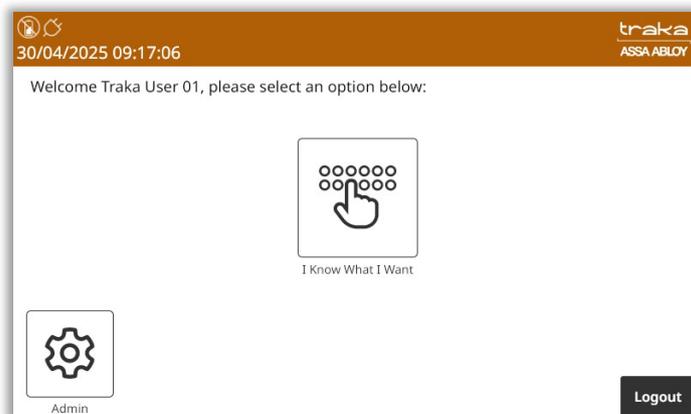

Users with User Admin & Items

Users with the User Admin & Items permissions will be given the choice of selecting the **I Know What I Want** button or accessing the Users Admin menu.


Users with Item Admin & Items

Users with the Item Admin & Items permissions will be given the choice of selecting the **I Know What I Want** button or accessing the Item Admin menu.

Internal

Users with System Reports & Items

Users with the System Reports & Items permissions will be given the choice of selecting the **I Know What I Want** button or accessing the System Reports menu.
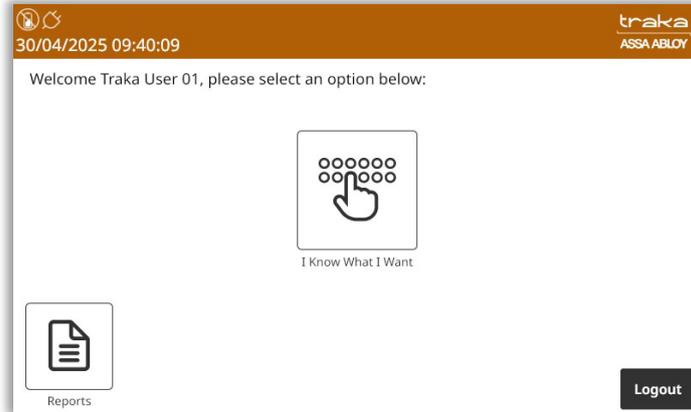
From the User Roles screen, it is also possible to create different combinations of roles that can be assigned to specific users. These can be applied to users with access to both admin roles and items or admin roles only.

NOTE: These combinations exclude the Super Admin Role which, when selected, is a combination of all the User Roles.

Combinations can include:

- System Admin, User Admin, Items Admin
- System Admin, User Admin, System Reports
- System Admin, Items Admin, System Reports
- System Admin, User Admin
- System Admin, Items Admin
- System Admin, System Reports
- User Admin, Items Admin, System Reports
- User Admin, Items Admin
- User Admin, System Reports
- Items Admin, System Reports

7.3 MULTIPLE ID & PIN ATTEMPTS

7.3.1 MULTIPLE ID ATTEMPTS

A user that has been assigned with ID access may be granted any number of attempts to access the system if they attempt to login with an incorrect ID. Although they will be refused access to the system it will not prevent them from attempting to login again. An exception report will be created which can be viewed in TrakaWEB. The default number of attempts required to generate a report is set to 3.

When a user unsuccessfully enters their ID, they will see the following message on the screen:
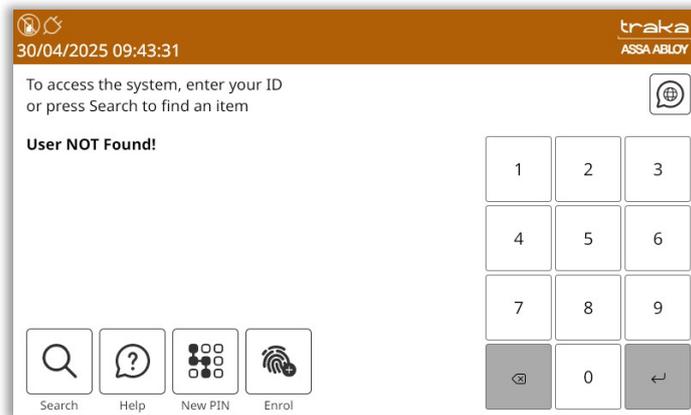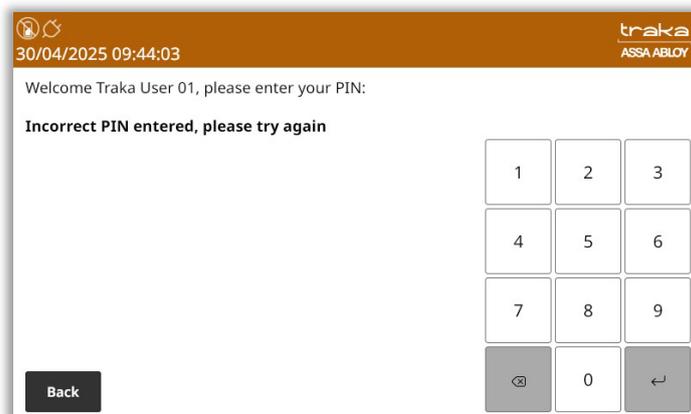

The number of attempts can be set via a configuration through Traka and also through **General Options** in Traka Touch. The value can be set between 0-10. However, setting the value to zero will still display the **User NOT Found!** Message after an unsuccessful ID entry but no report will be generated.

NOTE: This is only true if the System Lock Out option is left in the default 'Off' setting. The System Lock Out feature is included in Traka Touch App version 4.1.0 and higher. For further information, please refer to the System Lock Out section of this document.

7.3.2 MULTIPLE PIN ATTEMPTS

A user that has been assigned with a PIN maybe granted several attempts to access the system after successfully being identified by their primary means of identification. The default number of attempts is set to 3.

When a user unsuccessfully enters their PIN, they will see the following message on the screen:

Internal

If by the third attempt, the user still enters an incorrect PIN, they will see the following message on the screen:
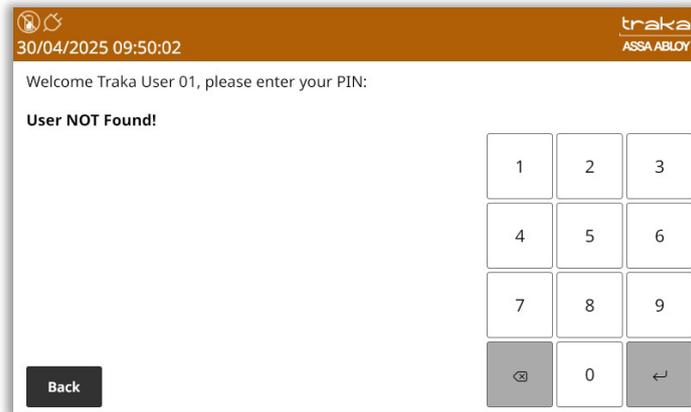
At this point, the user will be logged out and an event will be recorded which can be viewed as an exception report in TrakaWEB.

The number of attempts can be set via a configuration through Traka and through **General Options** in Traka Touch. The value can be set between 0-10. However, setting the value to zero will only display the **User NOT Found!** message after an unsuccessful PIN entry. The user will not be logged out and no report will be generated.

NOTE: This is only true if the System Lock Out option is left in the default 'Off' setting. The System Lock Out feature is included in Traka Touch App version 4.1.0 and higher. For further information, please refer to the System Lock Out section of this document.
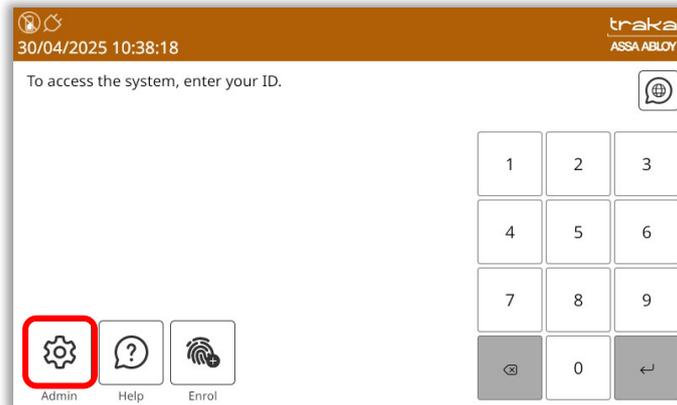
8. USERS

### 8.1 CREATING THE FIRST ADMIN USER

When using Traka Touch for the first time, the initial step is to create a user. The first user to be created must be an admin user.

NOTE: From here, you can select the language you wish the Touch System to display by selecting the Globe above the keypad. However, selecting a language from this screen will only last as long as the current user is logged in. The system will return to the default language when another user logs into the system. For further details on languages, please refer to the [Languages](#) section.

1. From the login screen, select **Admin**.

2. When the Admin screen appears select **Users**.
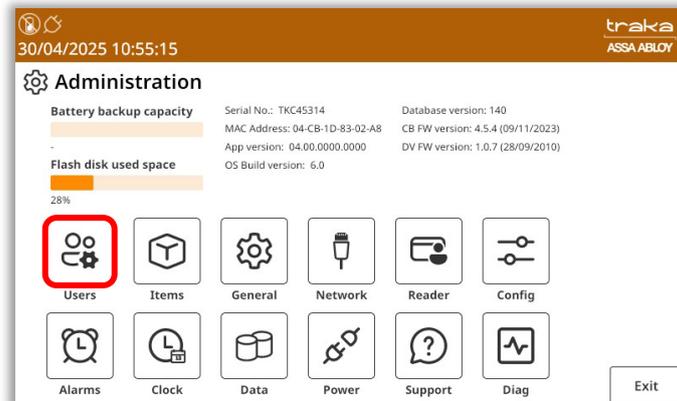
3. The User list will currently be empty. Select the **Add** button.

NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

4. Type your user details into the provided fields. To switch fields simply select the desired field or select the ↵ (Enter) button to scroll through them.

NOTE: Systems with Multiple Credentials enabled (available on Linux systems running future versions of the Traka Touch Application)will not allow a User's Credential ID to be edited in Traka Touch (see above right-hand image). Credential ID can only be edited in TrakaWEB – this is denoted by the message 'Available in TrakaWEB'. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

NOTE: If a single credential system is networked to one or more systems with multiple credentials enabled via TrakaWEB, it will still be possible to edit the Credential ID on Traka Touch. When synced with TrakaWEB, this Credential ID will create a new credential row and will be automatically assigned as the default credential, replacing the previous default. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

5. You can also select a default language for the user by using the dropdown menu to select the language. For further details on languages, please refer to the Languages section.

6. There are two levels of access when using a Traka Touch system, Primary and Secondary. A primary level of access can either be a Credential 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 (Credential ID, Keypad ID or Fingerprint).

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.

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, Credential ID or Fingerprint ID. For example, if you have a credential ID as your primary level of access, when you log into the system you will be prompted for your PIN after swiping your card.

Credential ID
Here you can input your swipe card ID number. Alternatively, you can swipe your card at the reader and the Traka Touch system will automatically fill in the field for you.

7. Select the **Access** button to take you to the next screen.

Internal

8. From the Access screen, select which items you wish to have access to and whether you wish to view and export key reports. Each of the access buttons on screen corresponds with an item in the system. E.g., The '1' button will only grant or remove access to the item in position 1. The tick and line symbols define whether you have access to the item or not. For example, any item with the tick symbol ✅, indicates that you currently have access to the item. The line symbol ⛔ indicates that you do not have access to the item.

NOTE: **The first user entered into the Touch system must be an admin user; therefore, the admin button cannot be disabled for the first entry of a user.**
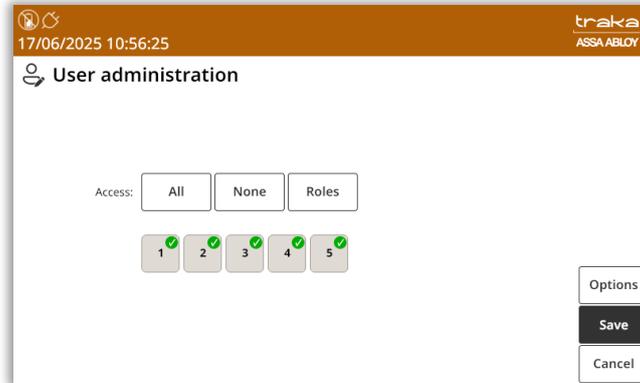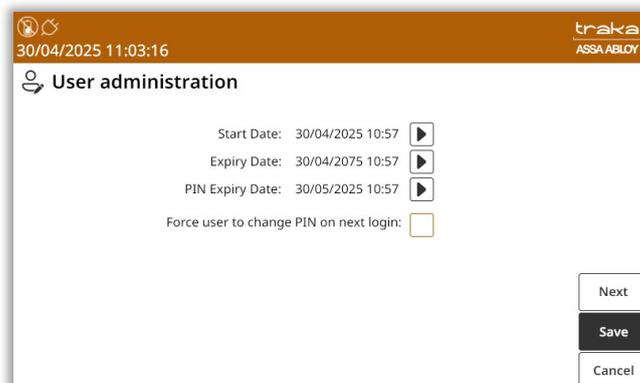

NOTE: **If the RRMS option has been enabled. The ability to allocate iFobs or Reports to users will not be available as shown in the example below:**

Options

Selecting the Options button will allow you to define certain activation and expiry dates relating to the users and their secondary PIN. From here, you can also force the user to change their PIN when they next log into the system.

NOTE: **If you have RRMS enabled, some of the options will not be available.**

Internal

Start Date

The user active date defines when a user becomes able to use the Traka Touch system. Selecting the arrow button will generate a pop-up window that allows you to manually define the date and time you wish the user to become active.

Selecting the arrow will take you to another screen where you can use the scroll function to adjust the Start Date as shown:

Expiry Date

The user expiry date defines when a user becomes unable to use the Traka Touch system. E.g., after this period, the user will no longer be able to do anything they were previously permitted to. Selecting the arrow button will generate a pop-up window that allows you to manually define the date and time you wish the user to expire.

Selecting the arrow will take you to another screen where you can use the scroll function to adjust the Expiry Date as shown:

PIN Expiry Date

From here, you can define when the users PIN will expire. After this period, the user will have to assign themselves a new PIN when they next access the system. Selecting the arrow button will generate a pop-up window that allows you to manually define the date and time you wish the PIN to expire.

Selecting the arrow will take you to another screen where you can use the scroll function to adjust the PIN Expiry Date as shown:

Internal

Force User to Change PIN on Next Login
Enabling this option will force the user to change their PIN when they next access the system, regardless of the PIN Expiry Date. Once they login and change, it will not ask again until the PIN Expiry Date, unless this option is selected again.

At the next screen, you will be able to allocate the User Item Allowance and User Curfew Type.

Item Allowance
This section allows you to select how many items the user can remove from the system. Simply scroll through the different options using the directional arrow keys. The options are as follows…

- No item Allowance Enforced
- User is allowed a maximum of 1-XX item(s)
- The Systems Default User Item Allowance Will Apply.

This is defined in the **General Settings** in the Admin menu.

User Curfew Type
Here, you will be able to select from None, Specific time of day and Days/Hours Minutes. Please refer to the **Curfews** section for more information.

Once you have selected the desired option, select **Save**.

NOTE: If you are using a Fingerprint Reader, at this point you can click the Enrol button instead of Save. Please refer to the Sagem MorphoSmart Reader Section for details on how to enrol the user.

After adding the user, you will be taken back to the User Admin page.

To add more users simply click the **Add** button and repeat this process. After adding the user, you will be taken back to the User Admin page.
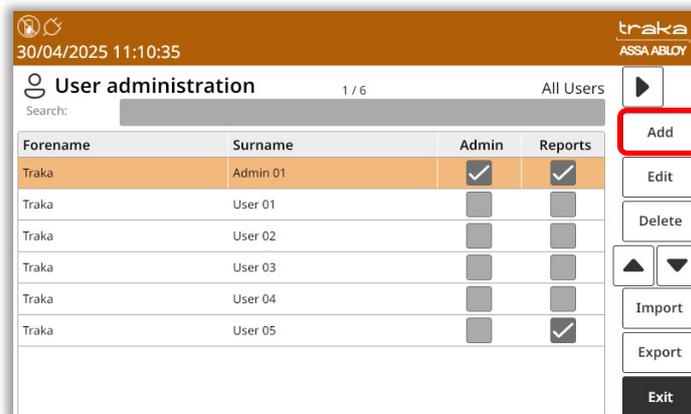
NOTE: If you are using RRMS, there is no option to allocate Reports to users; therefore, the Reports column will not be displayed on the User Admin page as can be seen in the example below:

At this point, you can add more users by selecting the **Add** button and repeating steps 4-8. If you wish to continue without adding any more users, please carry on to the next step. When you have finished adding users select **Exit**. You will be taken back to the Admin screen, from there select **Exit** again to return to the login screen.

8.2   ADDING MORE USERS

NOTE: This action can only be performed by an Admin user.
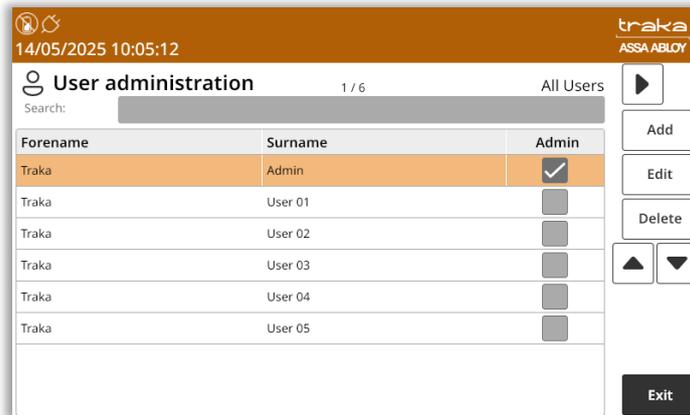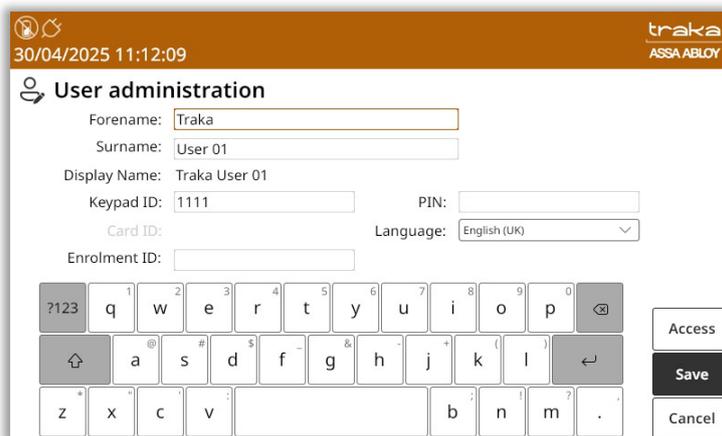
1. Access the system.

2. Select **Admin**.

3. From there select **Users**.

4. The current user list will then be displayed. Select the **Add** button.

5. Type your user details into the provided fields. To switch fields simply select the desired field or click the (Enter) button to scroll through them.

NOTE: Systems with Multiple Credentials enabled (available on Linux systems running future versions of the Traka Touch Application) will not allow a User's Credential ID to be edited in Traka Touch (see above right-hand image). Credential ID can only be edited in TrakaWEB – this is denoted by the message 'Available in TrakaWEB'. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

NOTE: If a single credential system is networked to one or more systems with multiple credentials enabled via TrakaWEB, it will still be possible to edit the Credential ID on Traka Touch. When synced with TrakaWEB, this Credential ID will create a new credential row and will be automatically assigned as the

Internal

default credential, replacing the previous default. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

6. You can also select a default language for that particular user by using the dropdown menu to navigate to the desired language. For further details on languages, please refer to the [Languages](#) section.

7. There are two levels of access when using a Traka Touch system - Primary and Secondary. A primary level of access can either be a Credential 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 (Credential ID, Keypad ID or Fingerprint).

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.

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

Credential ID
Here you can input your swipe card ID number. Alternatively, you can swipe your card at the reader and the Traka Touch system will automatically fill in the field for you.

8. Select the **Access** button to take you to the next screen.
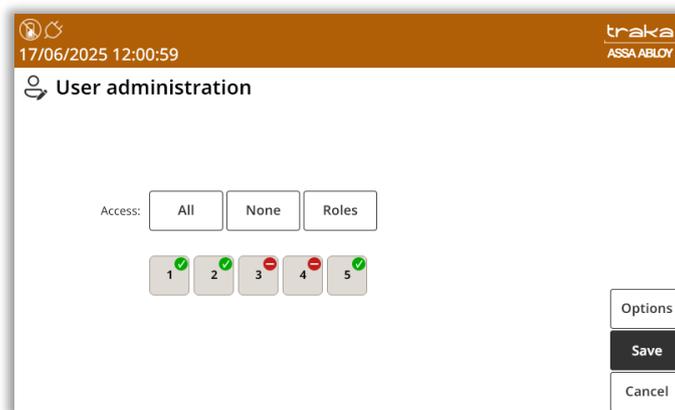
NOTE: If you have RRMS enabled, the option to allocate iFobs to users is not available as shown in the example below:

9. From the Access screen, select which items you wish to have access to and whether or not you wish to view and export item reports. Each of the access buttons on screen corresponds with an item in the cabinet. E.g., the '1' button will only grant or remove access to the item in position 1. The tick and line symbols define whether you have access to the item or not. For example, any item with the tick symbol ✅, indicates that you currently have access to the item. The line symbol 🚫 indicates that you do not have access to the item. The grey tick symbol ☑, indicates that the user has already been allocated these items through the 'Item Access Groups' within TrakaWEB.

NOTE: Item Access Groups is a TrakaWEB feature. It does not apply to stand-alone systems. For more information on Item Access Groups, refer to the TrakaWEB User Guide - UD0018 or UD0260 - TrakaWEB Version 4 User Guide.

<u>**Roles**</u>

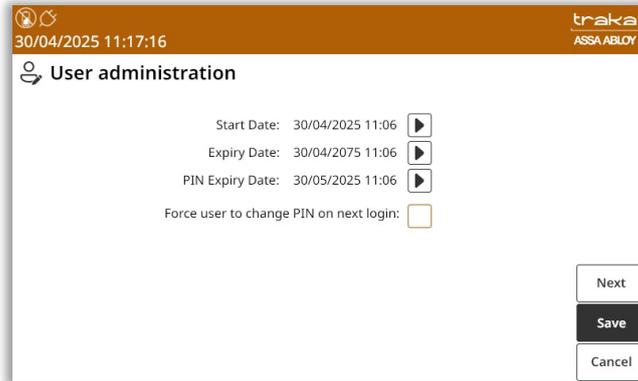From the User Administration Screen, the **Roles** option can also be selected.

The **Roles** function will enable an admin user to view a summary of specific roles that have been allocated to users. Some of these can only be enabled from TrakaWEB. For Item Users, no roles will be active. In the example shown below, the Fault Administrator role is shown as active to that particular user.
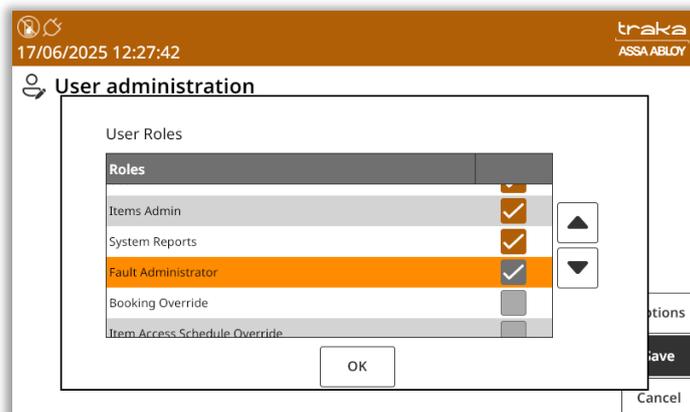
Internal

Options

Selecting the Options button will allow you to define certain activation and expiry dates relating to the users and their secondary PIN also you can force the user to change their PIN when they next log into the system.
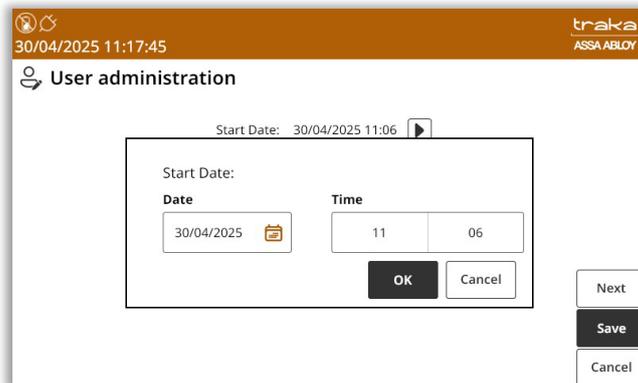

Start Date

The user active date defines when a user becomes able to use the Traka Touch system. Selecting the arrow button will generate a pop-up window that allows you to manually define the date and time you wish the user to become active.

Selecting the arrow will take you to another screen where you can use the scroll function to adjust the Start Date as shown:

Expiry Date

The user expiry date defines when a user becomes unable to use the Traka Touch system. e.g., after this period, the user will no longer be able to do anything they were previously permitted to. Selecting the arrow button will generate a pop-up window that allows you to manually define the date and time you wish the user to expire.

Selecting the arrow will take you to another screen where you can use the scroll function to adjust the Expiry Date as shown:
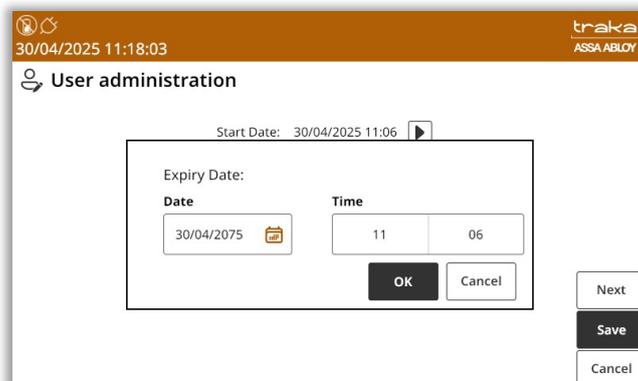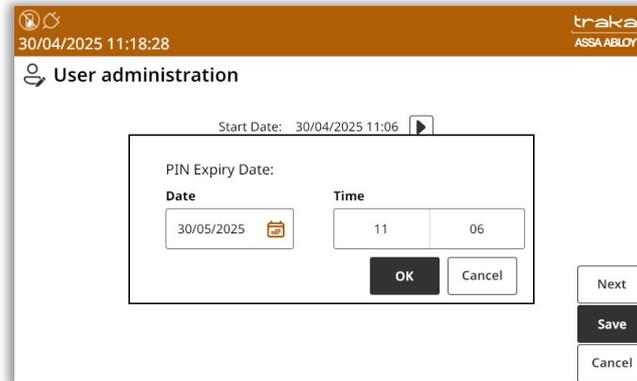
Internal

PIN Expiry Date
From here, you can define when the users PIN will expire. After this period, the user will have to assign themselves a new PIN when they next access the system. Selecting the arrow button will generate a pop-up window that allows you to manually define the date and time you wish the PIN to expire.

Selecting the arrow will take you to another screen where you can use the scroll function to adjust the PIN Expiry Date as shown:

Force User to Change PIN on Next Login
Enabling this option will force the user to change their PIN when they next access the system, regardless of the PIN Expiry Date. Once they login and change, it will not ask again until the PIN Expiry Date, unless this option is selected again.

Allow user to Authorise an Items and/or System Access
Selecting this option will allow this user to authorise other users when they remove an item from the system, or when they access the system. Please view the **Authorisation** section for more details.

Allow User to Override Authorisation
This option will allow a user to override authorisation that has been granted to other users. Please refer to the **Authorisation** section for more details.

At the next screen, you will be able to allocate the User Item Allowance and User Curfew Type.

Item Allowance
This section allows you to select how many items the user can remove from the system. Simply scroll through the different options using the directional arrow keys. The options are as follows…

- No item Allowance Enforced
- User is allowed a maximum of 1-XX item(s)
- The Systems Default User item Allowance Will Apply.

This is defined in the **General Settings** in the Admin menu.

User Curfew Type
Here, you will be able to select from None, Specific time of day and Days/Hours Minutes. Please refer to the **Curfews** section for more information.

Once you have selected the desired option, select **Save**.

NOTE: If you are using a Fingerprint Reader, at this point you can click the Enrol button instead of Save. Please refer to the Sagem MorphoSmart Reader Section for details on how to enrol the user.

After adding the user, you will be taken back to the User Admin page. To add more users simply click the **Add** button and repeat this process.

8.3   EDITING USERS

NOTE: This action can only be performed by an Admin user.

1. Access the system and select **Admin**.

2. From here, select **Users**.

3. The current user list will then be displayed. Highlight the desired user and select the **Edit** button.
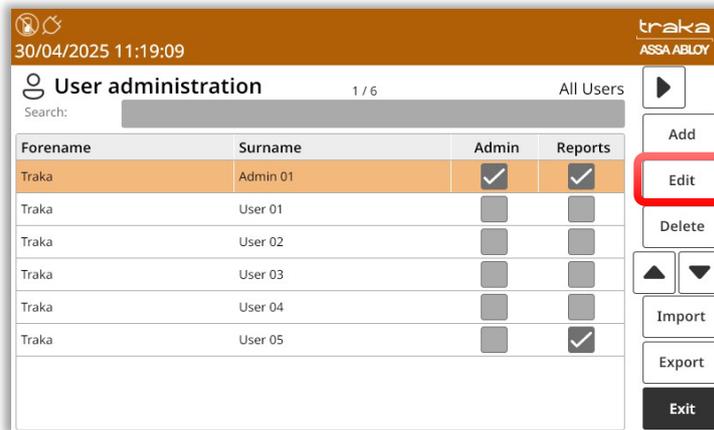
NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide. Multiple Credentials will be available on Linux systems running future versions of the Traka Touch Application

4. Simply scroll through the user details and change the desired settings.
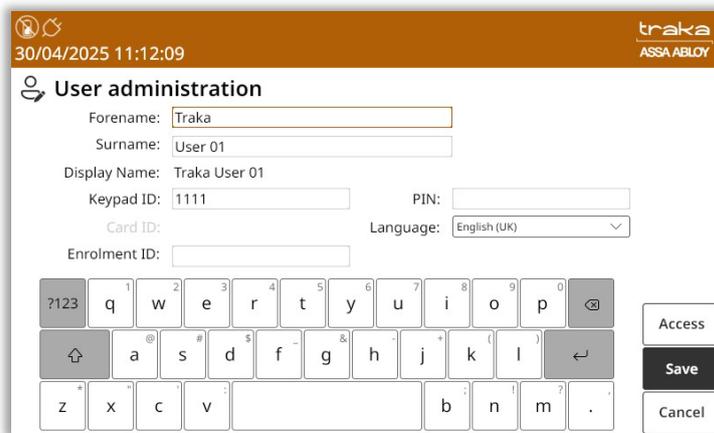
NOTE: Systems with Multiple Credentials enabled (available on Linux systems running future versions of the Traka Touch Application) will not allow a User's Credential ID to be edited in Traka Touch. Credential ID can only be edited in TrakaWEB. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

NOTE: If a single credential system is networked to one or more systems with multiple credentials enabled via TrakaWEB, it will still be possible to edit the Credential ID on Traka Touch. When synced with TrakaWEB, this Credential ID will create a new credential row and will be automatically assigned as the default credential, replacing the previous default. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

5. Once you have changed the appropriate settings click the **Save** button.

8.4   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 is 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).

NOTE: **This action can only be performed by an Admin user.**

1. Access the system and click **Admin**, **Users**, then highlight the desired user and select **Delete**.
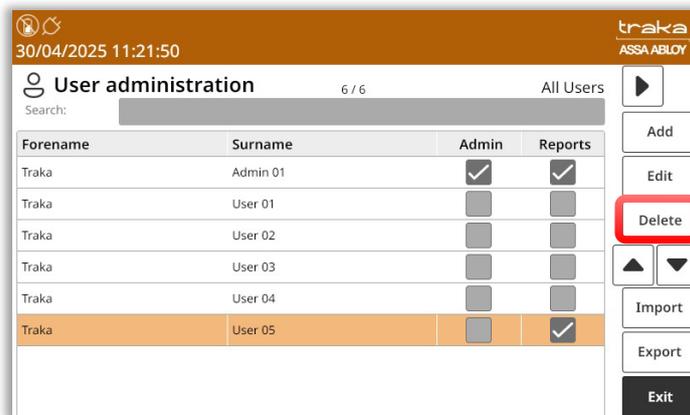
NOTE: **If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.**

2. The following screen will ask you whether you wish to permanently delete the user, click **Yes**.
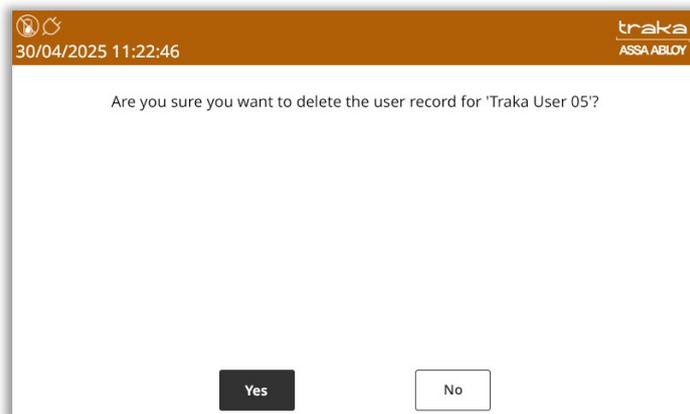
NOTE: **If you are deleting all of the users in the system, the last user to be deleted must be an admin user.**

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

3. You will then notice the user has been removed from the user list.
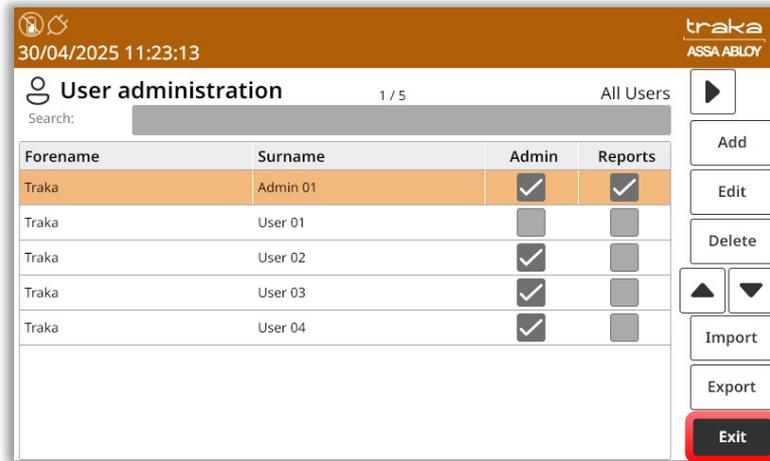
4. Click **Exit** to be taken back to the administration menu. From there, click **Exit** again to return to the login screen.

8.5 SUPPORTING A LARGE NUMBER OF USERS

In order to enhance system performance, a search bar is used within the User Administration screen on Traka Touch to handle a large number of users.

1. Click on the search bar.

Internal
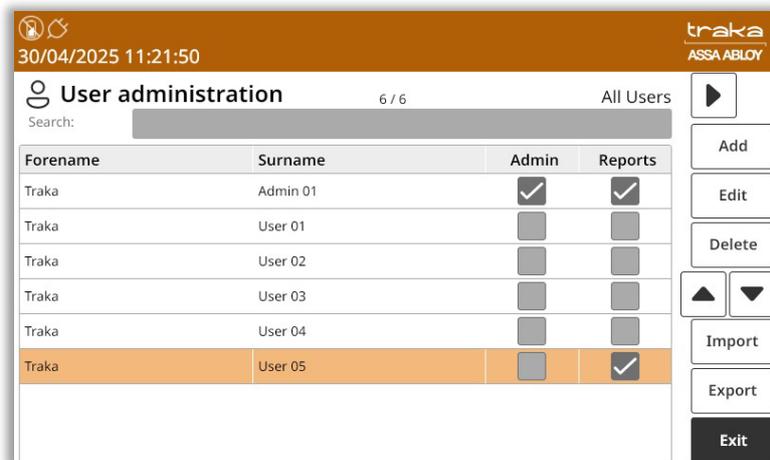
Less than 500 users

If there are 500 or less users within the system, the option to **Show All** button will be displayed.
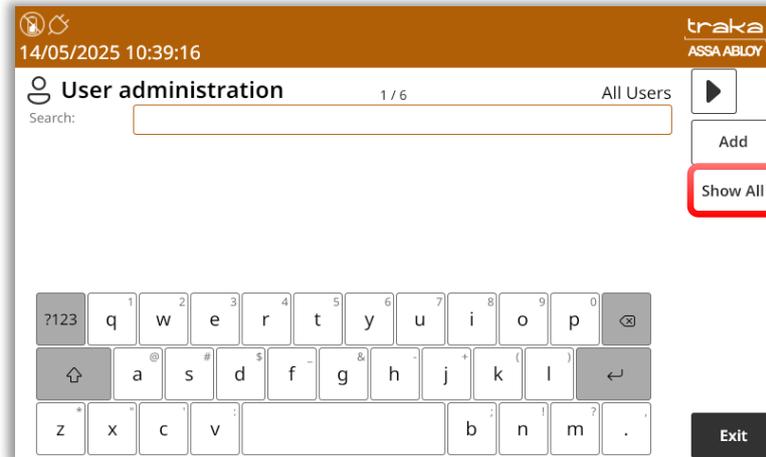
Selecting **Show All** will display all the users within the grid.

NOTE: A username can also be entered in the search bar. Selecting 'Search' will display all matching results.

More than 500 users

If there are more than 500 users within the system, only the option to **Search** will be available.
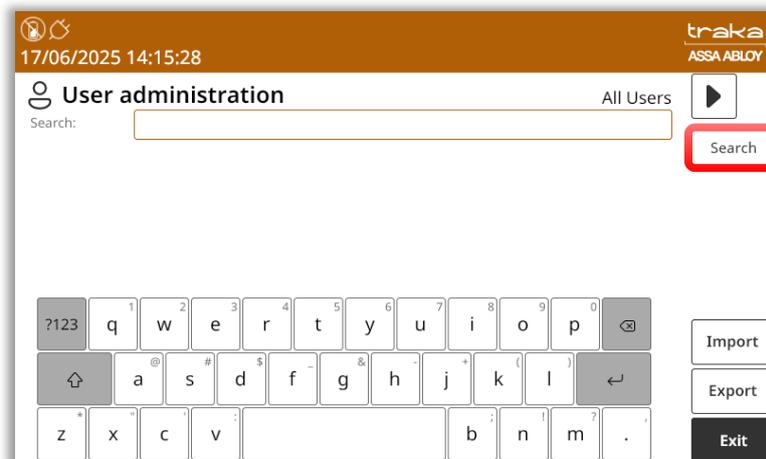
2. A username can be entered in the search bar. However, a minimum of 2 characters may be entered. Clicking on **Search** will display all matching results.

Internal

8.6 USER ENROLMENT ID

An Enrolment ID is a number assigned to a user to enable them to enrol directly at the Traka system without the need for an admin user to be present. This feature can be used only with Card or Biometric readers.

To use the enrolment ID feature, you must first specify whether the system is fitted with the integrated Sagem Biometrics Reader or a Card Reader in the Reader Admin options.

1. An admin user is required to access the system and select **Admin**.
2. Select **Reader**.

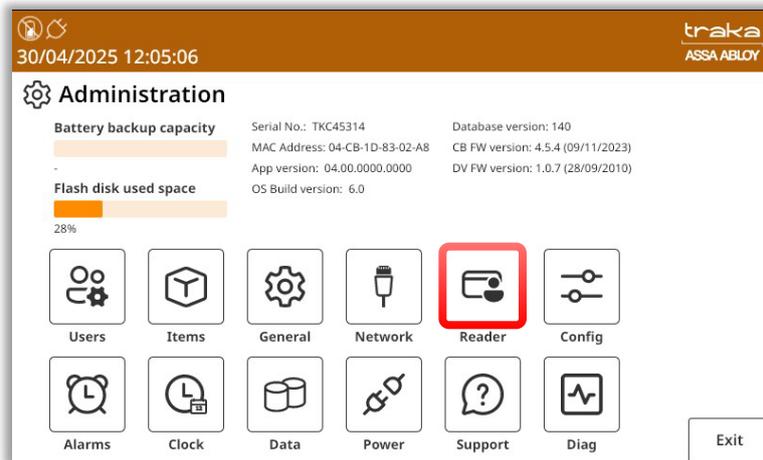3. Select the relevant reader type for the Enrolment ID enrolment method. If you have both types of reader fitted to your system, select the one you wish to use for enrolling with the enrolment ID. Click **Save.**
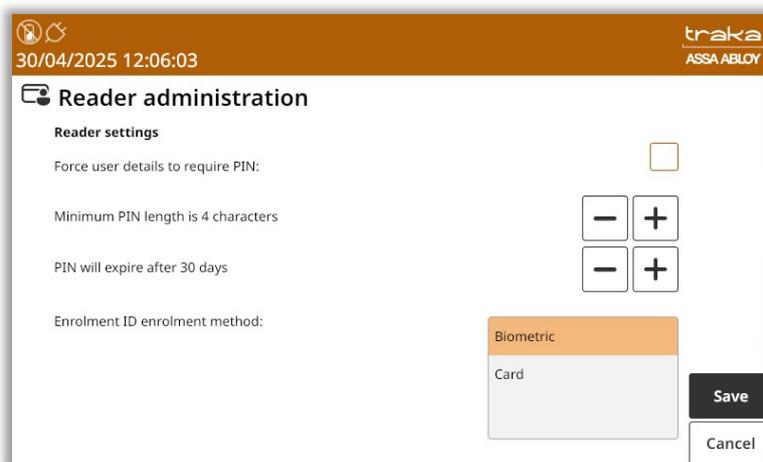
The Enrolment ID must be entered into the correct field either in the user record within the Traka Touch System, or in the Enrolment ID field in the user import spreadsheet. If your system is being used in conjunction with TrakaWEB, the enrolment ID can be entered in the user record under the 'System Access' tab. Refer to **UD0018 - TrakaWEB User Guide or UD0260 - TrakaWEB Version 4 User Guide** for more information.

The example below shows how to assign an Enrolment ID to a user at the Traka Touch system. For more information on how to import users via a spreadsheet, refer to the section 'Exporting & Importing'.

NOTE: **The following must be carried out by an Admin User.**

1. Create a new or edit an existing user.

2. Enter the Enrolment ID into the Enrolment ID field. Enter any other required details including any access the user may require and click **Save**.

3. The user can now select the **Enrol** button from the home screen.

4. The user will be prompted to enter their Enrolment ID. Enter the ID and click [↵] (enter).

Internal

5. If you are using a Sagem MorphoSmart Biometric reader, you will be asked to present your finger to start the enrolment process. For more information on enrolling with a Sagem MorphoSmart reader, please refer to the [Sagem MorphoSmart Reader](#) section. If you are using a card reader, you will be prompted to swipe your card.
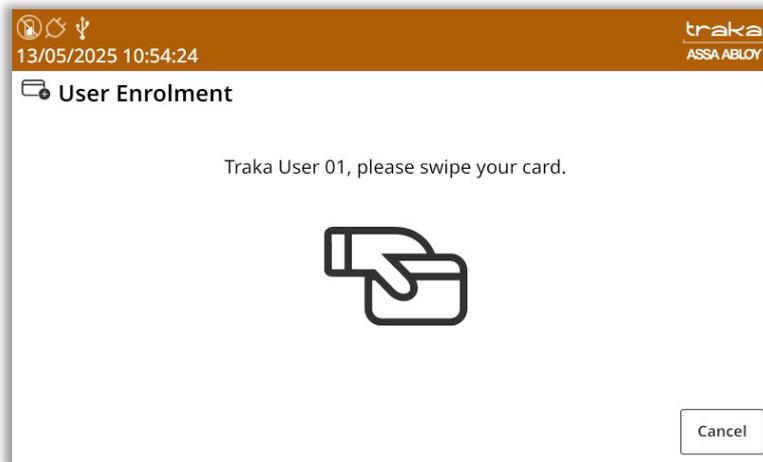
6. Swipe your card to complete the enrolment.
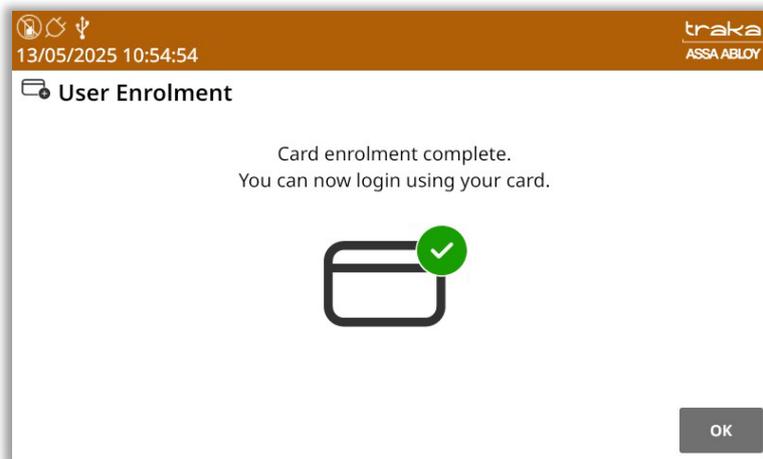
9. DOOR ADMINISTRATION

NOTE: This process can only be performed by an Admin User.

The door administration process allows you to configure each compartment number. For example, if you wanted the compartment numbers to run from left to right, or if you wanted them to run from top to bottom, any combination is possible.

1. Access the system and click **Admin**.

2. Click **Doors**.

3. Click **Setup**.
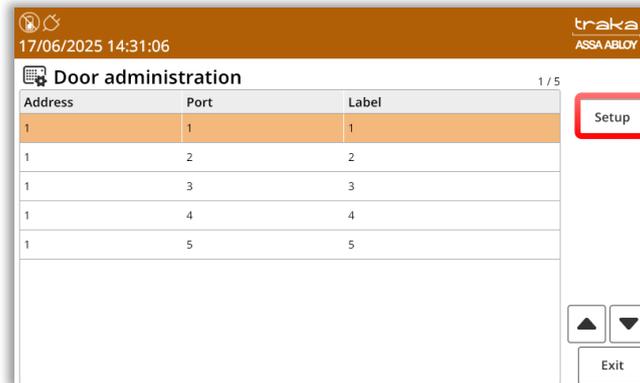
4. A message will appear asking if you wish to setup all doors. Click **Yes**.
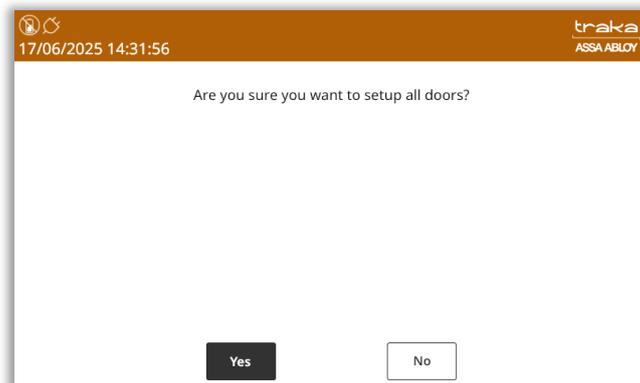
5. All of the doors in the system will now open. During this period, do not close any of the doors.

Internal
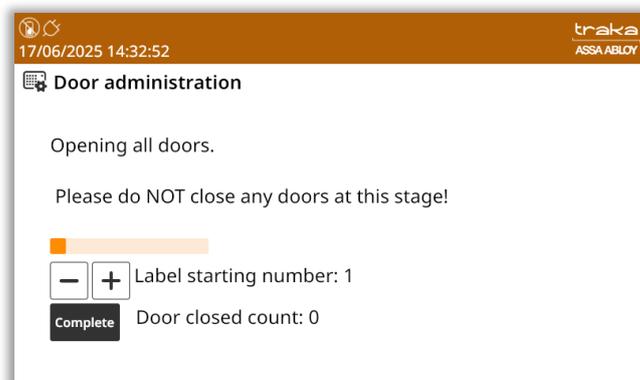
6. Using the directional arrow keys, select the door number you wish to start with.
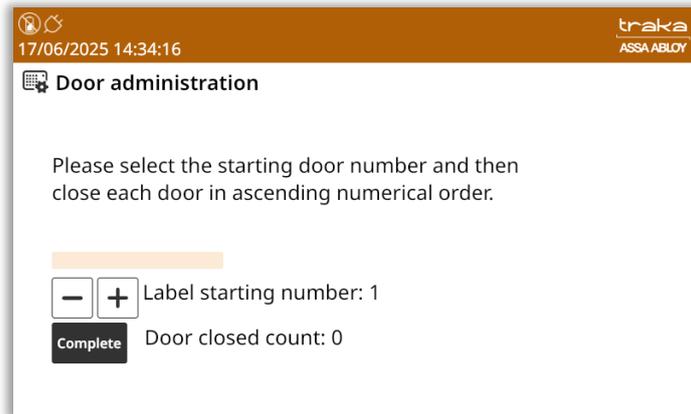
7. Once you have selected the starting number, begin closing each compartment door in ascending numerical order.

8. When you have finished closing all of the doors, click the **Complete** button.

9. If your hardware has the facility to connect more doors than your system has, the system will recognise this and present you with the message shown below. In this example, the hardware can connect to 10 doors but only 5 are connected.
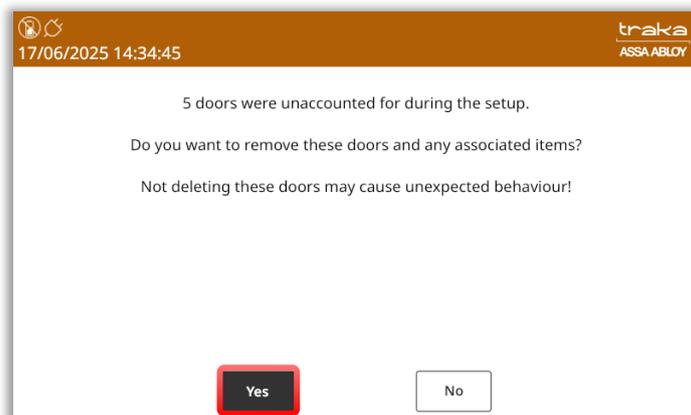
10. Select **Yes** and the system will remove these doors and any items that may have previously been associated with them. You will then be taken back to the Door Administration page.
11. Once completed, select **Exit** to return to the admin menu, and **Exit** again to return to the login screen.

Internal

9.1 RELEASE/RELEASE ALL DOORS ON LOCKERS

The option to release individual doors or release all doors is an option specific to stand-alone locker systems and can be performed during production or by a Traka Installation Engineer. It will enable a user to carry out basic checks to ensure that each locker door is responding without the interference of any additional options or features. The option will only be made available when there are no active Admin users in the Traka Touch database.

When a user accesses the Doors Admin screen, 2 buttons will be visible for **Release** and **Release All.**
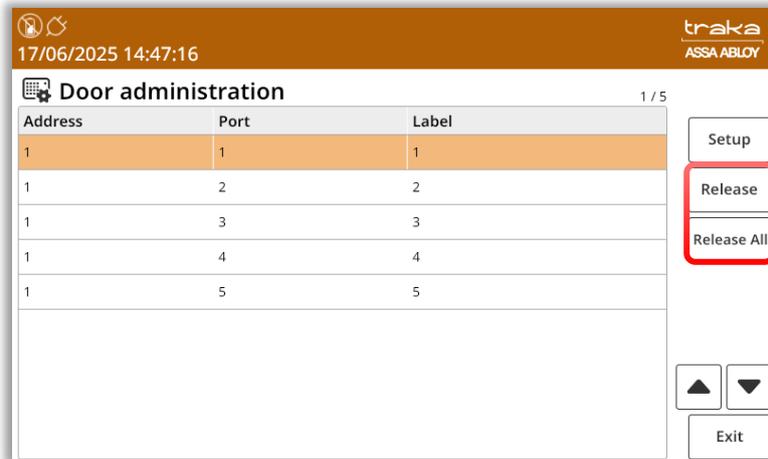
Release

This button will enable the User to select and release specific doors to the locker system.

Release All

When pressed, this button will release all the doors to the locker system.

Once an Admin User is added to the Traka Touch database, the **Release** and **Release All** doors buttons will no longer be visible.

Internal
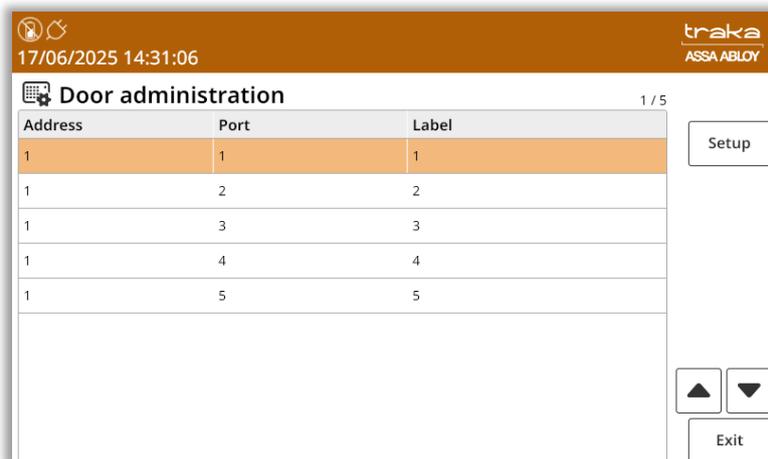
10. ITEM ADMINISTRATION

This section explains how to assign items to each locker compartment.

NOTE: **This section is only relevant if your Locker system is configured with the Traka RFID technology.**

10.1   RFID LOCKERS

Traka RFID lockers are used in situations where controlling who has access to the item is itself not enough. In such circumstances, it is often necessary to know exactly when the item was taken, when it was returned, and to ensure that it was returned to the correct location.

If your system is a RFID system, the locker compartments will have been designed specifically for the item(s) being stored. In addition to this, each item will have to be fitted with an RFID Tag.

10.2   RFID TAGGING

In a RFID locker system the compartments are designed specifically for the item(s) being stored. A guide on how to tag your item correctly will be supplied with your Traka Locker system.

The largest tag Traka use is the 50mm Adhesive Tag which is typically used on larger items such as Laptops and tablets. The smallest tag used is the 12mm glass tag, which is generally used on smaller assets such as radios, PDA's or mobile phones. Some examples of the RFID Tag types are shown below.

| 50mm Self Adhesive Tag | 35mm Self Adhesive Disk Tag | 25mm Traka Disk Tag | 20mm Clear Disk Tag | 12mm Black Logistics Tag | 12mm Glass Tag |

10.3   HITAG1/S RFID READER

Some radio manufacturers now embed the RFID tag within the radio itself. The Hitag1/S RFID Reader for Radio Management provides the same functionality as with other readers, to read the tag within the Locker compartment when an Item is removed or replaced.

10.4   CONFIGURING ITEMS

NOTE: **This section is only applicable to RFID systems.**

Configuring items must be carried out by an admin user. Please refer to the 'Users' section for more details.

1. Using the master override key, open each compartment and place the items in the correct locations and close the doors.

2. Log into the system.

Internal

3. Click **Admin**.

4. Click **Items**.

5. The item list will currently be populated with unrecognised items. To synchronise your items, click the **Setup** button.
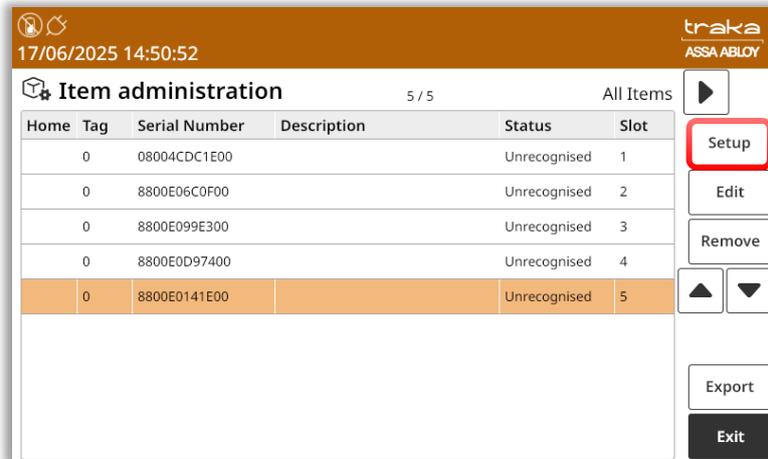
6. You will be asked if you wish to setup all items. Click **Yes**.
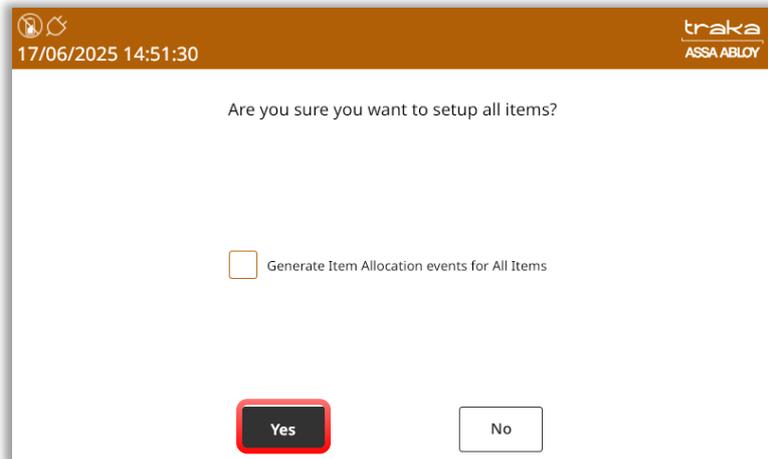
7. The item list will now begin to populate, showing all the items that are being recognised. This process is displayed via the small blue progress bar in the top right corner of the window.

Internal
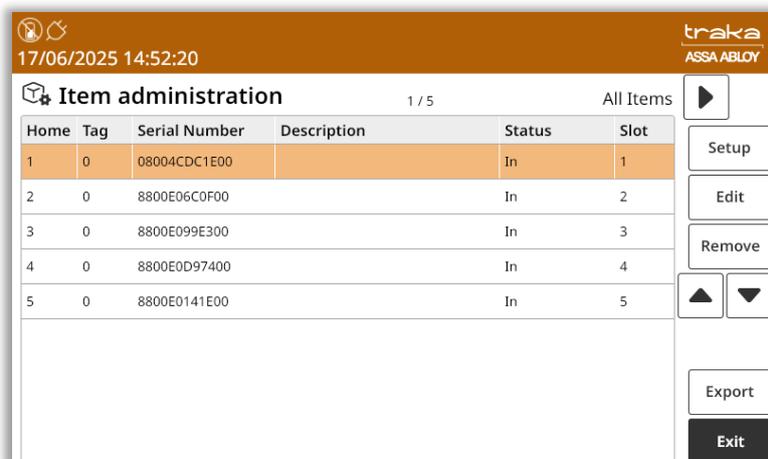
8.   At this point, you can choose to give each item a description. To do so, simply highlight the desired item and click the **Edit** button.
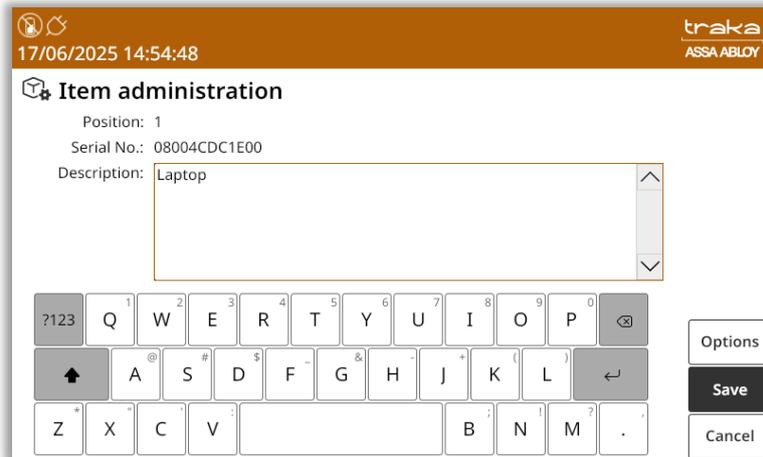
NOTE: **For further information on how to utilise the description feature see the 'Searching for Items' section.**

9.   At this point, you can also configure an item to require authorisation to be accessed and also choose to assign a curfew to the item. To do so, simply click the **Options** button.
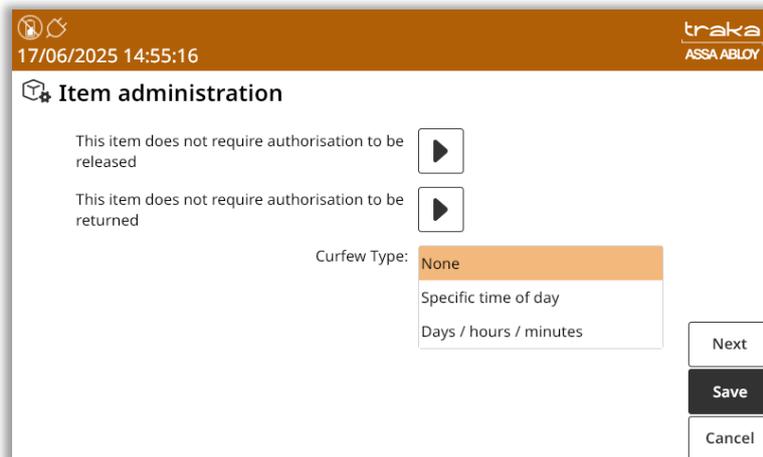
NOTE: **For further information on using authorisation, refer to the 'Item Authorisation' section. For further information on using curfews, refer to the 'Curfews' section.**

10. Click **Save** and you will return to the item list.

Internal

11. SYSTEM OPERATION

11.1 RETURNING AN ITEM

You **must** return the item to the correct compartment.

1. **Access** the system.
2. **Select** the door number you wish to open.
3. **Return** the item to the compartment and close the door.

4. When you return the item, the ⬤ button will change to 🟢 show the item has been returned.

NOTE: In a Non-RFID system there is no indication that the item has been removed or returned. The ⬤ button is displayed only whilst the door is open.

NOTE: With the "Allow any user to return items" configuration option enabled, the user with access to only 1 item, who logs in when their only item is out to another user, is now taken to the "I Know What I Want" screen where they can click on their empty locker compartment, and the empty locker compartment will open allowing them to return the item. The item must be returned to the correct compartment.

11.2 REMOVING AN ITEM

How you remove an item from the system will depend on how your system is currently configured i.e., which release method is selected. The latest Traka Touch application allows a locker compartment door to be opened in one of two methods, 'I Need To Search' or 'I Know What I Want'.

By default, each Traka Touch system is configured with the 'I Know What I Want' mode. For more information on the item release screen, please review the 'Item Release Screen' section. To change the item release preferences, please refer to the 'General Options' section.

1. Access the system and select 'I Know What I Want' (if applicable) and you will be presented with a screen similar to the following.
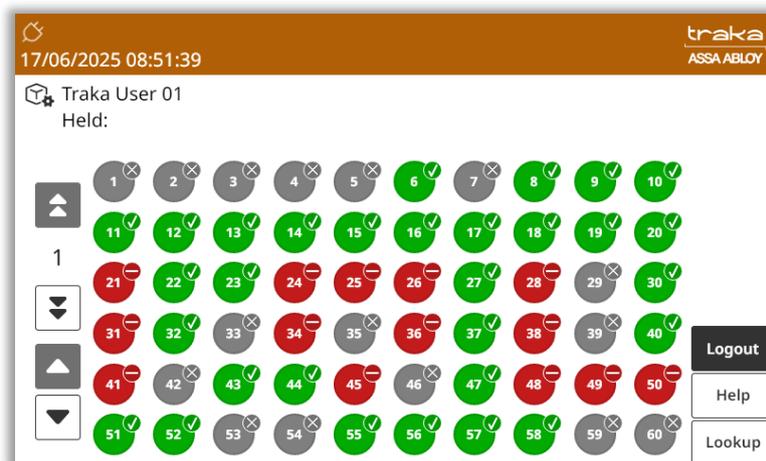
Listed below is every type of symbol that can be displayed for each position number.

NOTE: Some symbols are used only for RFID systems, and the meanings for some differ slightly for a Non-RFID system.

Internal

 - Green symbols with a tick show items that the user has access to.

 - Red symbols with a line indicate that the user does **NOT** have access to the item.

 - Red symbols with a cross indicate that an item is returned to the wrong position.

 - Red symbols with a question mark indicate that the item has become undetectable.

 - Grey symbols with a yellow tick show that you have removed the item from the system.

 - Grey symbols with a grey cross indicate that another user has the item out of the system.

 - Grey symbols mean no item is assigned to the slot.

 - Pressing the Help button will present you with a screen that has instructions on how to remove/return keys.

 - Pressing the Lookup button will allow you to select an item and view its description. Also, it will allow you to view the user who last used item, or who currently has the item out of the system.

 - Pressing the Logout button will return you back to the Login Screen.

2. **Press** the button on the touch screen of the item you wish to remove**.**
3. The compartment door will pop open.
4. **Remove** the item and close the door.
5. When you remove the item the button will change to to show the item has been removed.

NOTE: In a Non-RFID system the **button will change to** **when the door is open, not when the item has been removed.**

11.3   ITEM IN WRONG POSITION

NOTE: This section is only applicable to RFID systems.

When an item is returned to the incorrect compartment, the system will prompt you to remove the item and return it to the correct compartment. The red symbol with a 'cross' shows the incorrect compartment. The compartment it should be returned to is highlighted with a green symbol with a 'tick'.

Internal
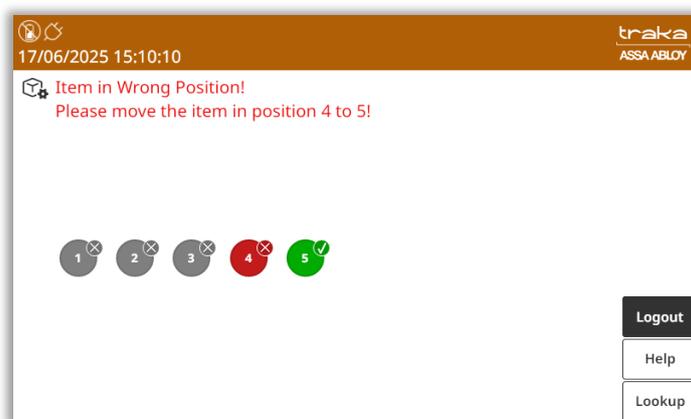
If the item is not returned to the correct compartment, the next time a user accesses the system, the position number with the incorrect item will display a red symbol with an exclamation mark.
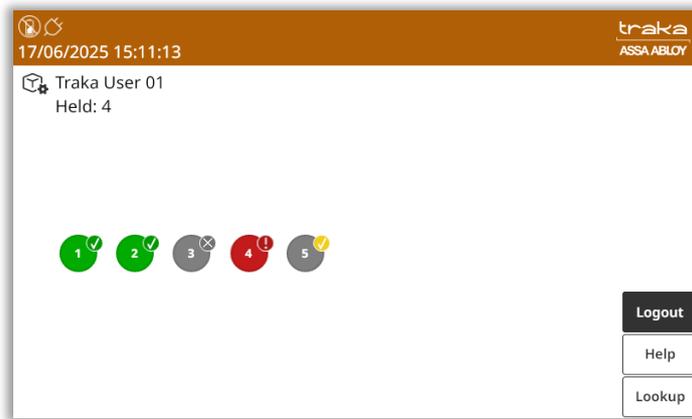
To return the item to the correct compartment, select either the incorrect position or the position the item should be returned to and both doors will open.

11.4   DELETING AN ITEM

As well as creating items, it is also possible to delete items. This operation must be performed by an Admin User.

1.   Log into the system as an admin user and select **I Know What I Want.**
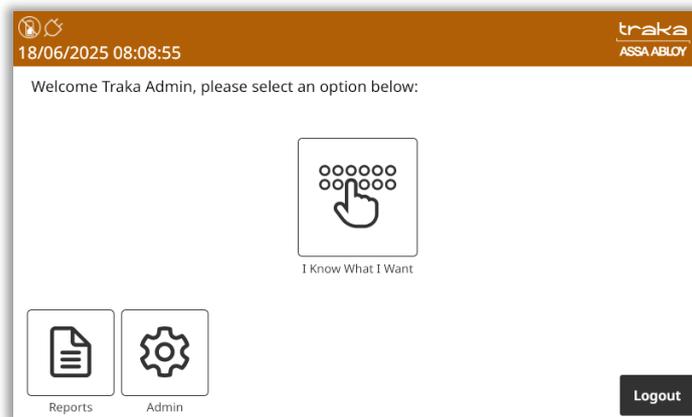
2.   Select an item and remove it from the locker.
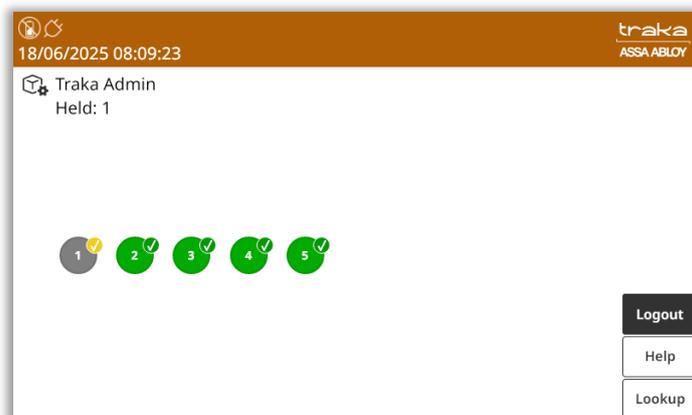
3.   Close the door and you will then be logged out.
4.   Log back into the system and navigate to the **Item Administration** screen.
5.   Select the position of the removed item and select the **Remove** button.
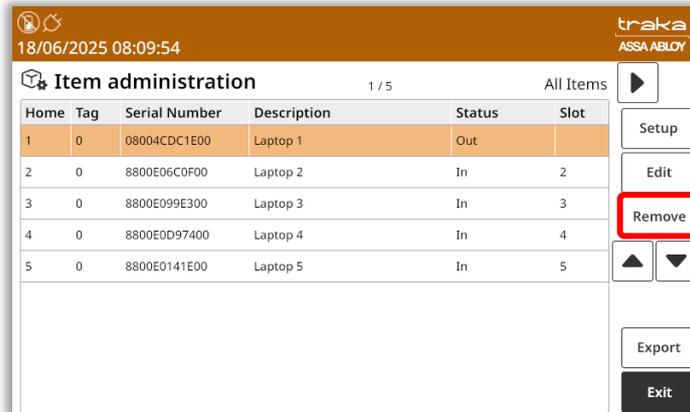
The system will request confirmation that you wish to remove the item record for that item.
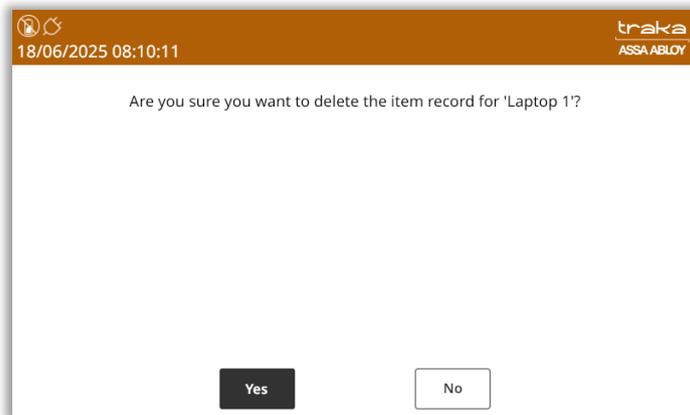
You will now return to the Item Administration screen and the item record for the selected item will no longer be shown.
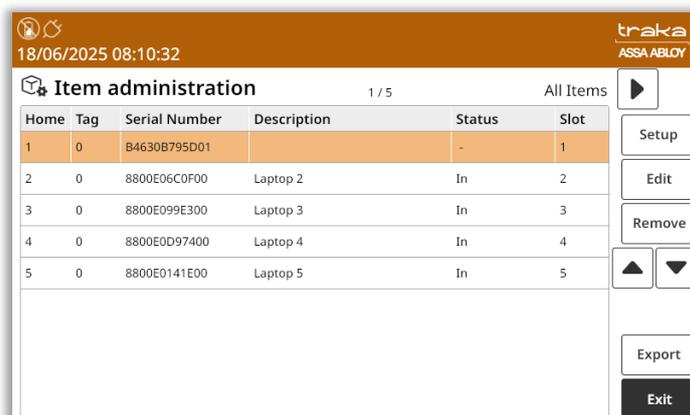
11.5 ADDING AN ITEM

In certain situations, you may wish to add a new item to the locker system. This operation can only be performed by an admin user.

1. As an admin user, log into the system and choose **I know What I Want.**
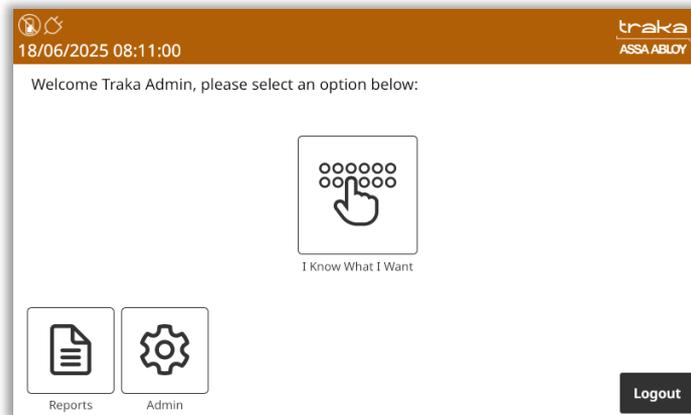
2. Select an empty locker compartment and insert a new Item. The item will shown as not recognised.

3. Now close the Door.
4. Log back into the system and navigate to the **Item Administration** screen.

The Status of the newly placed item will show as **Unrecognised.**

5. Select the item and then choose **Setup.**
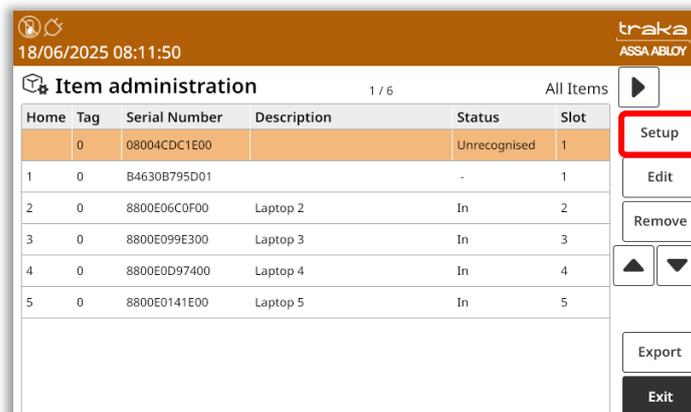
6. The system will ask if you want to setup all Items. Select **Yes.**
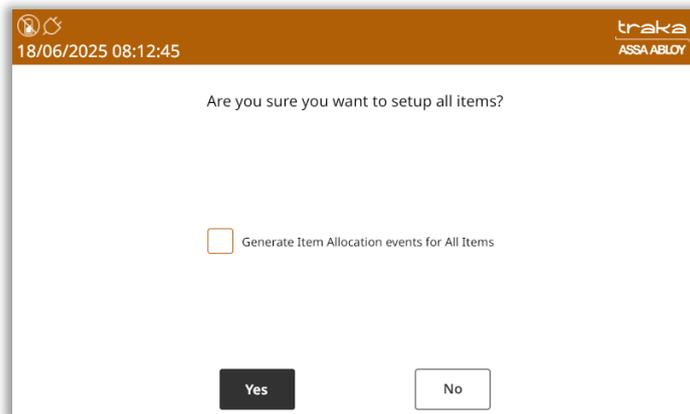
7. The system will now ask you if you wish to assign the item to the position that it was detected.
8. Select **Yes** to continue.
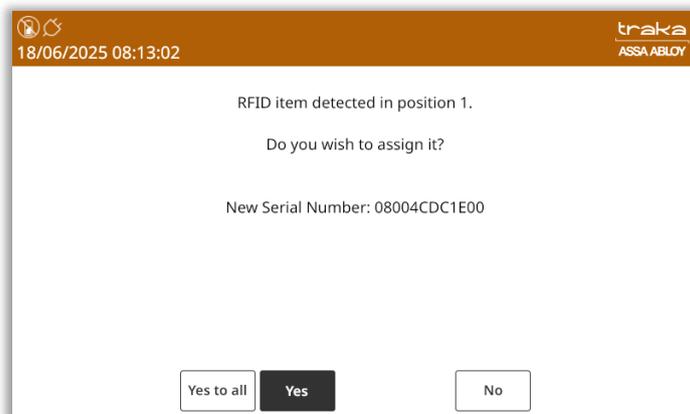
9. You will now return to the Item Administration screen and the new item's status will be displayed as **In.**

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal
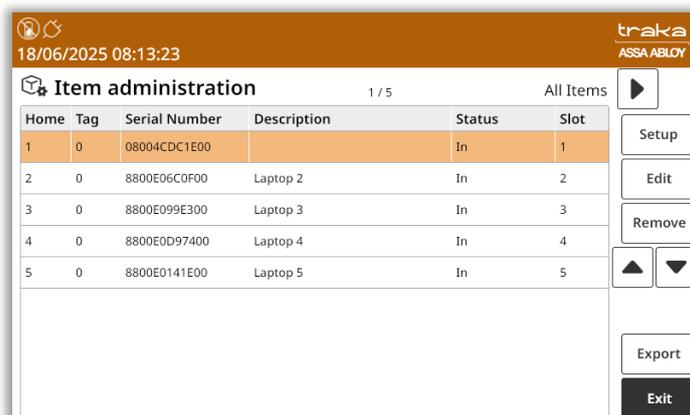
11.6   RELOCATING AN ITEM WITHIN THE SAME SYSTEM

If required, it is possible to assign a new home position for an item within the same system even if the designated position currently has an item associated with it. In this example, the item from position 2 is currently out of the system and the item from position 4 will be relocated to that position.

1.   As an admin user, log into the system and select **I Know What I Want**. After the door opens, select, and remove the item that you wish to relocate and then close the door.

2.   Log back into the system and select **I Know What I Want.** Once the door has opened, insert the item into a vacant position.

You will be presented with a message indicating that the item is in the wrong position.
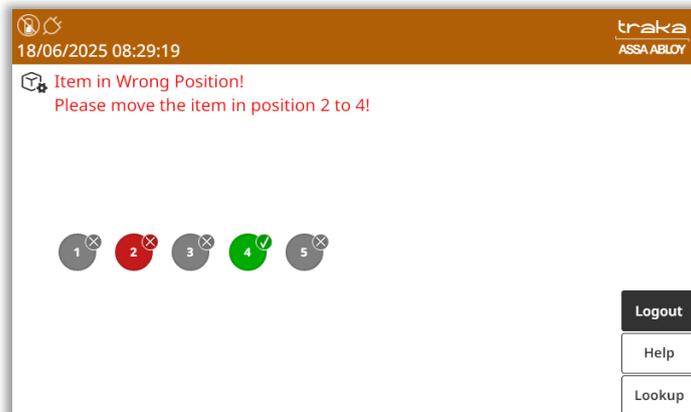
3.   Now close the door.

4. Log into the system and navigate to the **Item Administration** screen. You will see that the relocated item status is shown as **In Wrong Slot.**

5. Next, run the setup process.

6. At the next screen, select **Yes** to continue.

The next screen will inform you that there is already an item assigned to that position and if you choose to move another item into that position, the existing item will be deleted.

7. As it is the intention to relocate the item, select **Yes** to continue.

You will then be returned to the **Item Administration** screen. You will see that position 2 now holds the iFob record for the item that was previously in position 4.

NOTE: It is possible to reallocate the deleted item back into the system. The item's record will remain as shown below.

11.7   RELOCATING AN ITEM FROM ONE SYSTEM TO ANOTHER

If required, it is possible to assign a new home position for an item from a different system even if the designated position currently has an iFob associated with it. In this example, the item from position 2 of the designated system is currently out of the system and an item in position 3 from another system will be relocated to that position.

1.   As an admin user, log into the system and Select **I Know What I Want**. After the door opens, select, and remove the item that you wish to relocate and then close the door.
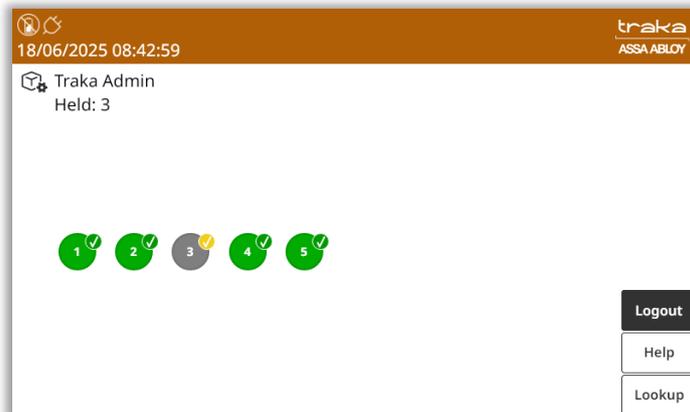
2. Log into the system that you wish to relocate the item to and select **I Know What I Want.** Select the compartment from the touch screen and once the door has opened insert the item into the vacant position. You will be presented with a message indicating that the item is not recognised.
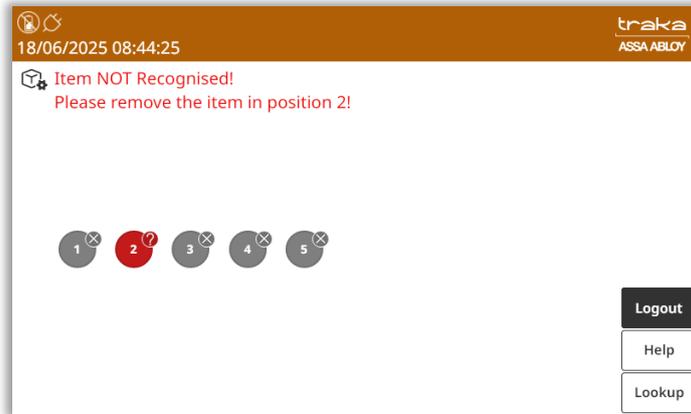

3. Now close the door.
4. Log back into the system and navigate to the **Item Administration** screen. You will see that the relocated item status for position 2 is shown as **Unrecognised.**
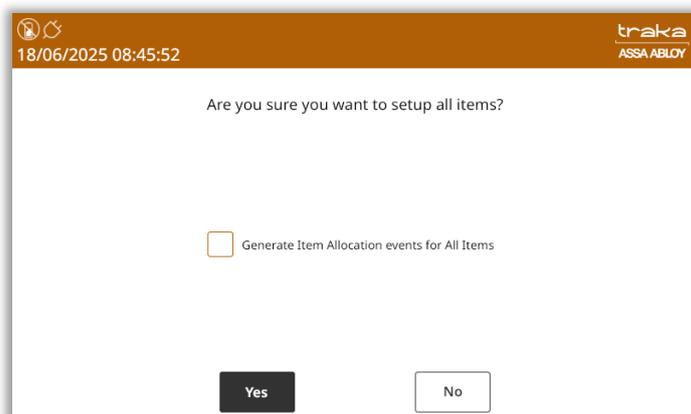
5. Next, run the setup process.

6. At the next screen, select **Yes** to continue.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

The next screen will inform you that there is already an item assigned to that position and if you choose to move another item into that position, the existing item will be deleted.

You will be given the option to **Setup** or **Replace.** If you choose **Setup**, a completely new item with no record will be setup which can be seen when you are returned to the **Item Administration** screen.
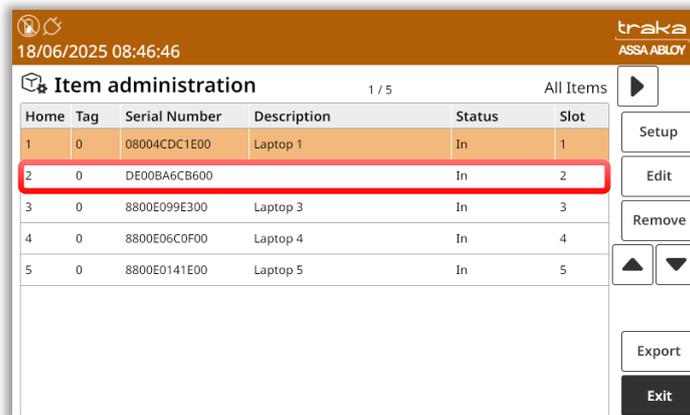
If you choose the **Replace** option. The new item will replace the existing item but use the existing item record.
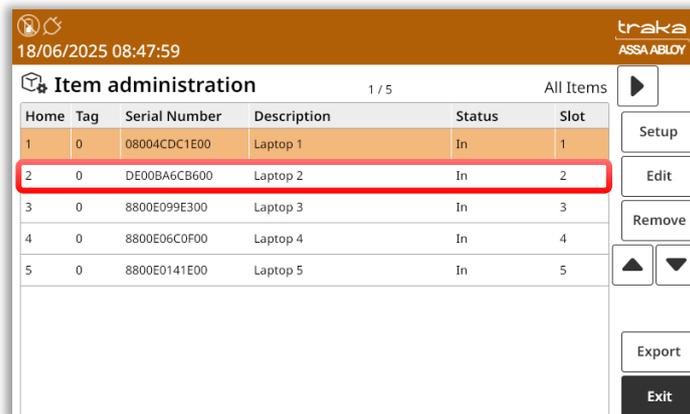
11.7.1 RELOCATING ITEMS WITHIN A COMMON ITEM ACCESS GROUP

The relocation of items from one system to another maybe performed on any system. However, if you wish to relocate items within a Common Item Access Group and maintain the group membership, the item must be a member of an Allowance Across Systems group. For non-Allowance Across Systems, if an item in an Advanced First in/First Out group is relocated, the item will be deallocated and removed from the group. For an item in a Fixed Return – Common Item Access Group, the relocated item will be assigned to the position in which it is placed. The setup process for relocated

Internal

items may be carried out as outlined in the previous section. For more information about Allowance Across Systems, please refer to **UD0260 – TrakaWEB Version 4 User Guide.**

11.7.2 RELOCATING ITEMS WITHIN AN ITEM ACCESS GROUP

If you wish to relocate an item associated with an Item Access Group from one system to another, the access level for the item will not be carried over to the other system and the access will not be removed from the Item Access Group. Therefore, if another item is setup in the position that the relocated item came from, it will inherit the previous access level of that item and anyone who had that item assigned via an Item Access Group or directly will inherit access to the new item. For more information about Item Access Groups, please refer to **UD0260 – TrakaWEB Version 4 User Guide.**

11.7.3 RELOCATING ITEMS WITH AN ASSOCIATED BOOKING

When an item associated to a booking is removed from the system to be relocated to another system, it will be deleted from the booking. The item may then be setup after relocation as outlined in the previous section. It is worth noting that if only one item was associated with the booking, then that booking will no longer be available once the item has been removed. For more information on Item Booking, please refer to **UD0260 – TrakaWEB Version 4 User Guide.**

11.7.4 RELOCATING PAIRED ITEMS

If an item that has been configured for Item Pairing is relocated to another system, it will no longer have the pairing functionality that was associated with it as Item Pairing cannot be performed across multiple systems. Once the item has been relocated to another system, it may then be setup as outlined in the previous section. For more information about Item Pairing, please refer to. **UD0260 – TrakaWEB Version 4 User Guide.**

11.7.5 RELOCATING ITEMS WITH AN ASSOCIATED ACCESS SCHEDULE

If you choose to relocate an item that has been associated with an Access Schedule to another system, then it will no longer be displayed in the list of items that have been setup with an Access Schedule. After the item has been relocated to another system, it maybe setup as outlined in the previous section. For more information about Access Schedules, please refer to. **UD0260 – TrakaWEB Version 4 User Guide.**

If necessary, the system clock setting may be changed from within the Administration menu.

1. From the Administration Menu, select the **Clock** icon.
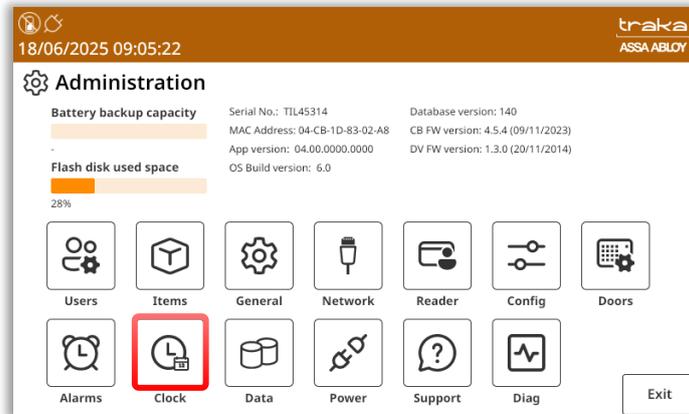
2. At the next screen, you will be able to edit the Date, Time, and Time Zone.
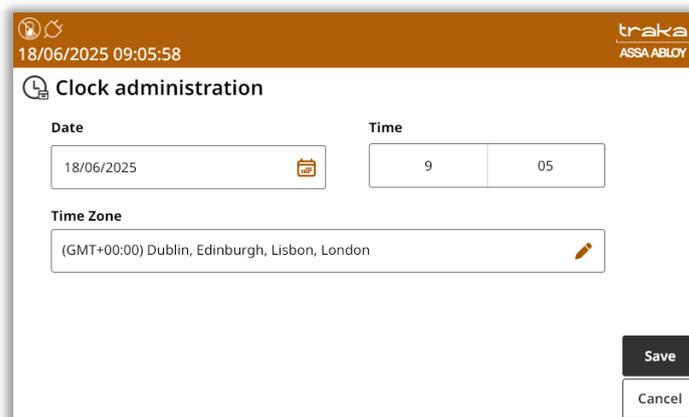
3. To change the date, click on the Date field. A calendar will appear, allowing you to select the new date as required. Scroll through the months by using the arrow keys highlighted in red on the image below. Alternatively, clicking on the Month/Year display will allow you to select a specific month or year without having to scroll to it.
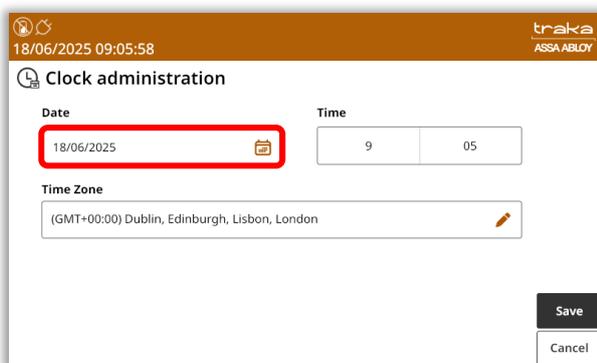
4. To change the time, click on the Time field. Simply scroll through, or use the arrow keys, to input the new time. Click on the accept button ✓ to input the changes or the cancel button ✗ to discard the selection.
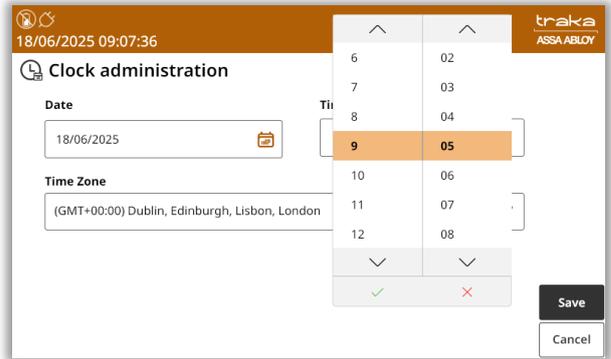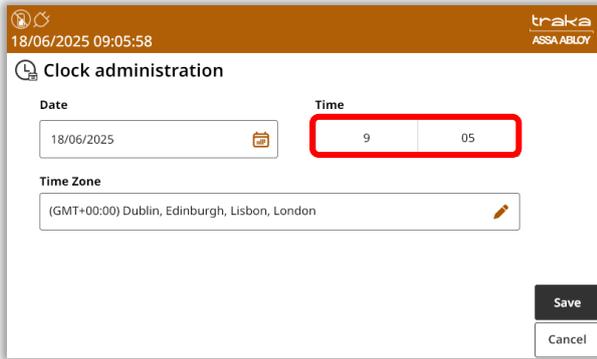
5. To change the time zone, click on the Time Zone field. A new window will appear displaying the available time zones. Simply scroll through the list or use the arrow keys and scroll bar to identify and select the required time zone. Once selected, click **OK** to return to the clock admin page.
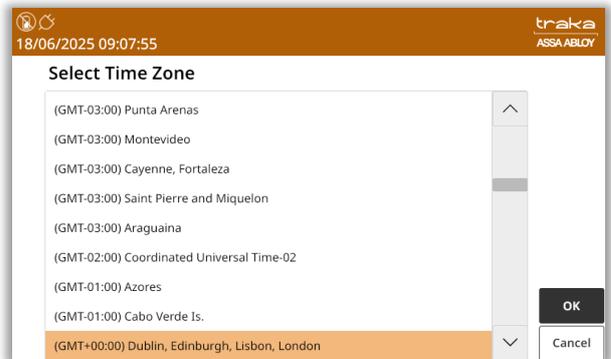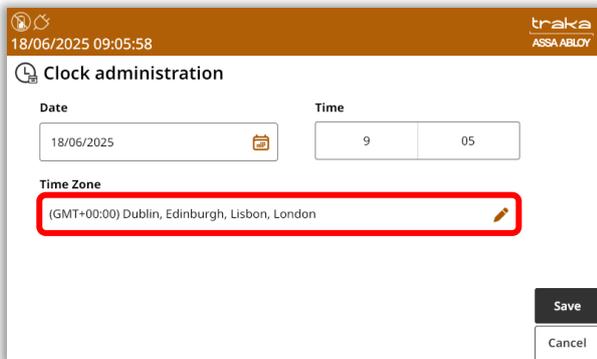
6. Once you have completed making your changes, click on **Save** to apply any changes and return to the Administration Menu.

Internal

Traka Touch systems allow you to run reports showing all activity and events that have occurred in a user definable period of time.

NOTE: Reports can only be accessed by a user with 'Reports' permissions. Please refer to the 'Users' section for further details.

13.1 GENERATING REPORTS

1. Access the system and click **Reports**.

2. A window will appear showing you three reports that can be run. The Event Report, Item Returned by a Different User Report and Active Alerts.
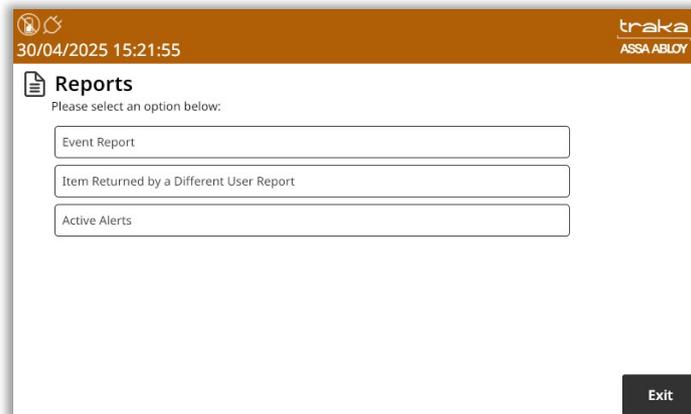
The Reports options will provide you with a number of set ways to filter the report as required. Alternatively, you can choose to set more specific dates.

Event Report

This report shows you all types of event activity.

Selecting the option will take you to another screen and enable you to filter the date range.

- The [Today] button will provide all the reports for today.
- The [Last 7] button will provide the events from the last seven days.
- The [Last 30] button will provide all the events from the past 30 days.

If you wish to set a more specific start date, selecting the button for the start date will present you with a function that will enable you to select and set the required start date.

Selecting the button for the end date will also present you with a function to select and set the required end date for the report.

3. Select one of the filtering options above and click the [Run] button.

4. The report list will now generate, using the filtering options you previously selected.

Item Returned by a Different User Report

This report will show you any items that were removed by one user then returned to the system by another.

Selecting the option will take you to another screen and enable you to filter the date range.

- The [Today] button will provide all the reports for today.

- The [Last 7] button will provide the events from the last seven days.

- The [Last 30] button will provide all the events from the past 30 days.

If you wish to set a more specific start date, selecting the button for the start date will present you with a function that will enable you to select and set the required start date.

Selecting the button for the end date will also present you with a function that will enable you to select and set the required end date.
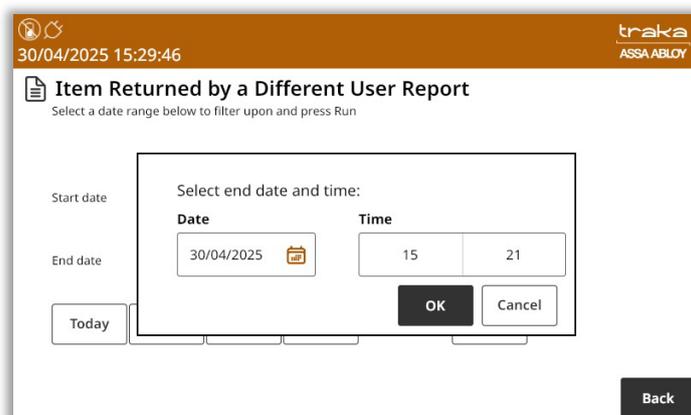
5. Select one of the filtering options above and click the [Run] button.

6. The report list will now generate, using the filtering options you previously selected.

Internal

Active Alerts

This report will show any of the following 'Alerts' that have appeared:

- Item in but not on charge
- Item in with charge fault
- Unidentified item on charge
- Unidentified item charged
- Unidentified charged fault
- USB charger undetectable
- Door left open

13.2 EXPORTING REPORTS

It is possible to export Event Reports and Illegal Handover Reports to a USB Memory Stick.

NOTE: **For further information on USB memory stick specification, please refer to the USB Memory Sticks section.**

NOTE: **Depending on the configuration of your Traka Touch Lockers the USB port may be located inside a locker compartment. In this case the door will open automatically through this process giving you access to the USB port.**

NOTE: **If your system does not have a USB port located inside a locker compartment, you will need to gain access to the inside of the Traka Touch Pod by opening the control panel. See the 'Opening the Control Panel' section for more information.**

1. To export the reports to a USB memory stick, click the ⌈Export⌋ button.

2. The door will open (if applicable) and ask that you insert a USB memory stick.
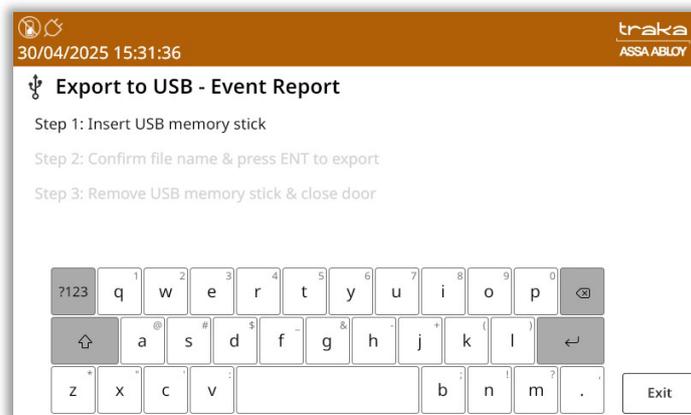
3. Enter the desired file name for the report and press ⌈↵⌋ (enter).
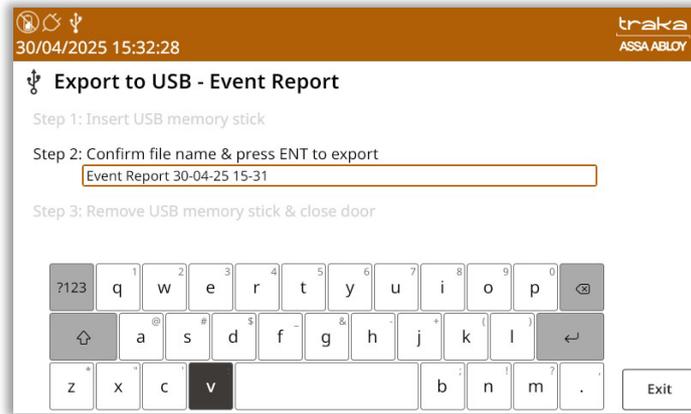
4. The report will now begin to export to the USB device.
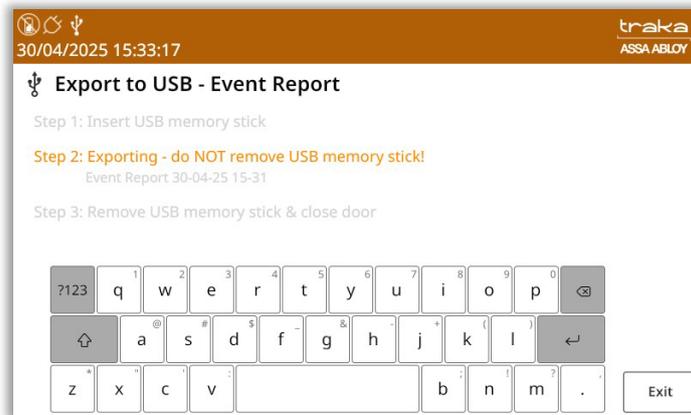
5. When the report has finished exporting, remove the memory stick and close the door (if applicable).

6. You will be taken back to the event report screen. Click the [Exit] button to be taken back to the login screen.

Internal

14.1   ITEM RELEASE SCREEN

The latest Traka Touch application can display a selection screen that appears when a valid user logs into the system. This selection screen can have one or both of the following buttons depending on what is selected in the 'General Options'.

NOTE: If a user has admin or report permissions, these buttons will also appear on the selection screen.
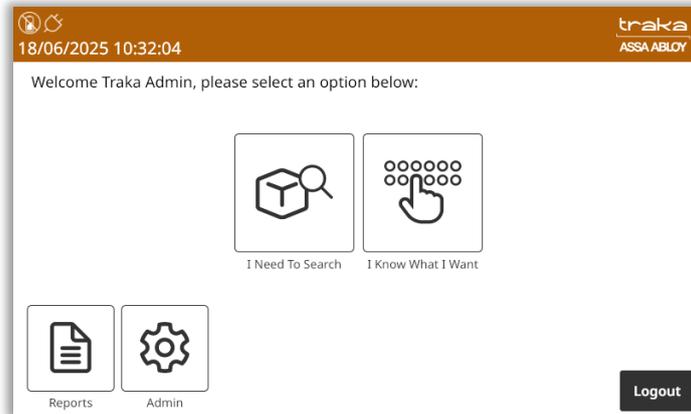
These two options allow the user to remove items from the system in different ways...

- **'I Need to Search' –** Will allow you to search for specific items in the system via their individual description. See the 'I Need To Search' section for more details.
- **'I Know What I Want'** – Will allow you to select which items you wish to remove via the on-screen display showing all the items currently in the system. See the 'I Know What I Want' section for more details.

NOTE: 'I Know What I Want' is the default release method for Traka Touch systems. To make changes to this please review the 'General Options' section.

14.1.1   'I NEED TO SEARCH'

Selecting the **I Need To Search** button will present you with the following screen...
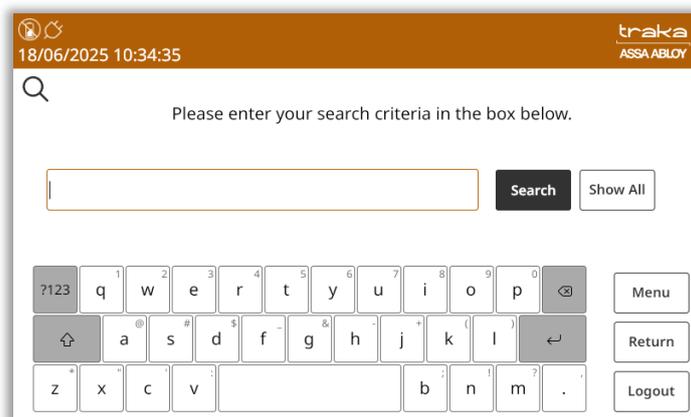
Enter a description into the provided field. Clicking 'Search' will quickly retrieve results that include the terms that were entered into the search field. If you leave the field blank and click the 'Show All' button it will list all of the items currently in the system.

NOTE: The search results will only include items that the user has access to.

For example, typing '**BA**' into the search field will retrieve any item description with 'ba' in the title. As shown below...

- **Ba**rcode Scanner
- Spare **Ba**ttery
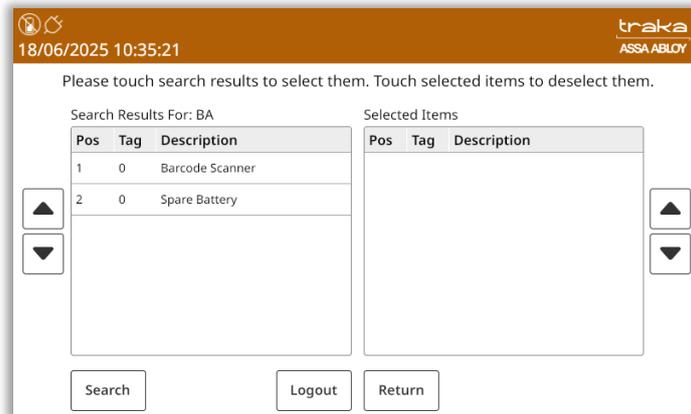
Selecting an item from the left hand column (results), will automatically move it into the right hand column (selected items).
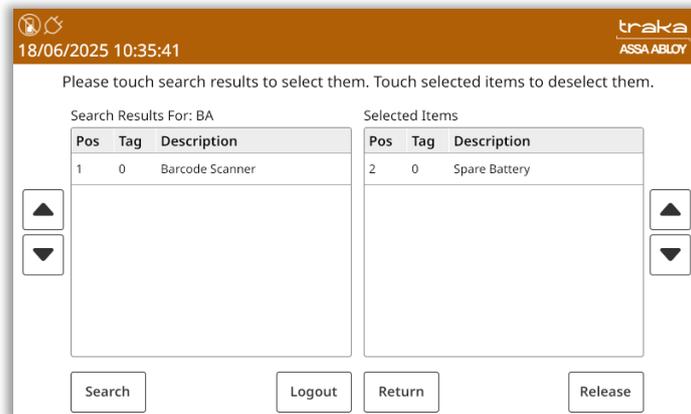
Once you have selected all the items you wish to remove, click the **Release** button. The compartment door(s) will then open, and you can remove the item(s).

14.1.2 'I KNOW WHAT I WANT'

Selecting 'I Know What I Want' from the Item Release Screen will take you to the Item Selection Screen where you can see a visual representation of every item in the system.

Here you simply select which items you would like, and the system will open the doors, providing you have the correct permissions.

NOTE: This is the standard release method for Traka Touch systems. To make changes to this, please review the General Options section.

14.2   NEW PIN

It is possible to allocate a user with a secondary level of access i.e., a PIN (personal identification number). If a PIN is allocated, after the user has entered their Keypad ID, swiped their card or scanned their fingerprint, they will be asked to enter their PIN. If no PIN is allocated, the user will be logged into the system as normal.

You can assign a user a PIN or even change a user's current PIN from the main Login Screen. You can also add a PIN to a user's profile when you first add them to the system. Please refer to the 'Users' section for more details.

NOTE: If the system option 'Force User Details to Require PIN' is enabled and a user doesn't have a PIN then they will be forced to create a PIN when they next log into the system. To enable the option 'Force User Details to Require PIN' please review the 'Reader Administration' section.
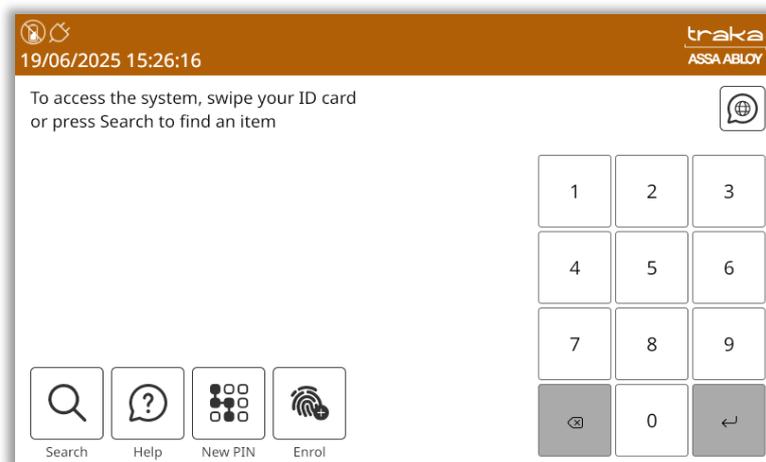
Adding a PIN

1. From the main login screen select **New PIN.**
2. You will then be asked to identify yourself at the cabinet via your Keypad ID, ID card or fingerprint.
3. Once you have identified yourself you will be asked to create a PIN of your choosing.
4. You will then need to re-enter the PIN for verifcation.

NOTE: There is a minimum PIN length required. By default, Traka Touch is set up with a minimum of 4 digits. This is user definable and can be changed in the 'Reader Administration' settings.

Editing a PIN

1. From the main login screen select **New PIN.**
2. You will then be asked to identify yourself at the cabinet via your Keypad ID, ID card or fingerprint.
3. Once you have identified yourself you will be asked to enter your current PIN.
4. You will then be prompted to enter your new PIN.
5. You will then need to re-enter the new PIN for verifcation.

NOTE: If a user has forgotten their PIN, an admin user will be required to login and access the admin menu and change the User's PIN from the User Administration page. See the 'Users' section for more details.

14.3   SEARCH REPORT

NOTE: Search Reports are not available if you are using RRMS.

By default, the **Search Report** option resides in the Reports section.
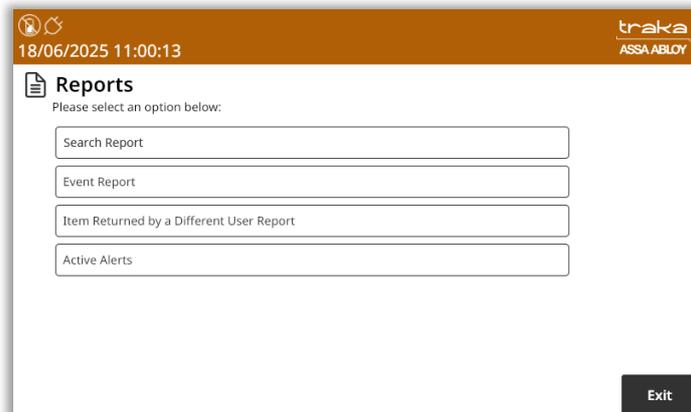
It can however be relocated by a user with Admin access to the Login screen. This section will explain how to accomplish this.

1. Access the system with a User ID, Card, or fingerprint.

Internal
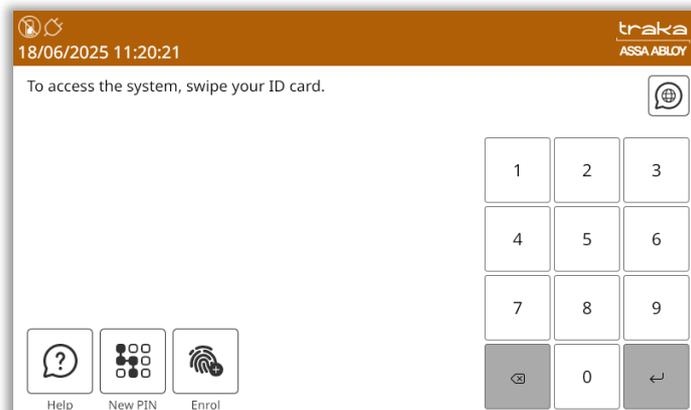
2. Click on **Admin** and then from the Administration screen, click on **General**.
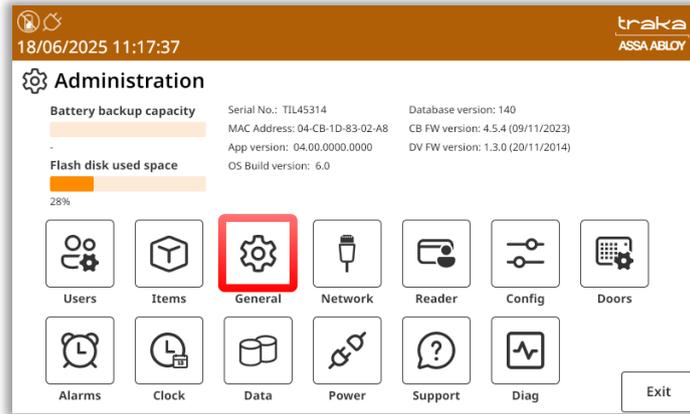
The General Options screen will display the current settings for the **Search Report**. The image below shows the default settings.
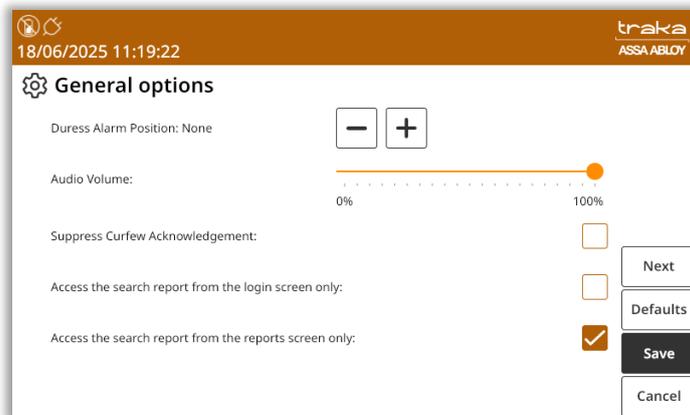
3. Click on the ☐ symbol. It will change to a ☑ symbol as shown below.
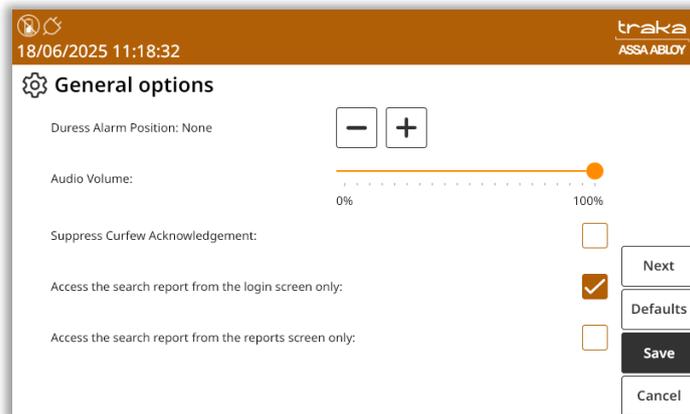
4. Click **Save** and then exit back to the Login screen.

Internal

From the Login screen, you will now be able to access the Search Report.
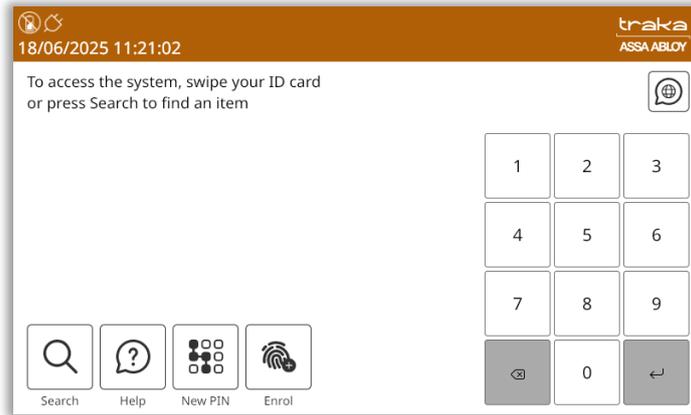
14.4   ITEM AUTHORISATION

In addition to the standard release of items, authorisation can be configured to force either 1, 2 or 3 people to authorise the access of specific items.

When using authorisation, there are generally two types of Users, Authorisers (for example security guards) and Standard Users (for example employees). Each item can be configured individually with no authorisation, 1 authorisation, 2 authorisations or 3 authorisations.

NOTE: To configure a User to be an Authoriser please refer to the 'Users' section.

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

14.4.1 SETTING UP THE ITEMS

NOTE: This action can only be performed by an Admin user. Please refer to the 'Users' section for further details.

1. Access the system.

2. Select the **Admin** Menu.

3. Select **Items**.

4. The current item list will then be displayed. Highlight the desired item and select the **Edit** button.

5. When the item details window appears, select the **Options** button.

6. From the top of the page, you can select the number of authorisers that are required to remove this item by using the directional arrow key.
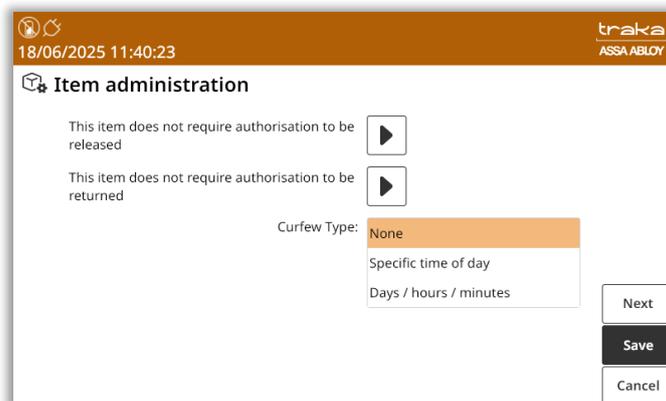
7. When you have made your selection click the **Save** button to go back to the item list. From there click **Exit** to go back to the admin menu and **Exit** again to go back to the main login screen.

14.4.2 USER PROCESS

1. A user without authorisation access logs into the system and attempts to remove an item that has 1 or more authorisers.

The following window will pop up and inform the user that 1, 2 or 3 authorisers are now required to identify themselves to the system before the item can be removed.
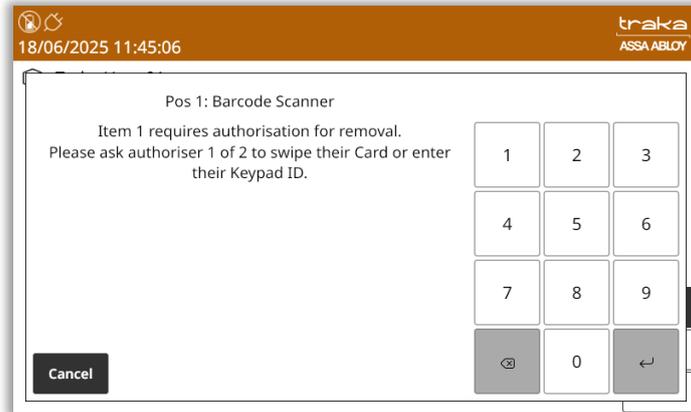
2. Authoriser 1 identifies themselves. The system will welcome the user and show that access has been granted.

3. If the item requires more than one authoriser, then a second and third (if applicable) must now identify themselves to the system.

Internal
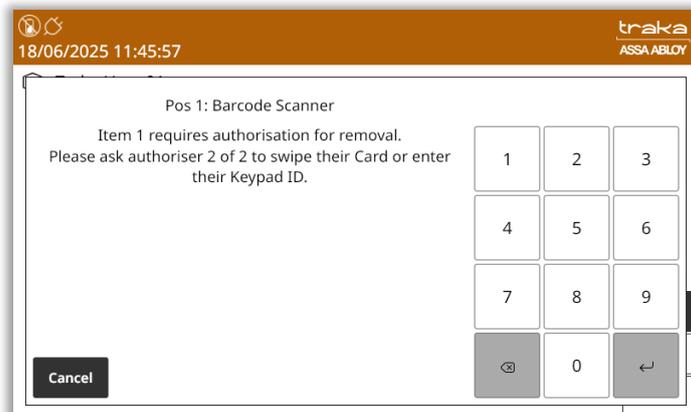
4. Once all authorisers have been verified the item will be released from the system.
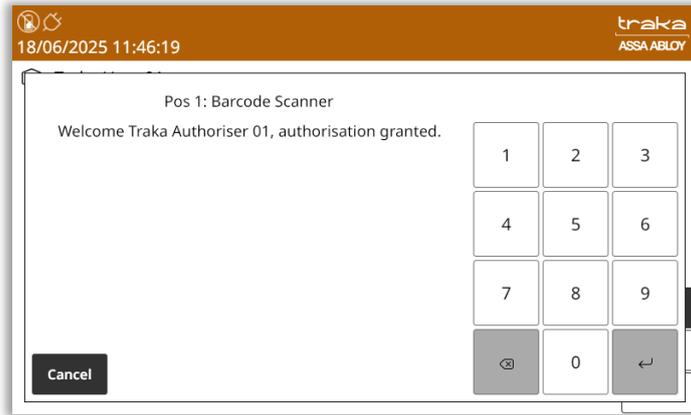
NOTE: If an Authoriser requests to take an item that has been configured with 1 or more authorisers, provided they have the appropriate permissions they can simply take the item without the need for authorisation.

14.4.3 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 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.

For more information on configuring the Authoriser from a Different Group option, please refer to **UD0018 – TrakaWEB User Guide** or **UD0260 TrakaWEB Version 4 User Guide.**

11.4.3.1 USER PROCESS - REMOVAL

The following example assumes that the User without the authoriser role is in a separate User Group from the Users that do have the authoriser role. The Item that the User is requesting requires two Authorisers. In turn, these must be in separate groups.

1. The user without authorisation logs into the system to remove an Item.

NOTE: If the user is not assigned to a User Group, they will be unable to access any items that require authorisation from authorisers in different groups. They will then see the following screen in Traka Touch:

Once successfully logged in, the following screen will appear requesting that authoriser 1 of 2 access the system.
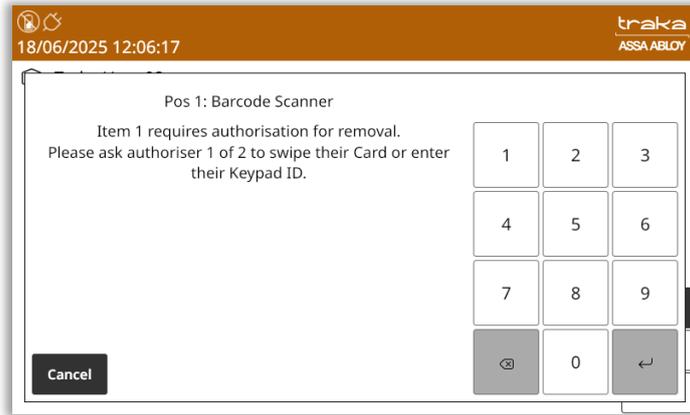
Once the authoriser has successfully logged into the system, the following message will appear:
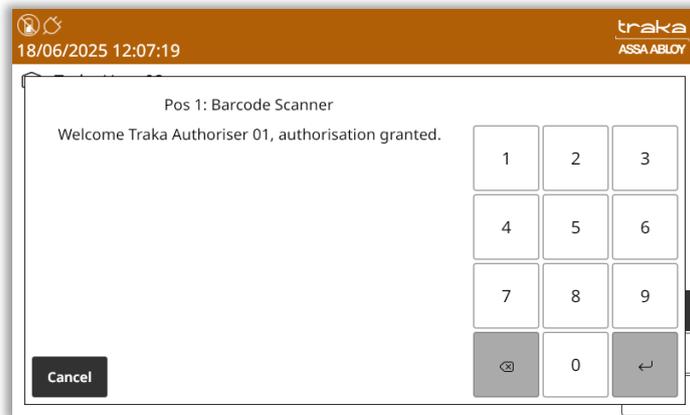
This will be followed by another message requesting that the second authoriser access the system.

Internal
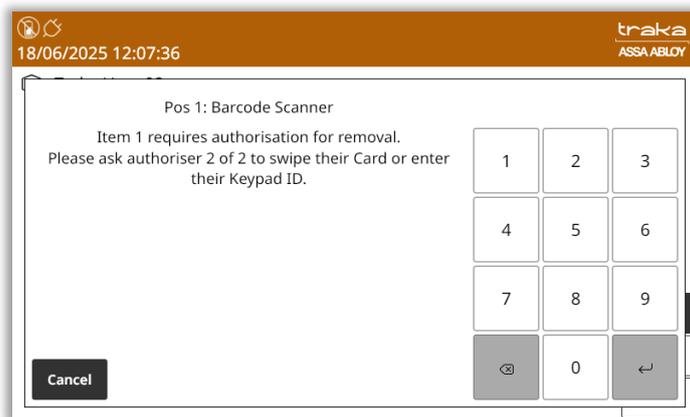
As previously mentioned, authorisers must belong to different User Groups. If an authoriser from the same group attempts to access the system, the following message will appear:
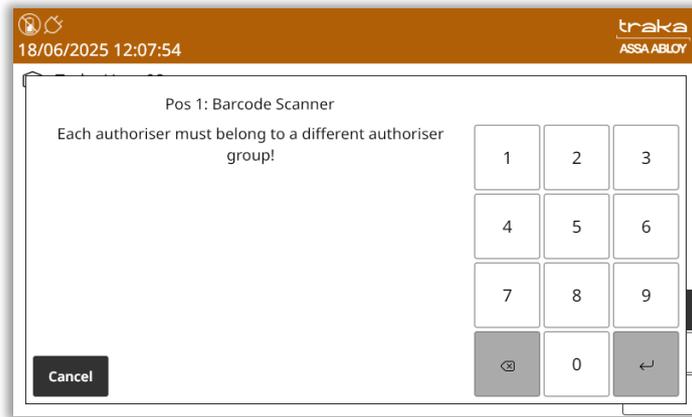
It is also important that each authoriser is different. The person attempting to remove the Item cannot authorise them self.
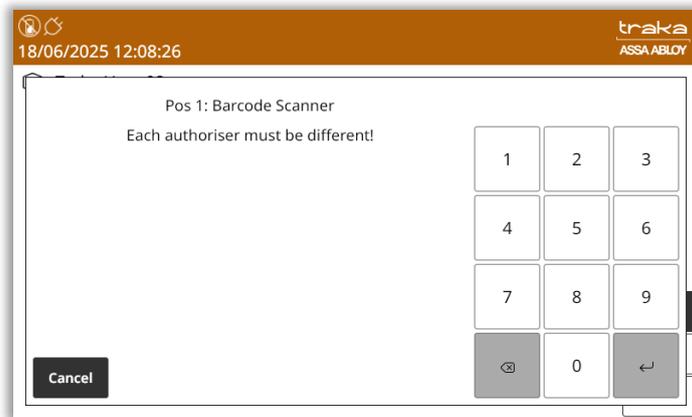
Once an authoriser from a different User Group accesses the system, the following message will appear:
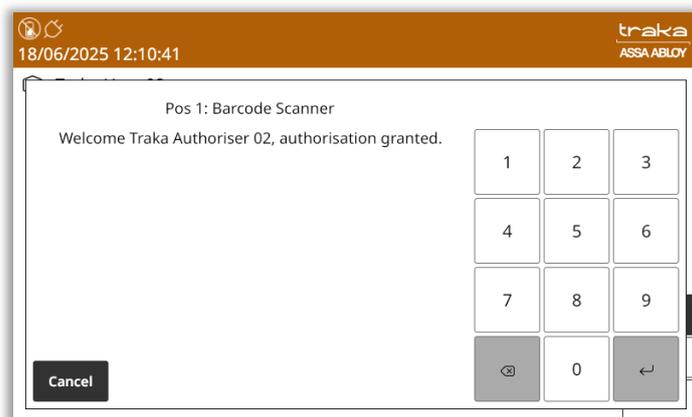
The Item will then be released to the User.

Internal

11.4.3.2 USER PROCESS – RETURN

This example assumes that the User without the authoriser role is in a separate User Group from the Users that do have the authoriser role. The Item that the User is returning requires two Authorisers. In turn, these must be in separate groups.

1. The user without authorisation logs into the system to return an Item and is presented with the following screen.
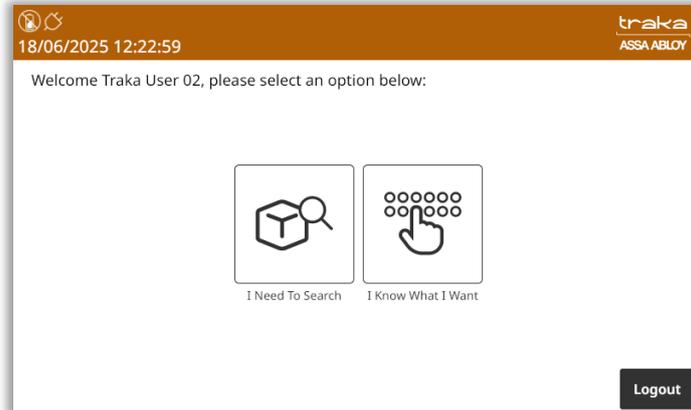
2. After selecting **I Know What I Want**, the User can select the item they wish to return. The door will open, and the user may return the item.

At this stage, a message will be displayed requesting that an authoriser must enter their ID at the touch screen.
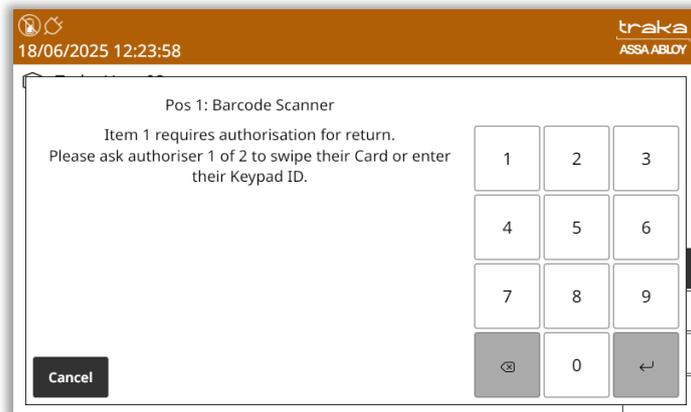
In this example, 2 authorisers are required.
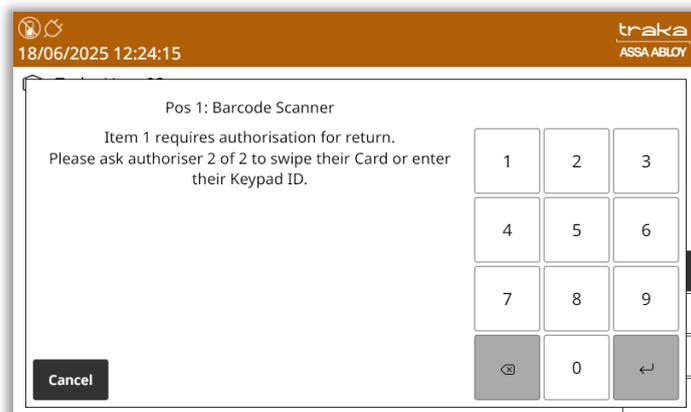
Upon successful completion, the door may be closed.
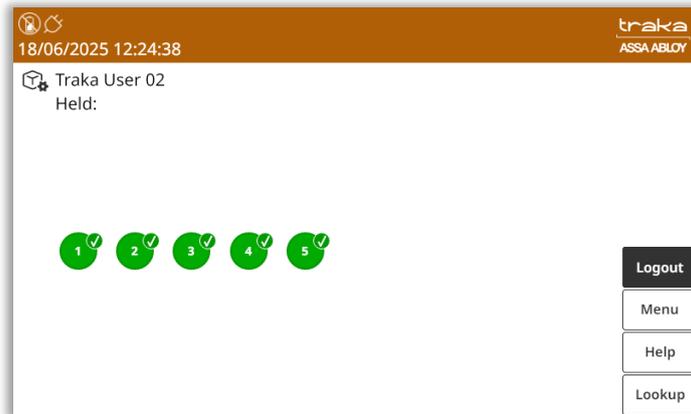
14.5 EXPORTING & IMPORTING

It is possible to export and import information such as users, items and permissions from/to the system via a USB memory stick from the Traka Touch application. The import feature is useful if you wish to add large lists of users in one go.

To use the import feature, you would first need to enter all of the required user details into the Traka Spreadsheet. To obtain the Traka Spreadsheet you will need to export your current user list to the USB memory stick.

NOTE: If your current user list is empty the spreadsheet will still be exported to your USB memory stick.

NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

14.5.1 EXPORTING USERS

NOTE: This action can only be performed by an Admin user. Please refer to the 'Users' section for further details.

1. Identify yourself to the system.

2. Click **Admin.**

3. Click **Users**.
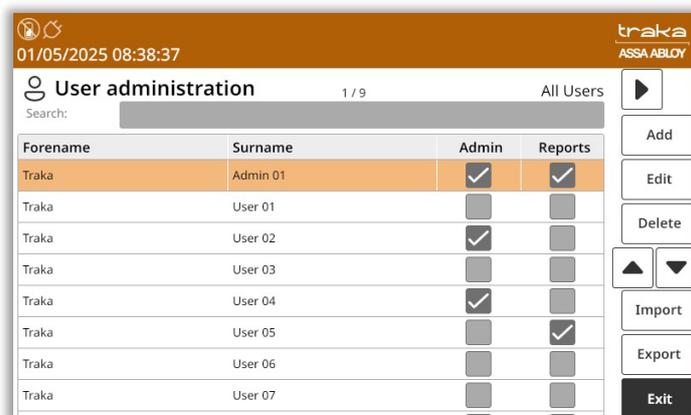
4. Select the **Export** button.

5. A compartment door will open (if applicable) and prompt you to insert a USB memory stick into the vacant socket.

NOTE: For further information on USB memory stick specification, please refer to the USB Memory Sticks section.

NOTE: Depending on the configuration of your Traka Touch Lockers the USB port may be located inside a locker compartment. In this case the door will open automatically through this process giving you access to the USB port.

If your system does not have a USB port located inside a locker compartment, you will need to gain access to the inside of the Traka Touch Pod by opening the control panel. See the 'Opening the Control Panel' section for more information.

6. Type a file name and press the (enter) button to start the export.

7. The system will then begin exporting.
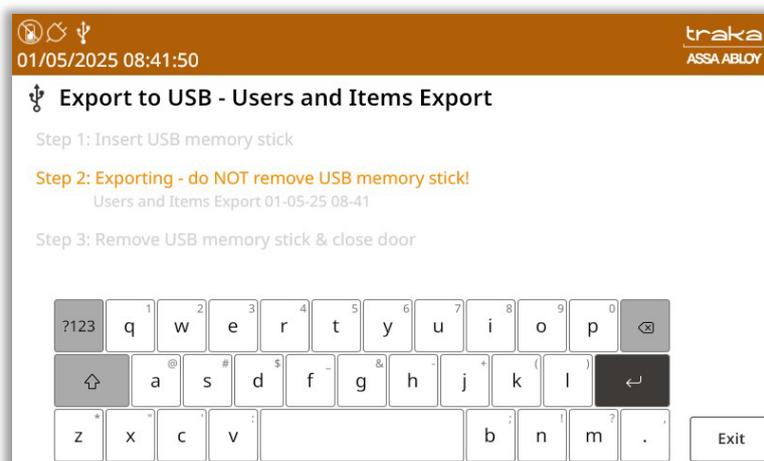
8. Once the system has finished exporting, you will be prompted to remove the USB stick.

9. The Traka Touch system exports an Excel Spreadsheet that will open on any PC with a valid Microsoft Office/Excel software licence.

14.5.2 IMPORTING USERS

To use the import feature, you would first have to have edited a Spreadsheet of users. To obtain the Spreadsheet you need to export your current user list (even if the list is empty) from the Traka Touch system. Please follow the 'Exporting Users' section above for more details.

13.5.2.1 ENTERING DETAILS INTO THE SPREADSHEET

This Spreadsheet covers user details, item descriptions and permission details. You don't need to fill in all of the information; it's there to be filled in if required.

1. Export the Spreadsheet as explained in the 'Exporting Users' section.

2. Open the Spreadsheet on a PC.

3. You can enter all the users' details here as well as the item details.

User & Security Details

Enter all the relevant information as you usually would. For the admin column simply put a capital 'Y' if the user is to have admin permissions, leave it blank if you wish them to remain a standard user.

Active Date	Expiry Date	Allowance	Admin	Reports	System Admin	User Admin	Items Admin	Authoriser
30 April 2025 10:57:37	30 April 2075 10:57:37		Y	Y	Y	Y	Y	Y
30 April 2025 11:06:00	30 April 2075 11:06:00							Y
30 April 2025 11:06:27	30 April 2075 11:06:27				Y			
30 April 2025 11:07:15	30 April 2075 11:07:15							
30 April 2025 11:09:21	30 April 2075 11:09:21						Y	
30 April 2025 11:23:46	30 April 2075 11:23:46			Y				
01 May 2025 08:37:31	01 May 2075 08:37:31							
01 May 2025 08:37:48	01 May 2075 08:37:48							
01 May 2025 08:38:15	01 May 2075 08:38:15							

Item Permissions

To grant a user access to an item simply put a 'Y' in the corresponding column. You can also assign a description to an item by double clicking above the desired position and entering a description of your choice.

4. When finished save the Spreadsheet onto a USB memory stick ready for importing to the Traka Touch system.

13.5.2.2 FAQ'S

Overwriting Users – When you enter a user's details into the Spreadsheet and that user already exists in the system, the user credentials from the Spreadsheet will be taken as the most recent edits and will overwrite the systems information.

Duplicate Keypad ID's – If a user being imported has the same Keypad ID as a user that already exists in the system, the import will fail. The user that already exists in the system will be kept and the attempted import user will be rejected.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal
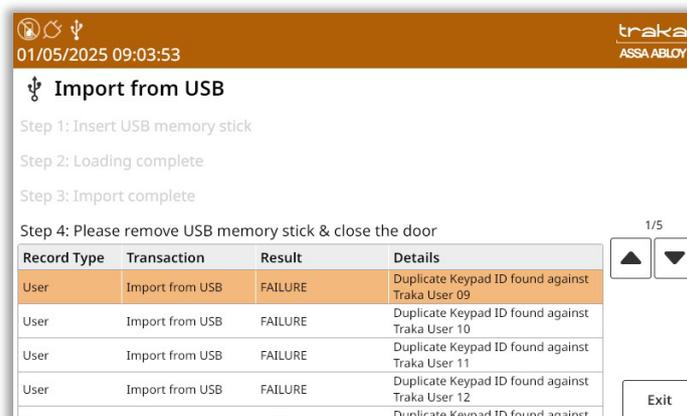
13.5.2.3 IMPORTING THE INFORMATION INTO THE SYSTEM

NOTE: **This action can only be performed by an Admin user. Please refer to the 'Users' section for further details.**

1. Identify yourself to the system.

2. Click **Admin.**

3. Click **Users**.

4. Select the **Import** Button

5. A compartment door will open (if applicable) and prompt you to insert a USB memory stick into a vacant socket.

NOTE: **For further information on USB memory stick specification, please refer to the <u>USB Memory Sticks</u> section.**

NOTE: **Depending on the configuration of your Traka Touch Lockers the USB port may be located inside a locker compartment. In this case the door will open automatically through this process giving you access to the USB port.**

If your system does not have a USB port located inside a locker compartment, you will need to gain access to the inside of the Traka Touch Pod by opening the control panel. See the 'Opening the Control Panel' section for more information.

Internal

6. Select the correct file from the USB memory stick.

7. You will then be asked if you would like to import the user list. Click **Yes**.
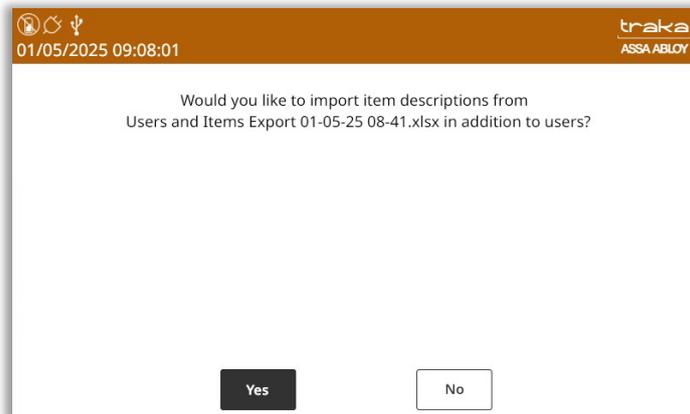
8. The system will then begin to load and import the list.

Internal

9. Once complete the table will show that the import was a success. You can now remove the USB memory stick.
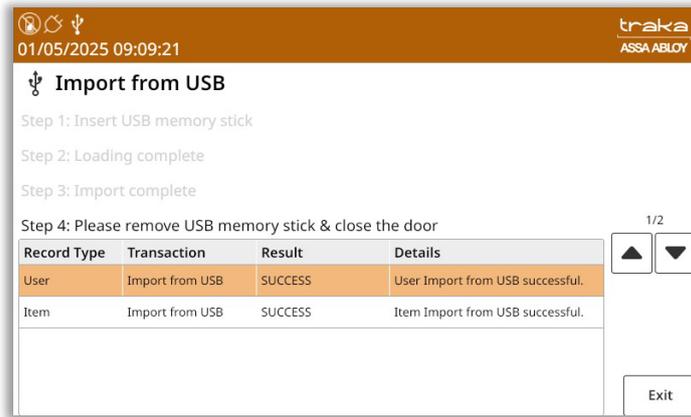
NOTE: Should an error occur during this process, please contact Traka Support using the technical support page at the back of this document.

14.6   GENERAL OPTIONS

Accessing the General Options must be carried out by an administrator. Please refer to the 'Users' section for further details.

1. Access the system and click the **Admin** button**.**

2. Click the **General** button**.** You will then be presented with the following screen.
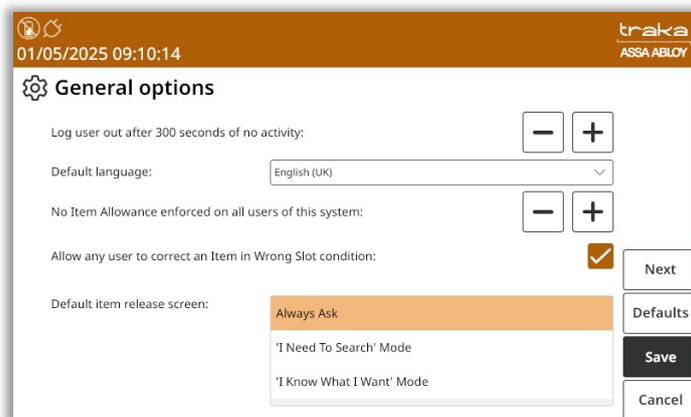
User Log Out Time

Here you can define the amount of time it takes for the system to log a user out after no activity. Using the directional arrows, you are able to configure the desired time in increments of 1 second. Traka recommends that you have this set to 20 seconds. This lowers the risk of a user walking away from the system before it has timed out allowing another user to use the system logged in as the previous user.

Default System Language

Using the directional arrows, you can navigate to the desired language and by selecting the flag icon enable a new system default language. When a user logs out of the system the system will revert back to the system default language in 5 seconds. It is also possible to set the language on a per user basis. Please refer to the 'Language' section for further details.

Internal

Item Allowance

The item Allowance can restrict how many items a user is allowed to have out of the system any one time. Using the directional arrows, you can configure how many items every user is allowed in increments of 1 item. Up to 10 items may be selected.

NOTE: The item Allowance here applies to all users using the system and can be set on a per user basis.

Allow Any User to Correct an Item in Wrong Slot Condition

When a user returns an item to an incorrect compartment in the system, the Traka Touch System will inform that user that the item belongs in another compartment. If the user ignores this message and closes the door, the next time a user accesses the system an icon will highlight the item in the wrong compartment. For more details on the various icons shown on the item selection screen please refer to the 'Removing/Returning Items' section.

If the 'Allow Any User to Correct an Item in Wrong Slot Condition' is ticked, any user can select the item in the wrong compartment and the system will release the door regardless of that user's access and permissions. Both doors will open allowing the user to return the item to the correct compartment.

If this option is **not** ticked, a user must have access to the incorrectly returned item or be an administrator to be able to return it to the correct compartment.

If you wish all users to be allowed to move incorrectly located items from the wrong compartment to the right compartment, leave this option ticked. Otherwise, un-tick this option to turn this feature off.

Default Item Release Screen

The latest Traka Touch application can display a selection screen that appears when a valid user logs into the system. This selection screen can have one or both of the following buttons depending on what is selected in the 'General options'.

I Know What I Want   I Need To Search
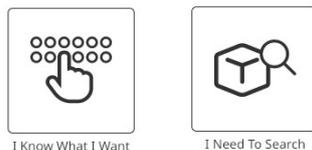
The default release options that are selectable in the general options are as follows...

- **Always Ask** – With this option enabled, the selection screen will display both options below.
- **'I Need to Search' mode** – Will allow users to search for specific items in the system via their individual description once they have entered their ID number. Whether the user chooses to manually 'Search' for an item or use the 'Show All' function, they will now only be able to view items that they have access to, regardless of the current state of any items within the system.
- **'I Know What I Want' mode** – With this option enabled, the selection screen will only display the 'I Know What I Want' button.

3. Click the **Next** button to move to the next page.
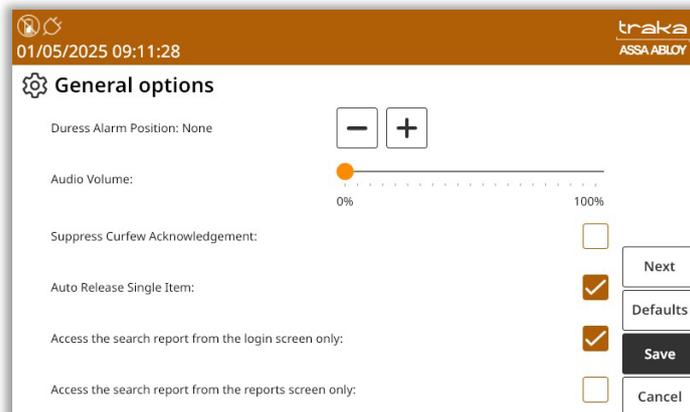
Duress Alarm Position

Selecting a position here will assign a duress alarm to the corresponding position in the system. Once the item in that position is removed the alarm will be triggered and an event will be generated. For more information on how to utilise alarm features please refer to the 'Alarms' section.

Audio Volume

This slide control allows you to set the volume of the system. Simply select the appropriate level from 0% - 100%.

Suppress Curfew Acknowledgement

Clicking on the icon next to 'Suppress Curfew Acknowledgement' will enable this option to be activated or deactivated.

Access the Search Report from the Login Screen only

Clicking on the icon will allow the user to toggle the option on or off to access a Search Report from the Login Screen only.

Access the Search Report from the Reports Screen only

Clicking on the icon will allow the user to toggle the option on or off to access a Search Report from the Reports screen only.

4. Click the **Next** button to navigate to the next page.
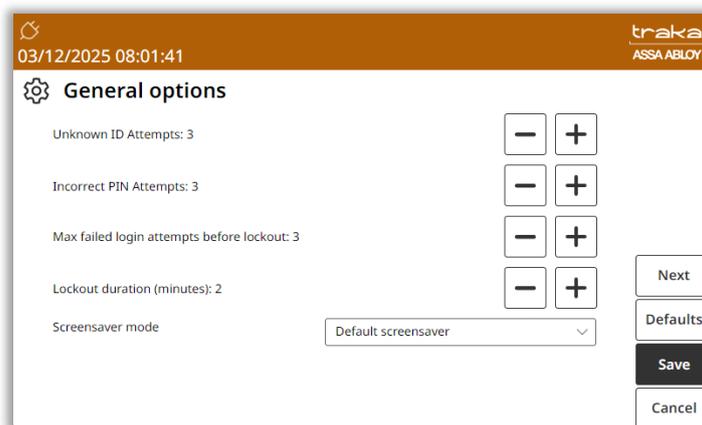
Unknown ID Attempts

Here, you can define the number of incorrect ID attempts a user can perform before an event is generated. The default value is set to three but may be changed between zero and ten where zero is off.

Incorrect PIN Attempts

Clicking on the arrows will enable you define the number of incorrect PIN attempts a user can input before an event is generated. The default value is set to three but may be changed between zero and ten where zero is off.

Max failed login attempts before lockout

Clicking on the plus/minus symbols will enable you to define the maximum number of login attempts a user will have before a System Lock Out is initiated. The default value is set to **Off** (zero) but may be increased or decreased to a maximum of 10 attempts.

Lockout duration (minutes)

Here, you can define the number of minutes a System Lock Out will last. The default value is set to five but may be increased or decreased between a minimum of one minute and a maximum of ten minutes.

Screensaver mode

Here, you can select to display either the default screensaver or the Item Availability screensaver.

Internal

5. Selecting **Next** will take you back to the previous page. Selecting **Defaults** will set all the options back to the Traka default settings.

6. When you have selected the appropriate settings click **Save**.

14.6.1 SYSTEM LOCK OUT

As of Traka Touch v4.1.0, a System Lock Out feature is included within the application. The System Lock Out feature is triggered via an adjustable number of failed login attempts and for a chosen length of time. By default, the System Lockout Feature is set as '**Off**', with a 5-minute lock out period. The number of failed login attempts and length of lock out time can be enabled via a configuration file or enabled within the general options of the Administration menu, as described in the '[General Options]' section.

NOTE: A failed login is classified as either an invalid ID, PIN, or Credential Attempt.

When a System Lock Out is triggered, Traka Touch will display the following screen:
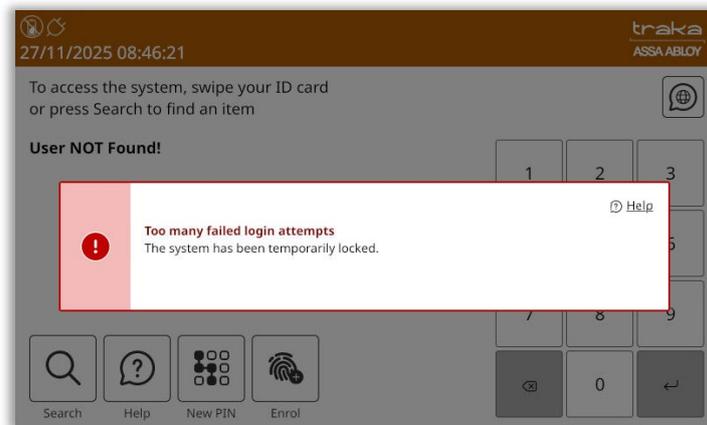
NOTE: When the System Lock Out is within the last minute of the defined time period, the Lock Out message will display a countdown:
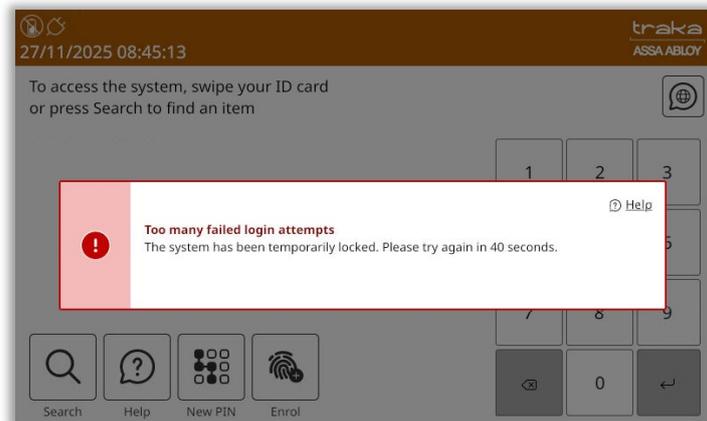
The length of the defined Lock Out time period is also the length of the cool down period in between attempted logins. For example, if a System Lock Out is set with a maximum of 3 attempted logins and with a Lock Out duration of 8 minutes, the system will monitor all attempted logins within an 8-minute time period starting from when the first attempted login occurred.

NOTE: If no Users are registered in the system's database, then a lockout will not be triggered, even if the number of attempted logins to trigger a lock out is met.

Each System Lock Out that occurs will trigger an event within the Events Report:

14.7 UPDATES

This section is used to apply upgrades to the Traka Touch system. For further information on applying upgrades, please refer to **TD0227 - Traka Touch OS Migration to Linux**.

14.8 NETWORK ADMINISTRATION

This section is only applicable if you wish to connect your Traka Touch system to TrakaWEB.

Please ensure TrakaWEB has been installed and configured before continuing. Please read the latest revision of **TD0013 – Traka Web Installation Guide** for more information.

NOTE: This action can only be performed by an Admin user.

1. Access the system and click the **Admin** button.
2. Click the **Network** button.

Internal

3. To enable communications with TrakaWEB simply select the red line button and ensure the symbol changes to a green tick. The Comms Engine and the Security Mode will remain unknown until you are connected to Traka Web. Once connected the comms engine will display the IP address and the security mode will show the security type used e.g., Comms Engine – 192.168.0.1. Security Mode – SSL.
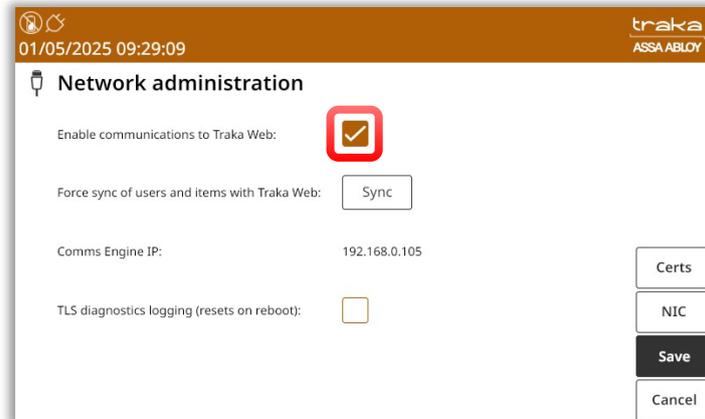
4. Force sync of users and items with Traka Web. Clicking this will force a sync with TrakaWEB to take place. A message will appear asking for confirmation of this sync, click Yes.

5. To save changes click **Save**. To view/change other settings please click the **NIC** button.

14.8.1 TLS DIAGNOSTICS LOGGING

As of Traka Touch v4.0, only TLS 1.2 is supported. Within the Traka Touch Network Administration, there is an Administration Option called **TLS diagnostics logging**. The enabled/disabled checkbox can be used to toggle network traffic logging on/off.

Internal
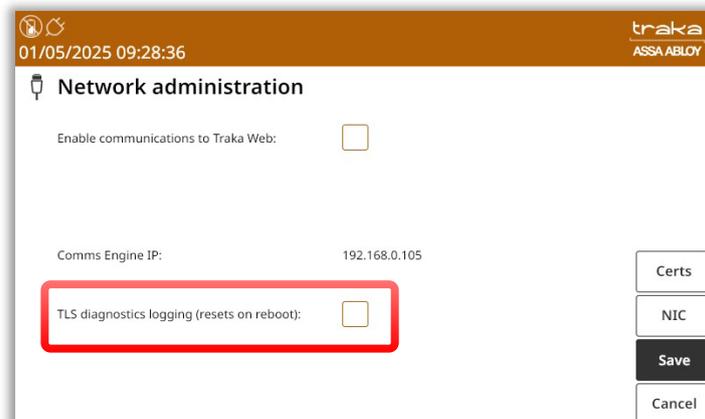
14.8.2 NIC (NETWORK INTERFACE CONTROLLER) SETTINGS

Selecting the NIC button will take you to the Network Interface Controller settings.

From here, you can view and change your IP address, IPv4 or IPv6, subnet mask, gateway, DNS etc.

To change settings simply highlight the information you wish to change e.g., IP address, and then use the keypad to delete and retype the IP address.

To change the IP Mode, select IP Mode, followed by the Internet Protocol version that you want, IPv4 or IPv6.
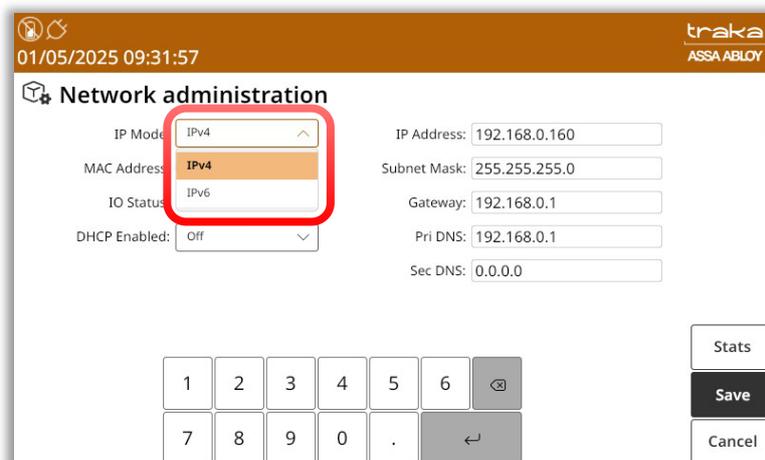
It is also possible to change the DHCP (Dynamic Host Configuration Protocol), select DHCP Enabled, followed by on or off. The DHCP option in the list will automate the IP address configuration without the use of a network administrator.

NOTE: It is strongly recommended to keep DHCP Enabled 'off'. By setting this to 'on' the communication between the Traka Touch system and TrakaWEB could be interrupted.

By selecting **DHCP Enabled** to 'on', 'Renew DHCP' will present you with a screen asking whether you wish to renew your DHCP settings. Select **Yes** if you wish to renew your settings, select **No** to return to the Network Administration page.

When you have selected the appropriate settings, you can click **Save** to apply any changes made and be taken back to the Administration menu or click **Stats** to view more detailed information on the connection to TrakaWEB.

The **Stats** screen displays various pieces of information regarding the connection health between Traka Touch and TrakaWEB. At the very top of the page there are on screen LED's that indicate the stage of communication with TrakaWEB.

When all the lights are red, this means no communication is taking place and the system is not attempting to make a connection.

When the Announce Listening light turns green, this indicates that the system is attempting to make a connection.

Once a connection is established, the Connected and Health lights will turn green. The listening light will remain red as long as a continuous connection is maintained.

Clicking **Save,** will save any changes you have made and take you back to the administration menu. From there, click **Exit** to be taken back to the login screen.

14.8.3 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The Simple Network Management Protocol (SNMP) is an internet standard protocol for collecting and organising information regarding managed devices on IP networks through customer defined parameters.

NOTE: As of Traka Touch v4.0, SNMP functionality will only be available through a configuration file. Please contact Traka for more information.

To support the functionality of SNMP, OS v5.4 or higher must be installed for the iMX6 control board. SNMP will only be supported by Traka Touch App version 2.13 or higher.

NOTE: Traka Touch will only support SNMP v2

1. Access the system as an Administrator and select the **Admin** button.

2. Select the **Network** button.

Internal
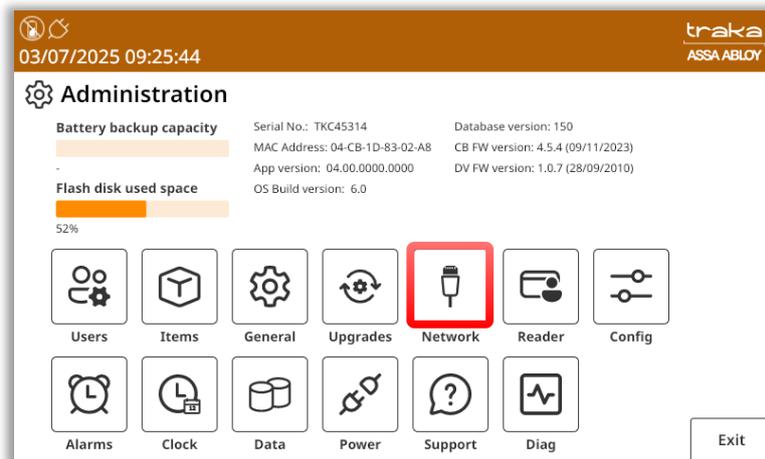
3. Select the **SNMP** button to the right of the screen. You will now be taken to the SNMP Administration screen.
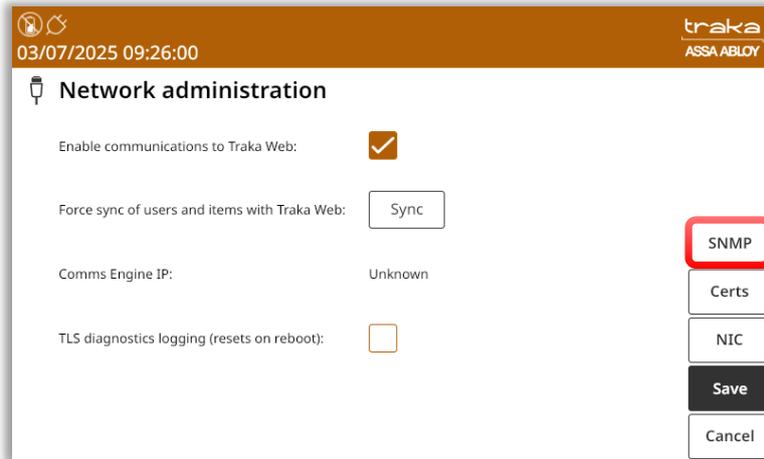
4. To enable SNMP, select the **SNMP Enabled** checkbox. The icon will change to a tick.
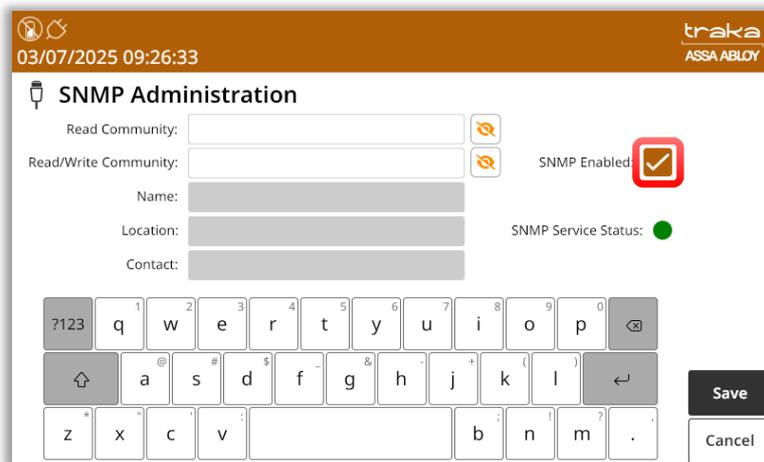
NOTE: If you decide to select the save button at this point, it is worth noting that the system will force a reboot. This will occur after saving any applied changes.

You will now be required to complete the fields shown on the screen using the keypad.

Read Community:

Enter the required Read Community string in the **Read Community** field. The string must be no more than 32 characters. The field may be hidden or shown by selecting the eye symbol located to the right. When hidden, the characters will be displayed by asterisks.

Read/Write Community:

Complete the **Read/Write Community** string in the available field. The string must be no more than 32 characters. Like the **Read Community** string, you may show or hide the value by selecting the 'eye' icon located to the right of the field. When hidden, the characters will be displayed by asterisks.

Name:

Enter a system name in the **Name** field that is no more than 15 characters.

Location:

Enter a value for the location that is not more than 255 characters.

Contact:

Enter the information for the **Contact** string. This should be no more than 255 characters.

5. After entering all the required information, select **Save.** The system will now reboot.

Internal

Once you have completed entering the required information in the SNMP Administration, you may then configure the SNMP service. The status of the service may be viewed in SNMP Administration at the Traka Touch system.

6. Access the system as an Admin user and navigate to the **SNMP Administration** screen.

A traffic light icon will display the service status. A green light will indicate that the service is running correctly. A red light will indicate that the service failed to start.
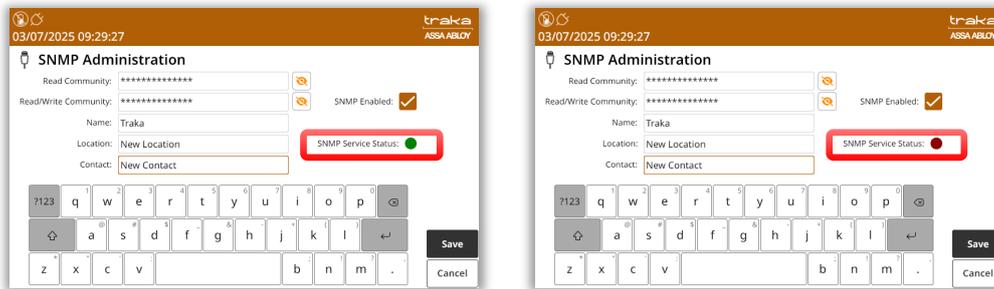
14.8.4 COMMUNICATION STATUS

When you are in the login screen, you will now notice that in the top right corner of the screen next to the Traka logo are thirteen small blocks, one of which is black. These are status blocks, showing each stage of communication with TrakaWEB.
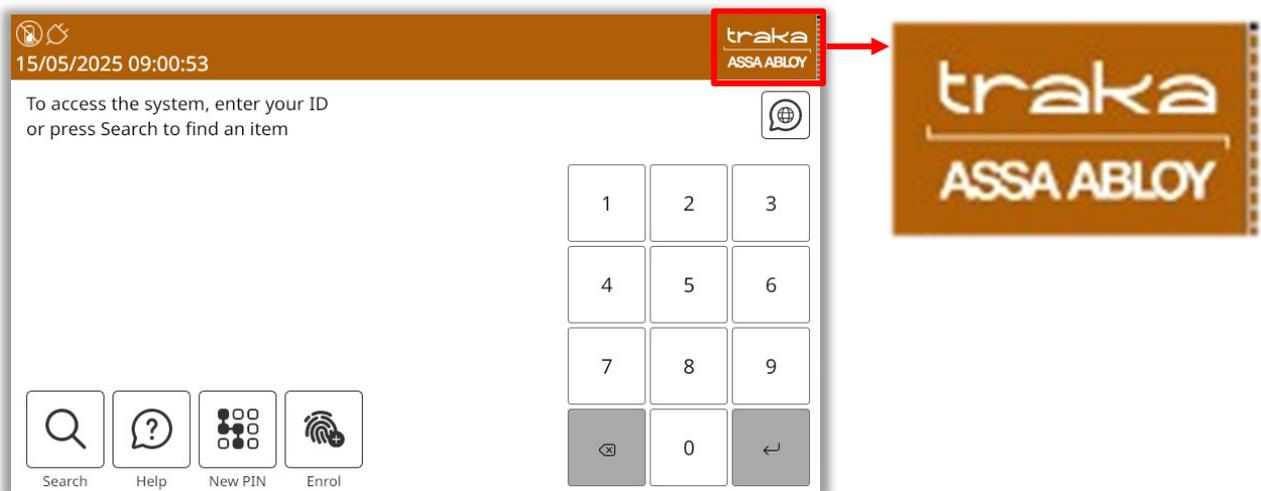
Each block represents a different stage of communication with TrakaWEB. See below for a description of each stage.

Block	Description
1	Awaiting contact from TrakaWEB
2	Synchronising System details to TrakaWEB
3	Synchronising System details from TrakaWEB
4	Synchronising Users from TrakaWEB
5	Synchronising Users to TrakaWEB
6	Synchronising Reasons, Item Types and Item Bookings from TrakaWEB
7	Synchronising Items to TrakaWEB
8	Synchronising Faults from TrakaWEB
9	Sending Events to TrakaWEB
10	Synchronising Items from TrakaWEB
11	Command request (for example, Remote Release) and synchronising Access Schedules from TrakaWEB
12	Synchronisation Finished
13	Synchronisation Error

NOTE: This table is correct as of Traka Touch App v2.0.0

The blocks will turn black as each new stage of communication begins. If an error occurs at any stage, then the final block will turn black and then light grey for one second before reattempting the cycle again. For example, if there was a communication problem whilst receiving user changes from TrakaWEB (block 4), then the status cycle will skip all other stages and move straight to the Synchronisation Error block (block 13).
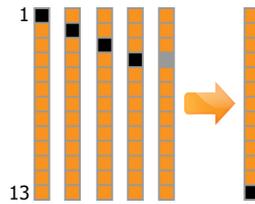
As long as the error remains, the status block will continue to cycle through the stages they have already completed accompanied by the Synchronisation Error block. Once the error has been fixed, normal communication will resume.

NOTE: One of the most frequent causes of a communication error is attributed to the firewall inbound and outbound port configuration.

NOTE: It is possible for a background communication synchronisation to occur. The user must however be a non-admin user and the control board must be a mk.3 (iMX6) control board.

14.8.5 ADDING CERTIFICATES INTO THE TRAKA TOUCH CERTIFICATES STORE (V4.0 & LATER)

In v4.0 or later of the Application software, the certificate store dropdown options have changed.

Select the **Network** menu from the **Admin** menu, followed by the **Certs** button.
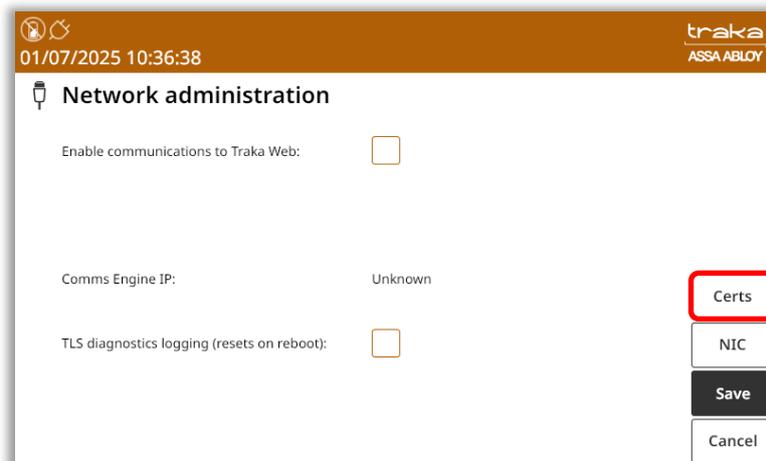
The Certificate Store dropdown options were previously:

- Root
- My
- Certificate Authorities
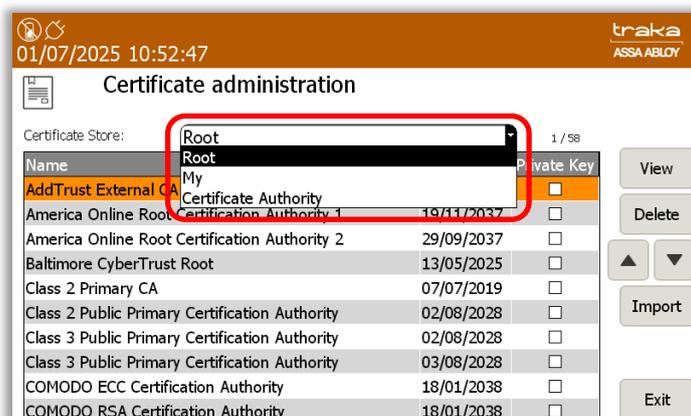
They are now:

- System Certificate Authorities
- Custom Device Certificates
- Custom Certificate Authorities
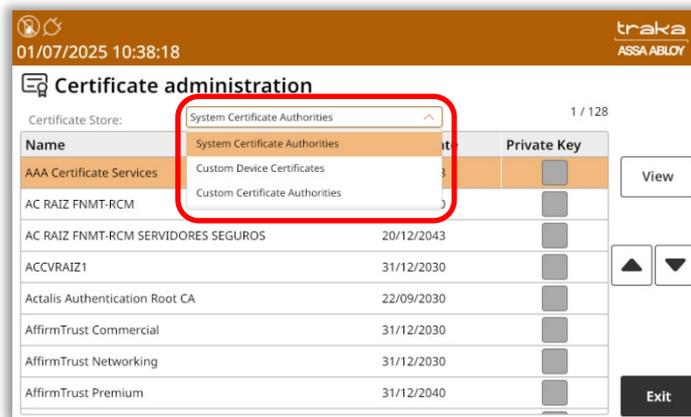
System Certificate Authorities

The System Certificate Authorities (previously Root) store is now read-only.
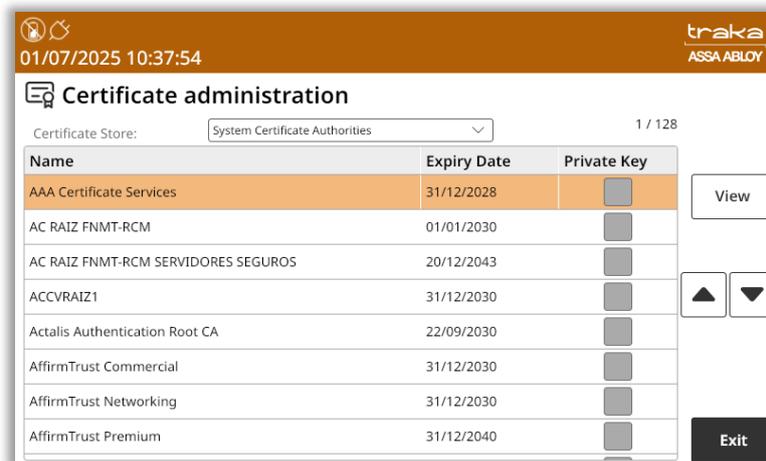
Custom Device Certificates

Custom Device Certificates are used to replace the default encryption certificates and stored in the Custom Device Certificates Store. To do this:

1. Expand the Certificate Store dropdown field and select Custom Device Certificates.

Internal

2. Select **Import**.

3. Insert a USB stick, which contains the CA Certificate you wish to load and select **Confirm.**

4. When prompted, if the certificate requires a private key, select **No**.

Internal
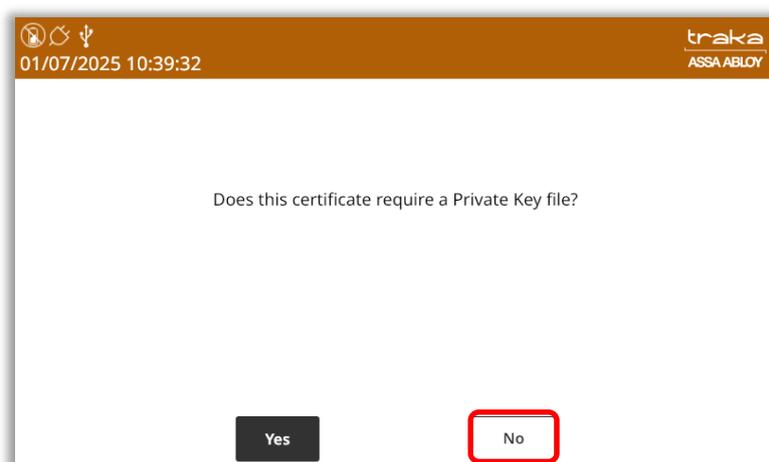
5. Ensure that the selected import store is **Custom Device Certificates** and select **Confirm**.
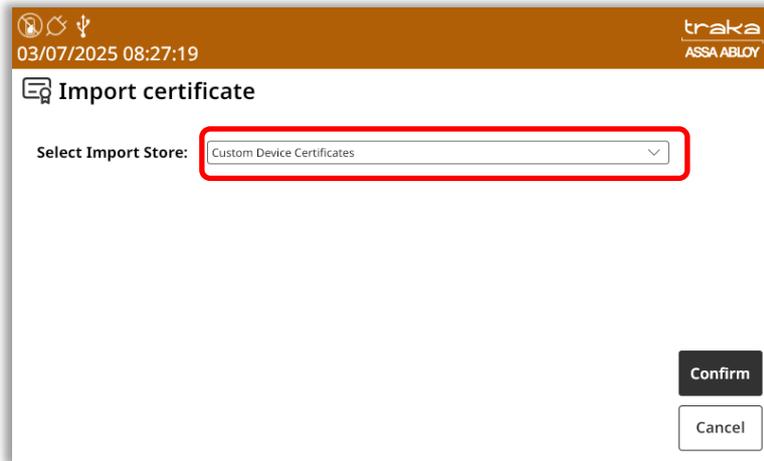
6. Once completed, you will see the newly added Certificate listed in the Custom Device Certificates store.
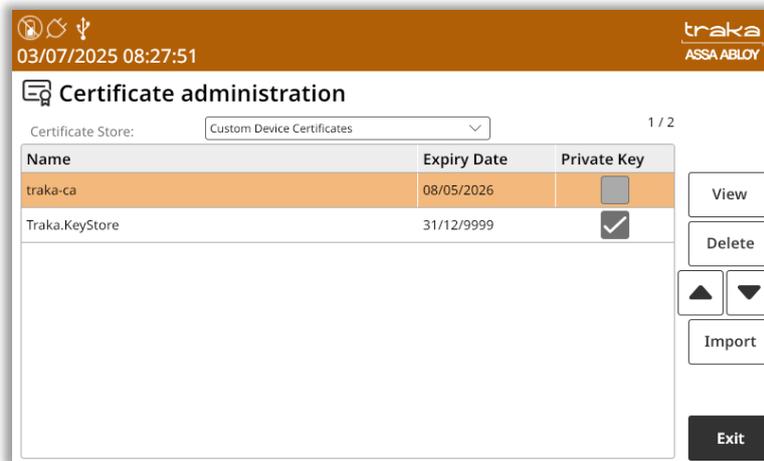
Custom Certificate Authorities

Customer own CA Certificates intended for TrakaWEB Comms should now be imported into the Custom Certificate Authorities store. To do this:

1. Expand the Certificate Store dropdown field and select **Custom Certificate Authorities**.
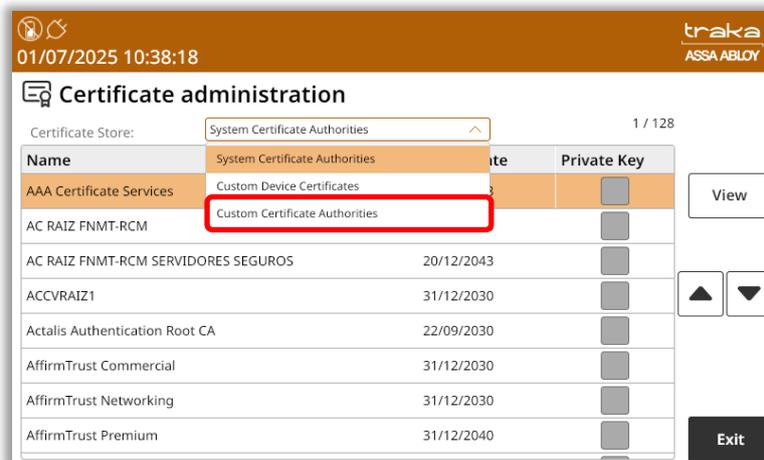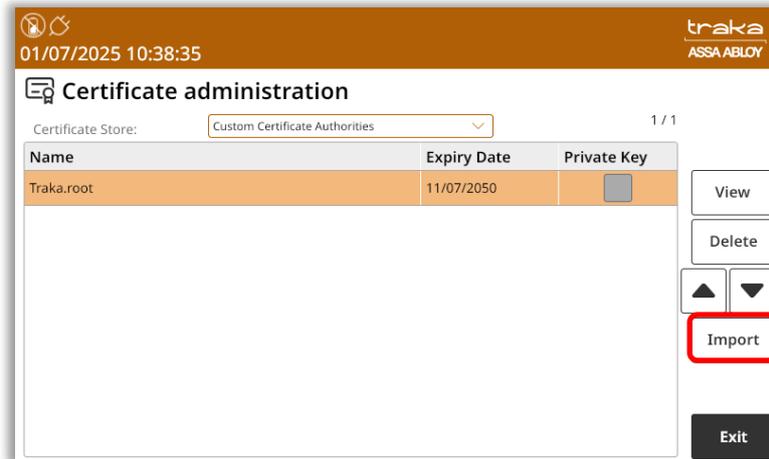
This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

2. Select **Import**.

3. Insert a USB stick, which contains the CA Certificate you wish to load and select **Confirm.**

4. When prompted, if the certificate requires a private key, select **No**.
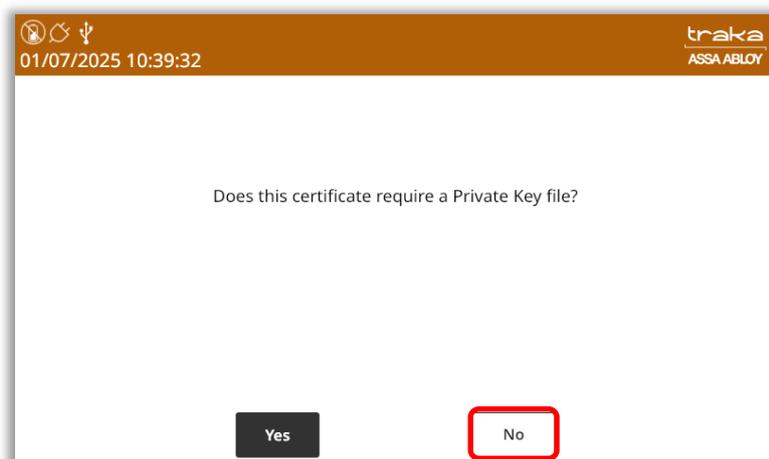
5. Ensure that the selected import store is **Custom Certificate Authorities** and select **Confirm**.
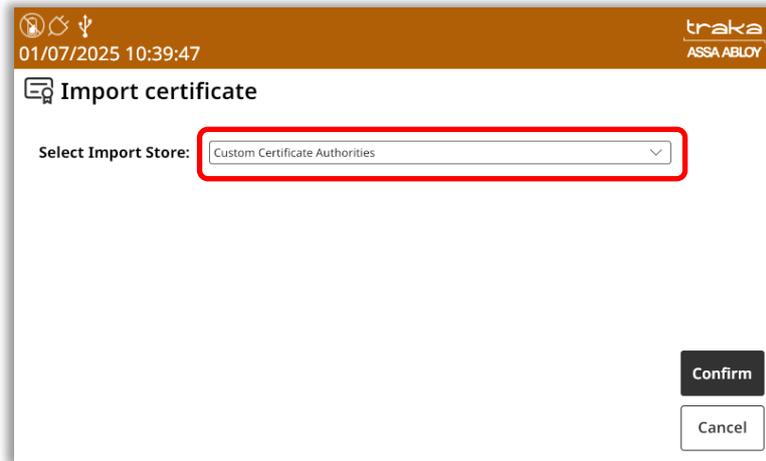
6. Once completed, you will see the newly added CA Certificate listed in the Custom Certificate Authorities store.

Internal
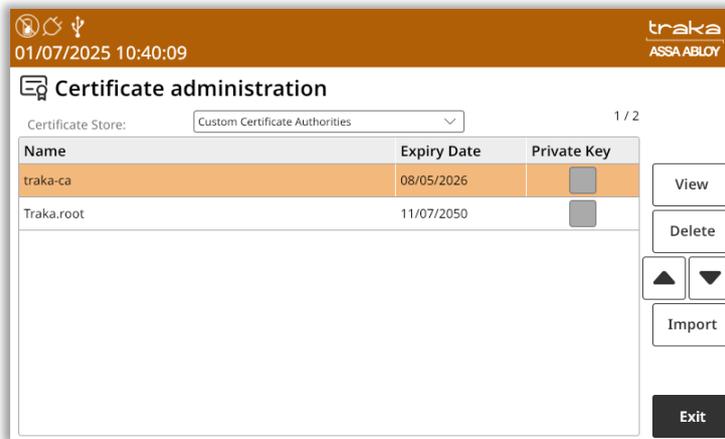
14.9   READER ADMINISTRATION

The Reader Administration Section allows you to define the system default settings for every user's PIN.

NOTE: Accessing the Reader Administration page must be carried out by an administrator. Please refer to 'Accessing the System' for further details.

1. Access the system and click the **Admin** button.

2. Click the **Reader** button.

Force User Details to Require PIN

Select this to force every user in the database to use a PIN. This will mean every time a user is created, they cannot be saved unless a PIN is entered into the user details.

Minimum PIN Length

Using the arrow keys, select the desired length of the users PIN. The minimum number of digits this can be set to is four, the maximum length is 10.

PIN will expire after XX days

Using the arrow keys, select the desired amount of time you wish before the users PIN will expire. This can be set in increments of 1 day with the maximum being 365 days. You can also select the option 'PIN will Never Expire'.

3. Once you've selected the desired options click the **Save** button.

14.10 SEARCH FACILITY

The search facility displays detailed information regarding the Item and User. This information includes....

- The last user of an item
- The current user of an item
- Status of the item
- Position of the item
- Description of the item

The search facility does not require a user to access the system; it can be used straight from the login screen.

1. Click the **Search** button.

2. The search window will then appear allowing you to type text to search, such as usernames, item descriptions and Compartment numbers.
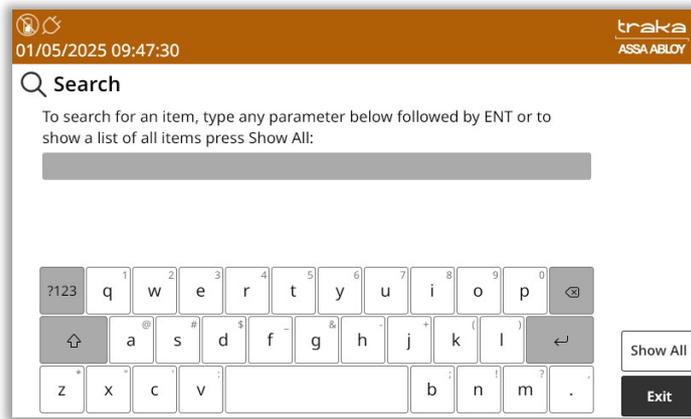
NOTE: Partial searches can be made, e.g. if you wanted to find an item that matched the description 'Barcode Scanner' instead of typing the whole description you could enter 'scanner' and the system will search for any description with that word. The searches are also not case sensitive.

3. Enter the description or the number of the item you wish to search for and click the ⏎ (enter) button.

4. After a few seconds your results will appear.
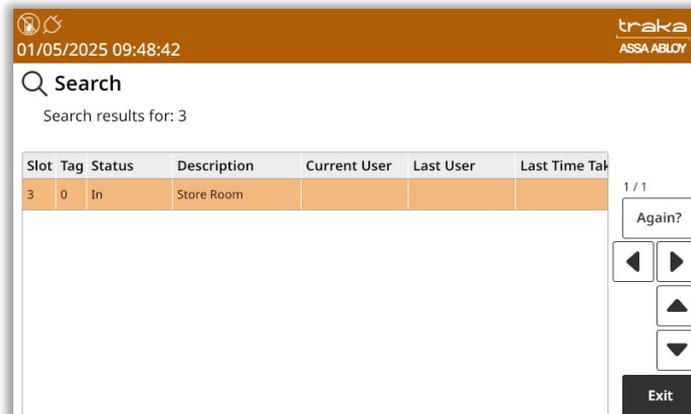
Show All

Selecting the **Show All** button will list every item in the system, the position it came from, its description, the current user and the last user.
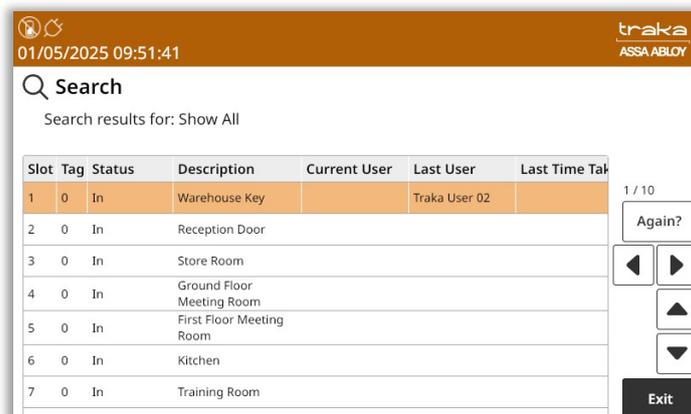
5. To conduct another search, simply click **Again**.

6. Click **Exit** to be taken back to the login screen.

14.11 LANGUAGES

The Traka Touch system can support multiple languages on a per user basis. You can also change the language for a single login only as well as change the default language for the entire system.

14.11.1 CHANGING THE LANGUAGE FOR A SINGLE LOGIN

From the main screen before you login, there are several language options to choose from. Using the Globe button, navigate to the desired language. Selecting another language will change all the text and button descriptions for as long as the user is logged into the system. If the user logs out and then decides to log back in, the system will revert to its default language.
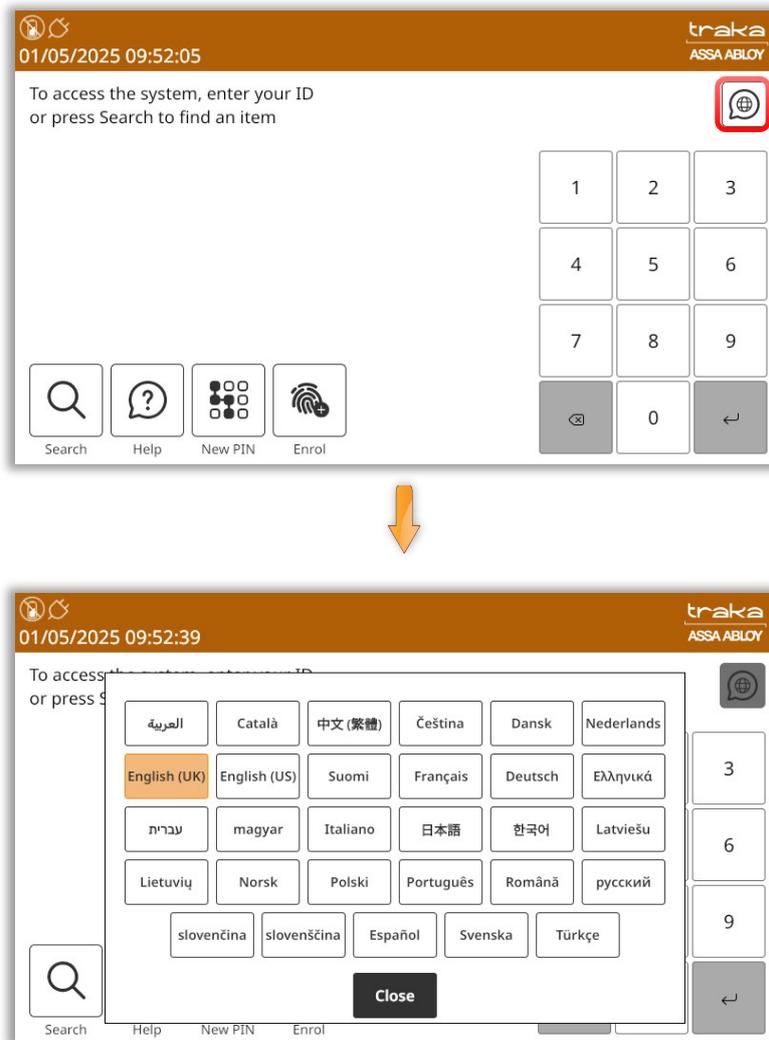
14.11.2 CHANGING LANGUAGES FOR A USER

NOTE: This action can only be performed by an Admin user. Please refer to 'Accessing the System' for further details.

1. Access the system and click the **Admin** button.

2. Click the **Users** button**.**

3. Highlight the required user and click **Edit**.

Internal

4. From here you can select the language you wish this user to view whenever they access the system. To change the language, simply use the dropdown menu to navigate to the desired language. Once you have selected the desired language click **Save** clck **Exit** to be taken back to the Admin screen.

14.11.3 CHANGING THE DEFAULT LANGUAGE OF THE SYSTEM

NOTE: This action can only be performed by an Admin user. Please refer to 'Accessing the System' for further details.

1. Access the system and click the **Admin** button.

2. Click the **General** button.

3. From here you can select the default language for the system. To change the language, simply use the dropdown menu to navigate to the desired language.

NOTE: As a default the Traka Touch system language is set to English.

4. Once you have selected the desired language click **Save**.

5. Click **Exit** and you will be taken back to the Admin screen. From there click **Exit** again to return to the login screen.

Internal

There are three Alarm Relays fitted to the Traka Touch PCB which can be configured to activate and deactivate under certain conditions. To set alarms, an admin user will need to log into the system. For further details on how to access the system please refer to the 'Accessing the System' section.

1. Access the system and click the **Admin** button.

2. Click the **Alarms** button.

   Here you can assign specific alarm conditions to the three relays on the PCB. Each alarm can only be assigned to one relay at a time. The 'On' and 'Off' columns detail what conditions must be met before an alarm is switched on or off.

   In the example below, an alarm with 'Battery Critical' as the 'On' event has been selected. Only when the battery has a critically low level of power left will the alarm activate. Once the power has been restored the alarm will deactivate.

3. To set an alarm against a relay, simply highlight the desired alarm and using the directional arrows to the right of the grid, select the appropriate relay.

Certain alarms can be activated for a set period of time. For example, if you select the 'Item Removed' alarm, you can define how long the alarm will be active for. This is definable in 1 second increments.

4. Once you have selected the desired alarms click **Save**.

5. Click **Exit** and you will be taken back to the Admin screen. From there click **Exit** again to return to the login screen.

Internal

14.12.1 MULTIPLE ALARM OUTPUTS PER RELAY

This feature will allow multiple alarm outputs from the 3 main alarm relays on the control board. This will enable multiple alarm events of a similar nature on a single relay output. A user can then be alerted to a situation via their remote monitoring system. Currently there are 2 alarm events available that will enable multiple alarm outputs as described on the next page.

On Event	Off Event
Any Tamper Open	All Tamper Closed Event

Activated under the following conditions:

- Panel Open *Or*
- Door Open Manually *Or*
- Wall Tamper Open *Or*
- Receptor Panel Open

Cleared under the following conditions:

- Panel Closed *And*
- Door Closed *And*
- Wall Tamper Closed *And*
- Receptor Panel Closed

On Event	Off Event
System Alert	System OK

Activated under the following conditions:

- Flash Storage Low *Or*
- Flash Storage Critical *Or*
- Memory Low *Or*
- Memory Critical *Or*
- One or more Item/RFID Tags is undetectable

Cleared under the following conditions:

- Flash storage OK *And*
- Memory OK *And*
- All Item Tags detectable

On the next page you will find a table of the current alarm events.

Internal

The table below shows a list of all Alarm Events.

On Event	Off Event
Any Tamper Open	All Tamper Closed
Battery Critical	Power Restored
Battery Disconnected	Battery Connected
Battery Low	Power Restored
Battery/Alarm Panel Open	Battery/Alarm Panel Closed
CAN Device Undetected	Timer
Door Emergency Opened	Door Closed
Door Left Open	Door Closed
Door Opened	Door Closed
Door Opened Manually	Door Closed
Duress Via PIN +/-1	*Timer*
Emergency Open Activated	Emergency Open Deactivated
Flash Disk Storage Critical	Flash Disk Storage OK
Flash Disk Storage Low	Flash Disk Storage OK
Item Duress Activated	Item Duress Cleared
Item Overdue	*Timer*
Item Removed	*Timer*
Item Returned	*Timer*
Item Returned by a Different User	*Timer*
Item Returned To Wrong Slot	*Timer*
Item Undetectable	Item Detectable
Items Available	Items Not Available
Items Not Available	Items Available
Memory Critical	Memory OK
Memory Low	Memory OK
Multiple Incorrect PIN Attempts	*Timer*
Overdue Item Returned	*Timer*
Override Key Unlocked	Override Key Locked
Panel Opened	Panel Closed
Power Restored	Power Fail
System Lockdown	System Lockdown End

Unauthorised Item Removed	*Timer*
Unauthorised Item Returned	*Timer*
Unknown ID Attempts	*Timer*
Unrecognised Item Returned	*Timer*
Unsupported Item Returned	*Timer*
User Logged In	User Logged Out
Wall Tamper Open	Wall Tamper closed
Receptor Panel Open	Receptor Panel Closed
System Alert	System OK

14.13 CURFEWS

Curfews 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 curfews, Specific Time of Day & Number of Days, Hours & Minutes. 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 they are not returned to the system by the end of a user's shift.

NOTE: If the System Lock Out feature has been enabled, Traka Touch allows a 5-minute grace period for items under curfew to be returned. After this 5-minute grace period, items under curfew will be recorded as 'overdue'.

You can set curfews from TrakaWEB also. Please see the latest version of **UD0018 –TrakaWEB User Guide** for more details.

14.13.1 ITEMS WITH A 'SPECIFIC TIME OF THE DAY' CURFEW

This curfew will prompt any user when they attempt to remove the item that it is due back in the system by a specific time. You will be able to define exactly what time of day the item must be back in the system e.g., the item must be returned by 17:00 once it is removed.

NOTE: When activated this curfew applies only to the item it is enabled on.

13.12.1.1 HOW TO SET THE CURFEW

1. An administrator will need to access the system.

2. Click the **Admin** button.

3. Click the **Items** button.

4. Select an item from the list and click the **Edit** button.

5. From the bottom right-hand side of the screen select **Options** to be taken to the curfew page.

Internal

6. From here select the Specific Time of Day curfew from the drop-down box and set the hours and minutes using the directional arrow keys.

7. Once you have set the curfew click the **Save** button to be taken back to the user list. From there click **Exit** to go back to the admin menu and click **Exit** again to go back to the login screen.

13.12.1.2 THE USER PROCESS

1. A user will access the system.

2. The user will then attempt to remove the item with a curfew. A message will appear stating that the item is under curfew and is due back by the defined time, e.g., 17:00. If the item is removed after 17:00 the item will be due back by 17:00 the following day and a date will also be shown above the time.
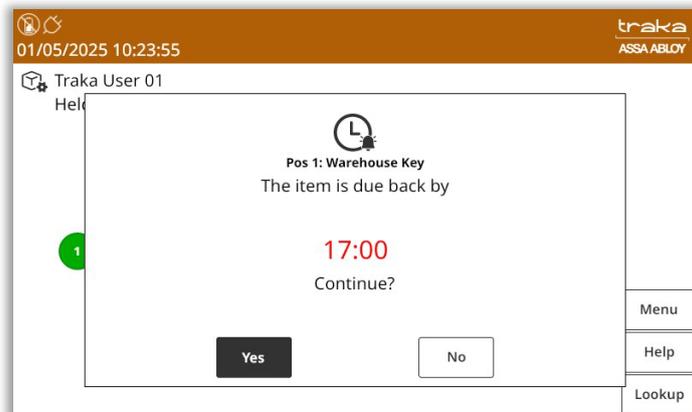
3. To remove the item, the user must click the 'Yes' button. Selecting 'No' will cancel the transaction and will require the user to log in again.

4. After selecting 'Yes,' the compartment door will open allowing the user to remove the item. The on-screen icon will change from the 'green tick' to the following...
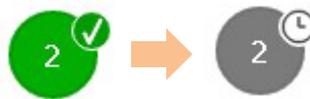
14.13.2 ITEMS WITH A 'NUMBER OF DAYS, HOURS AND MINUTES' CURFEW

This curfew will prompt any user who attempts remove the item that it is due back in the system by a specific time. You will be able to define exactly how many hours and minutes the item is allowed to be out of the system.

NOTE: When activated this curfew applies only to the item it is enabled on.

Internal

13.12.2.1 HOW TO SET THE CURFEW

1. An administrator will need to access the system.

2. Click the **Admin** button.

3. Click the **Items** button.

4. Select an item from the list and click the **Edit** button.

5. From the bottom right-hand side of the screen select **Options** to be taken to the curfew page.

6. From here select the Number of Hours and Minutes curfew from the drop-down box and set the hours and minutes using the directional arrow keys.

7. Once you have set the curfew click the save button to be taken back to the user list. From there click **Exit** to go back to the admin menu and click **Exit** again to go back to the login screen.

13.12.2.2 USER PROCESS

1. A user will access the system.

2. The user will then attempt to remove the item with the curfew. A message will appear stating that the item is under curfew and is due back by a specific time. This time is calculated based on the number of hours and minutes specified when setting up the item curfew. In this example a curfew of 1 hour has been set.
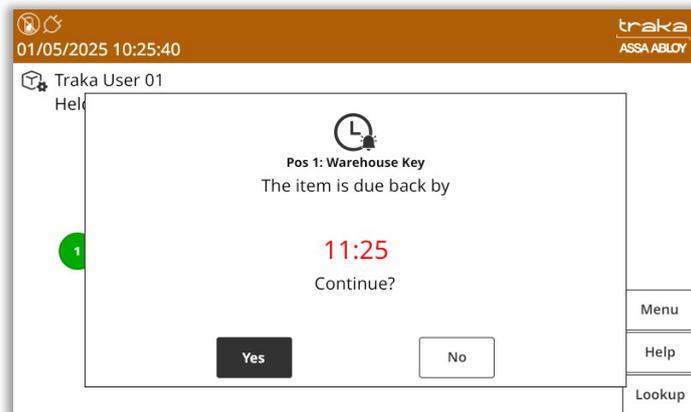
3. To remove the item the user must click the 'Yes' button. Selecting 'No' will cancel the transaction and will require the user to log in again.

4. After selecting 'Yes' the compartment door will open allowing the user to remove the item. The on-screen icon will change from the 'green tick' to the following…
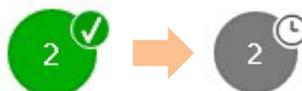
14.13.3 USERS WITH A 'SPECIFIC TIME OF THE DAY' CURFEW

This curfew will prompt the user when they remove an item that it is due back in the system by a specific time. You will be able to define exactly what time of day the user must return their item(s) to the system.

NOTE: When activated this curfew applies to all items the user has access to, as it is enabled in the user's profile.

13.12.3.1 HOW TO SET THE CURFEW

1. An administrator will need to access the system.

2. Click the **Admin** button.

3. Click the **Users** button.

4. Select a user from the currently list. And click the **Edit** button.

5. From the bottom right-hand side of the screen select **Access**, **Options** and **Next** to be taken to the curfew page.

6. From here select the Specific Time of Day curfew from the drop-down box and set the hours and minutes using the directional arrow keys.

7. Once you have set the curfew click the **Save** button to be taken back to the user list. From there click **Exit** to go back to the admin menu and click **Exit** again to go back to the login screen.

13.12.3.1.1   THE USER PROCESS

1. The user will access the system.

2. The user will then attempt to remove an item. A message will appear stating that the item is now under curfew and is due back by a set time that has been defined in the users' details, e.g., 17:00.
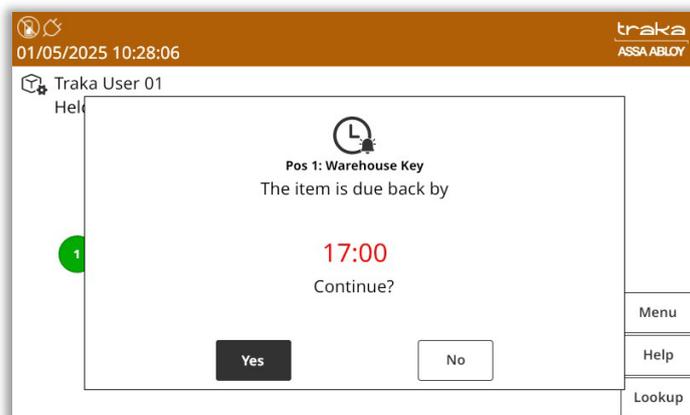
3. To remove the item the user must click the 'Yes' button. Selecting 'No' will cancel the transaction and will require the user to log in again.

4. After selecting 'Yes', the item will be released from the system. The on-screen icon will change from the 'green tick' to the following...
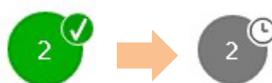
14.13.4 USERS WITH A 'NUMBER OF HOURS AND MINUTES' CURFEW

This curfew will prompt the user when they remove an item that it is due back in the system by a specific time. You will be able to define exactly how many hours and minutes the item is allowed to be out of the system.

NOTE: When activated this curfew applies to all items the user has access to, as it is enabled in the user's profile.

13.12.4.1 HOW TO SET THE CURFEW

1. An administrator will need to access the system.

2. Click the **Admin** button.

3. Click the **Users** button.

4. Select a user from the currently list. And click the **Edit** button.

5. From the bottom right-hand side of the screen select **Access**, **Options** and **Next** to be taken to the curfew page.

6. From here select the Number of Hours and Minutes curfew from the drop-down box and set the hours and minutes using the directional arrow keys.


7. Once you have set the curfew click the **Save** button to be taken back to the user list. From there click **Exit** to go back to the admin menu and click **Exit** again to go back to the login screen.

13.12.4.2 THE USER PROCESS

1. The user will access the system.

2. The user will then attempt to remove an item. A message will appear stating that the item will now be under curfew and is due back at a specific time. This time is calculated based on the number of hours and minutes specified when setting up the user curfew. In this example a curfew of 1 hour has been set for the user.
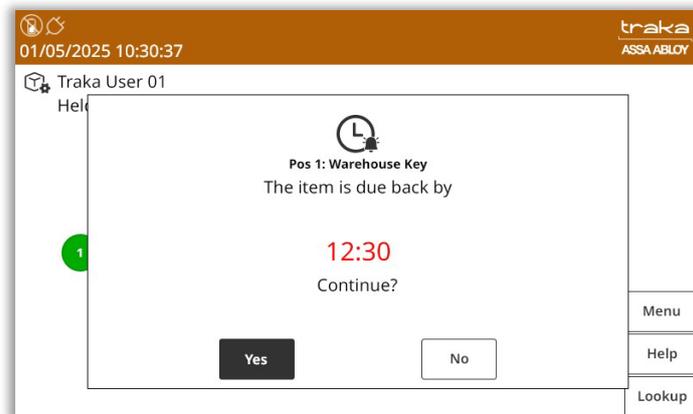
5. To remove the item the user must click the 'Yes' button. Selecting 'No' will cancel the transaction and will require the user to log in again.

6. After selecting 'Yes', the item will be released from the system. The on-screen icon will change from the 'green tick' to the following...

14.13.5 ALL CURFEWS

When an item under curfew is late back to the system it becomes 'overdue' and the icon will change as shown below.

When you access the system and the icon below is shown, this indicates another user has removed the item from the system and that item is currently under a curfew.

14.13.6 SUPRESS CURFEW ACKNOWLEDGEMENT

Activating the Supress Curfew Acknowledgement prevents notifications for curfews being displayed. It does not affect curfew functionality.

1. After logging on to the Traka Touch system with your ID PIN, swipe card or fingerprint, click on 'Admin'.
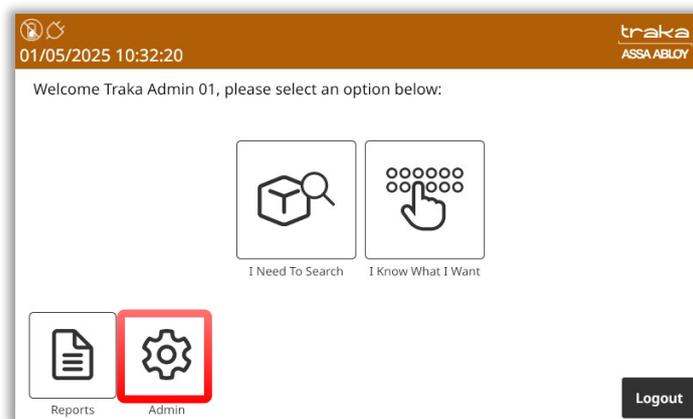
2. Next, click on 'General'.
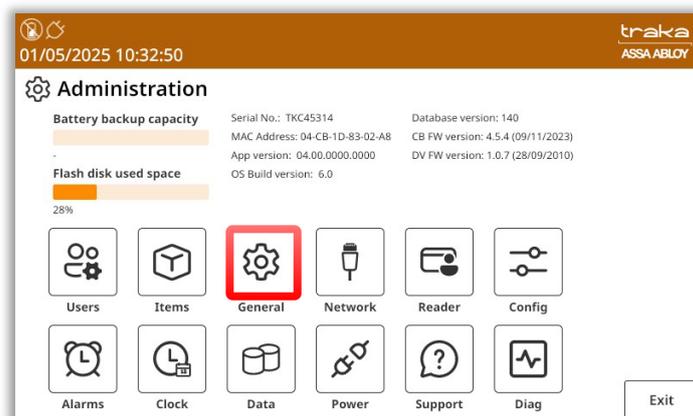
3. At the general options screen, click on next to proceed.
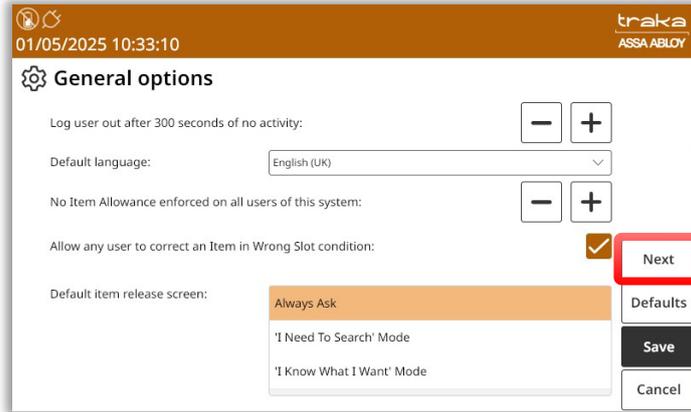
At the next 'General Options' screen, a user can enable or disable the 'Suppress Curfew Acknowledgement' option.
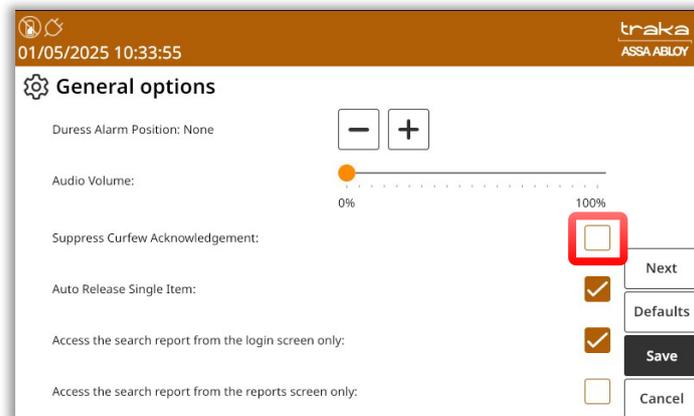
4. Click on the ☐ icon to enable the option.

5. Click on the ☑ icon to disable the option.

Once the selection has been made, click 'Save' to continue.

14.14 DATA SETTINGS

The Data Administration section allows you to define the SQL CE Database options and tools. To edit these options, an admin user will need to log into the system. For further details on how to access the system please refer to the 'Accessing the System' section.

1. Click the **Admin** button.

2. Click the **Data** button.
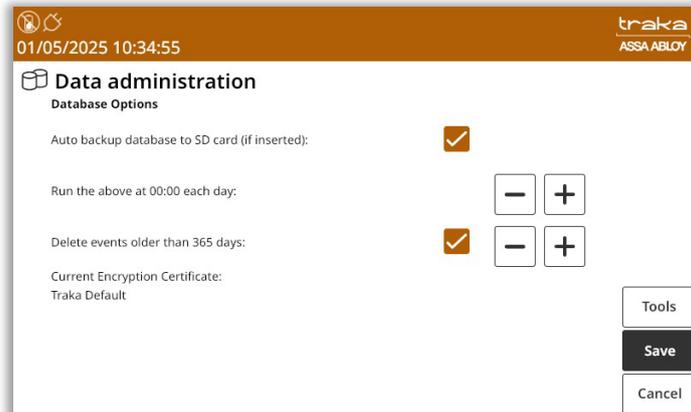
SQL CE Database Options

Auto Backup Database to SD card (if inserted) - This option can be enabled or disabled by clicking the small tick or line.

Run the above at xx:xx each day – Selecting this option will allow you to set a specific time in which the options above will take place.

Delete events older than x days - This option can be enabled or disabled by clicking the small tick or cross button. The maximum number of days this can be set to is 1825.

NOTE: You can define how many days' worth of data the system will return. Any event older than the number of days specified will be deleted. USE WITH CAUTION!

Current Encryption Certificate – this is the current encryption certificate that is being utilised.

Tools Page

Clicking the Tools button will take you to the SQL CE Database Tools page.

Internal
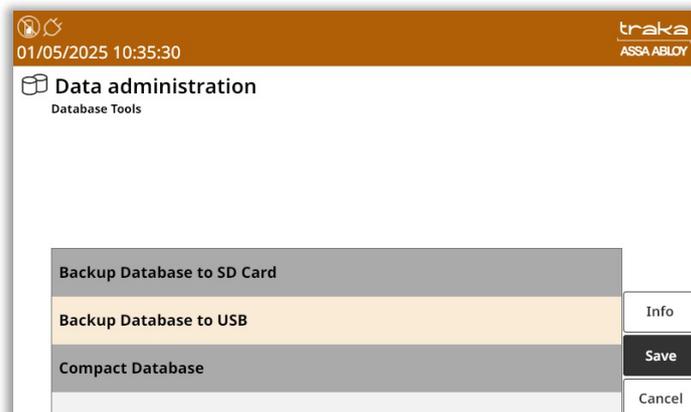
From here you can do the following...

- Backup Database to SD Card
- Backup Database to USB
- Shrink Database
- Compact Database

Once you have selected one of these options, simply follow the on-screen instructions to complete the action.

Information page

The information page displays the memory usage of flash disk and SD card and provides the size of the Database and application. To view the information page, click the **Info** button on the Data Admin screen.
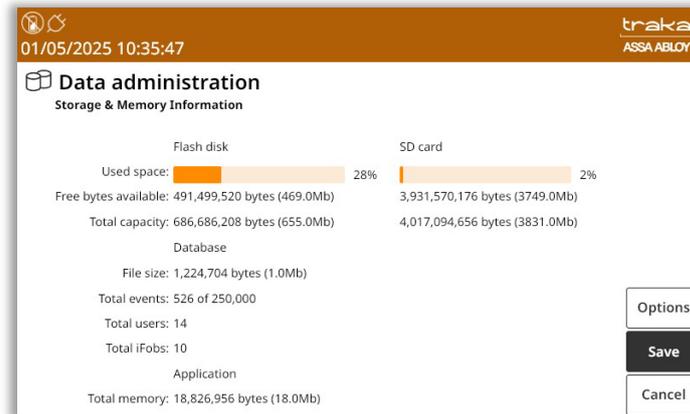
To return to the Data Admin screen click the Options button.

Click **Save** to save any changes or **Cancel** to return to the admin menu. From there click **Exit** to be taken back to the login screen.

14.15 POWER SETTINGS

The Power Administration section allows you to change the touch screen brightness under certain conditions, such as when the Battery is Low or Critical, or when the system is running on Mains etc.

To edit these options, an admin user will need to log into the system. For further details on how to access the system please refer to the 'Accessing the System' section.

1. Click the **Admin** button.

2. Click the **Power** button.

Internal
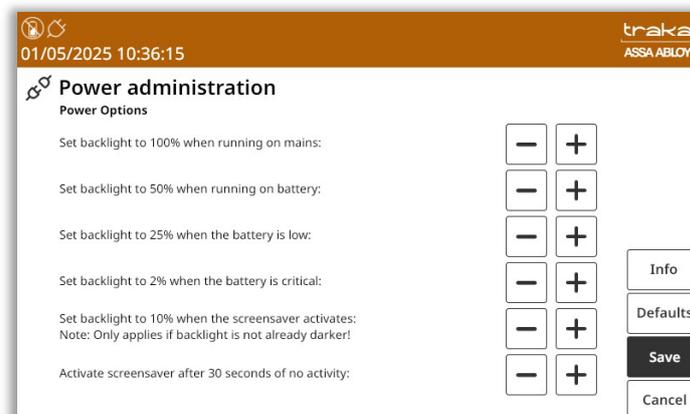
Power Options

To change any of the power options simply click either of the arrow keys to the right of the description. The power options are as follows...

- Set backlight when running on mains
- Set backlight when running on battery
- Set backlight when the battery is low
- Set backlight when the battery is critical
- Set backlight when the screensaver activates

NOTE: Only applies if backlight is not already darker

- Activates screensaver after x seconds of no activity.

The **Defaults** button sets all your custom power options back to the Traka default settings.

The **Info** button displays all the power supply information, such as the battery backup capacity and Voltage, the mains power level etc. Click the **Options** button to return to the power options.
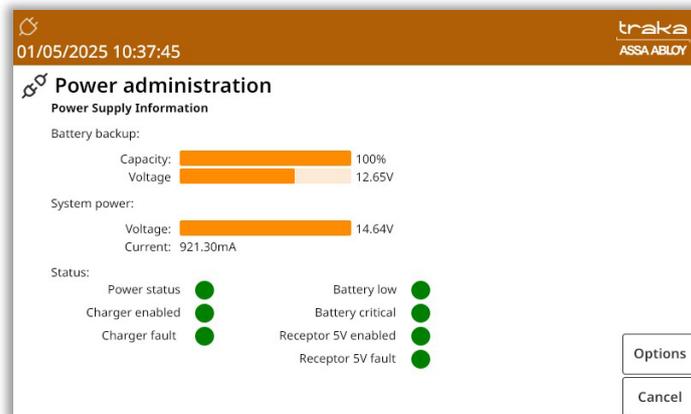
When you have completed your changes click **Exit** and you will be taken back to the admin menu. From there click **Exit** to be taken back to the login screen.

14.16 CONFIGURATION

The Config administration section allows you load a new configuration file into the system. This is required if a customer has requested additional software options or has had a change of reader for example. Traka will then compile a new configuration file and send it to you to import via a USB memory stick.

To access the configuration page an admin user will need to log into the system. For further details on how to access the system please refer to the 'Accessing the System' section.

1. Once you have the new configuration file, copy it to a usable USB memory stick.

Internal
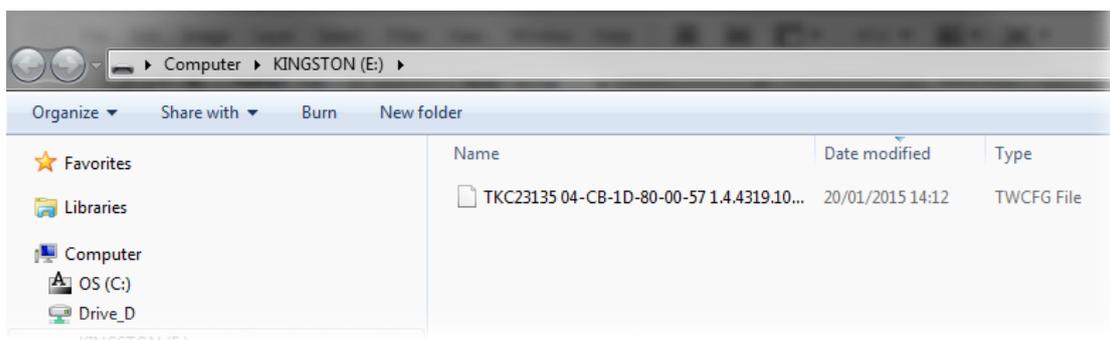
2. Access the system and click the **Admin** button.

3. Click the **Config** button.
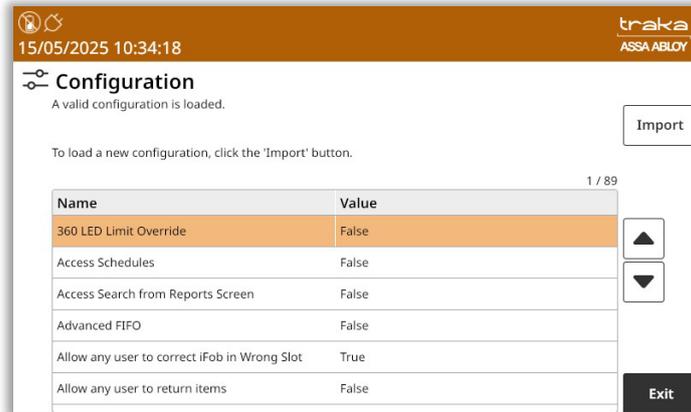
4. Click the **Import** button in the bottom right-hand corner of the Configuration screen.
5. The system will then open the door and prompt you to insert a USB memory stick.

NOTE: **For further information on USB memory stick specification, refer to the** [USB Memory Sticks](#) **section.**

NOTE: **Depending on the configuration of your Traka Touch Lockers the USB port may be located inside a locker compartment. In this case the door will open automatically through this process giving you access to the USB port.**
If your system does not have a USB port located inside a locker compartment, you will need to gain access to the inside of the Traka Touch Pod by opening the control panel. See the 'Opening the Control Panel' section for more information.

6. Check the file name and click confirm to begin the import process.

Internal
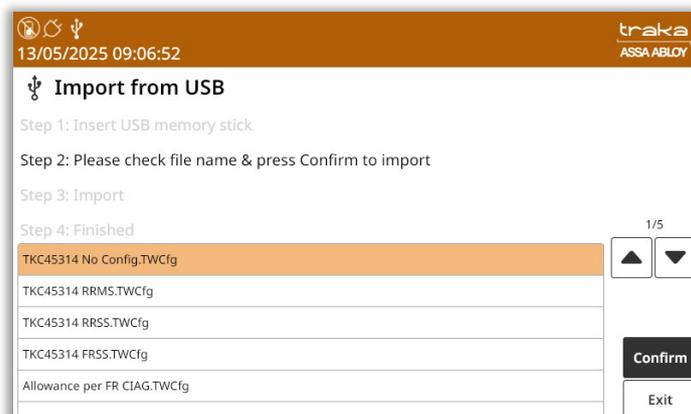
7. The import process will then begin. A message will appear stating the import was successful and an immediate restart is required. Click OK to begin the system restart.
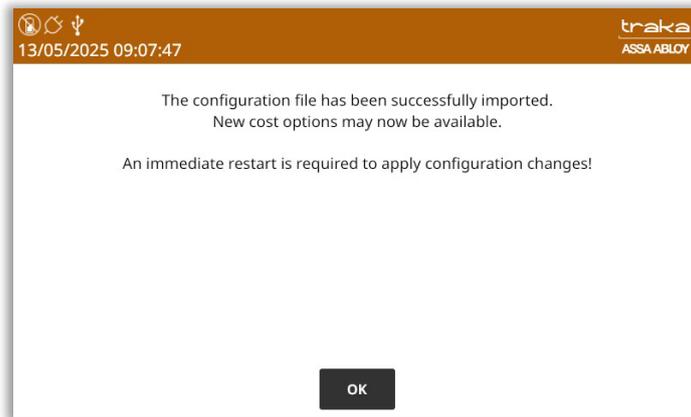
8. The system will then restart; this may take a few minutes.
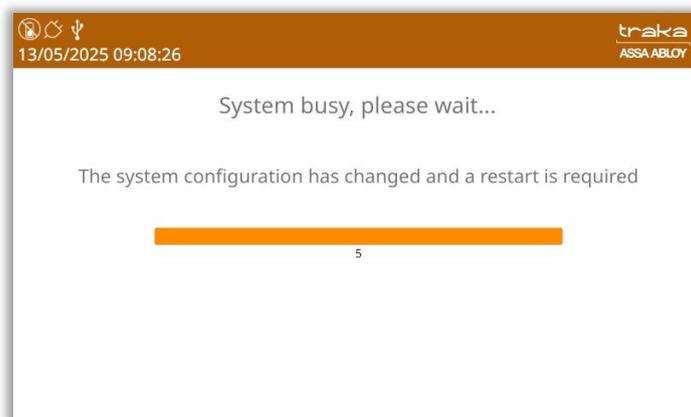
9. Once the system is rebooted you can use it as normal, with all the new features that came with the configuration.

Internal

14.17.1 VIEWING THE HELP SECTION

The Help section holds all of the information for your point of contact in case of assistance. The Help icon is on the main Traka Touch screen and does not require a user to access the system to view it.

1. Click the **Help** button.

2. The Help window will then appear allowing you to obtain all the relevant contact information in case of any problems or errors.

3. Click the **Exit** button to return to the login screen.

14.17.2 CHANGING THE SUPPORT SECTION

To edit the information in the Support section, an admin user will need to log into the system. For further details on how to access the system please refer to the 'Accessing the System' section.

1. Click the **Admin** button.

2. Click the **Support** button.
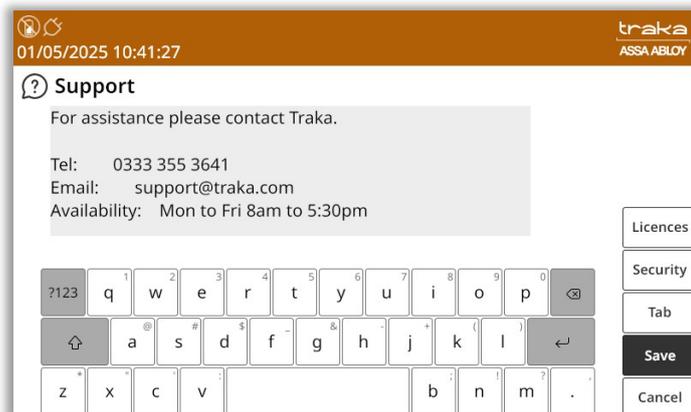
3. To edit the help information, simply click on the desired field and use the onscreen keyboard to type the relative information.

4. Clicking the **Licenses** button allows you to view all software licenses associated with the system.
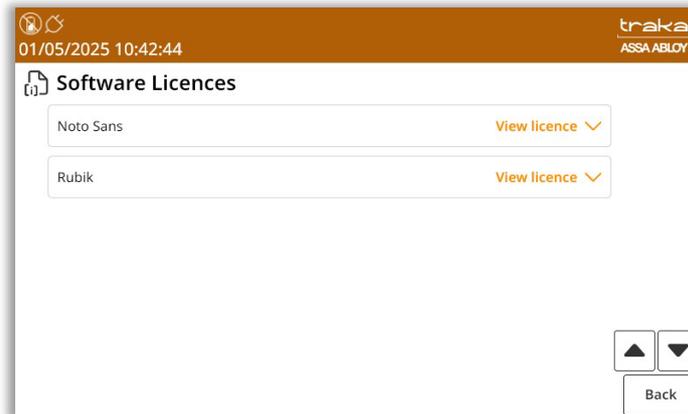
5. Clicking the Security button will take you to the Support Code Administration page.

6. When you have completed your changes click **Save**. Click **Exit** and you will be taken back to the admin menu. From there click **Exit** to be taken back to the login screen.

Internal

14.18 BACKING UP THE TRAKA TOUCH DATABASE

The database holds all the information Traka needs to operate including the users, items, and event history. Traka Touch is supplied with an SD card to store database backups. The live database is stored on the flash disk. If the database is not backed up regularly and the machine fails for any reason you will have to start over again.

An admin user will need to log into the system. For further details on how to access the system please refer to the 'Accessing the System' section.

1. Click the **Admin** button.
2. Click the **Data** button.
3. Click the **Tools** button from the bottom right-hand side of the screen.
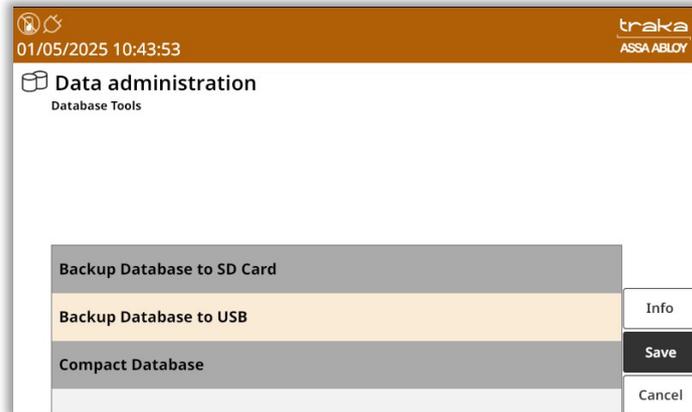
You can choose from two backup options:

- **Backup Database to SD Card**
- **Backup Database to USB**

And there are two other options that allow you to minimise the size of your database.

i. **Compact Database** - Compacts wasted space in the database by creating a new database file from the existing file and permanently deleting data that has been deleted in Traka Touch e.g., user records.

Backup Database to SD Card
This option will fully backup your database to the SD Card (if inserted)

1. Select the **Backup Database to SD Card** button.

2. The system will then ask if you wish to back up the database. Click the **Yes** button.
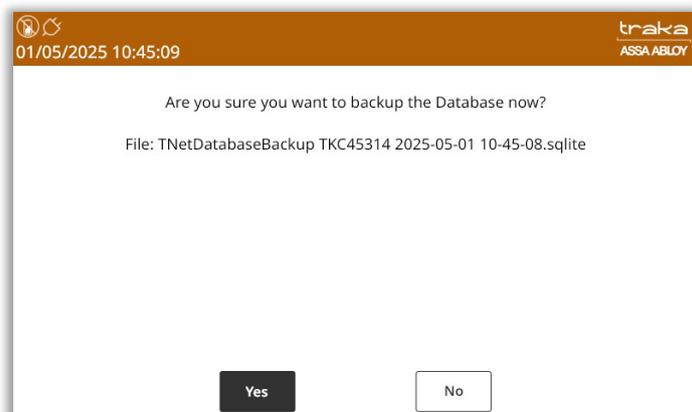
3. When the backup has successfully completed, click the **OK** button.

Backup Database to USB

This option will fully backup your database to a USB memory stick.

1. Click the 'Backup Database to USB' button.

Backup Database to USB

2. A compartment door will open (if applicable) and prompt you to insert a USB memory stick into the vacant socket.

NOTE: For further information on USB memory stick specification, refer to the USB Memory Sticks section.

NOTE: Depending on the configuration of your Traka Touch Lockers the USB port may be located inside a locker compartment. In this case the door will open automatically through this process giving you access to the USB port.

If your system does not have a USB port located inside a locker compartment, you will need to gain access to the inside of the Traka Touch Pod by opening the control panel. See the 'Opening the Control Panel' section for more information.

3. You can rename the database file if you wish by using the provided keyboard. When finished click the ↵ (enter) button.

Internal

4. The system will now export the database to the USB device.
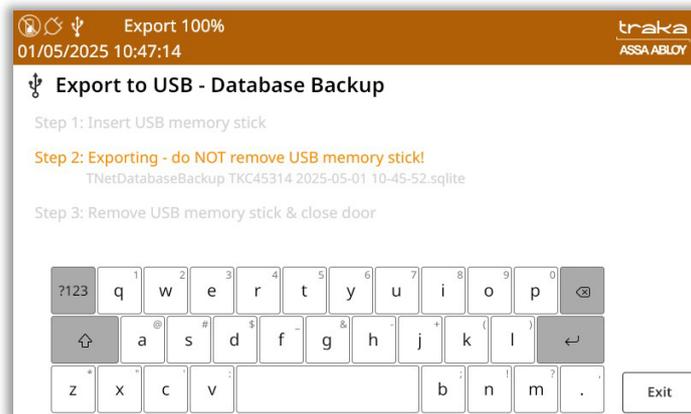
5. Once the export is complete you can remove the USB device. You will be taken back to the Data Admin menu.

15. SAGEM MORPHOSMART READER

15.1   INTRODUCTION

This section has been produced to outline some essential information regarding the Sagem MorphoSmart Fingerprint Reader. Prior knowledge of the Traka Touch System is assumed.

15.2   SYSTEM REQUIREMENTS

Below is a list of minimum hardware and software requirements required for the Sagem MorphoSmart Fingerprint Reader to operate correctly on Traka Touch.

15.2.1 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.

15.2.2 TRAKA TOUCH OPERATING SYSTEM

For the Sagem MorphoSmart Fingerprint Reader to work with Traka Touch, the Traka Touch unit must have an OS build version of 1.9 or later installed. Navigate to the Help section to check the Build Version.
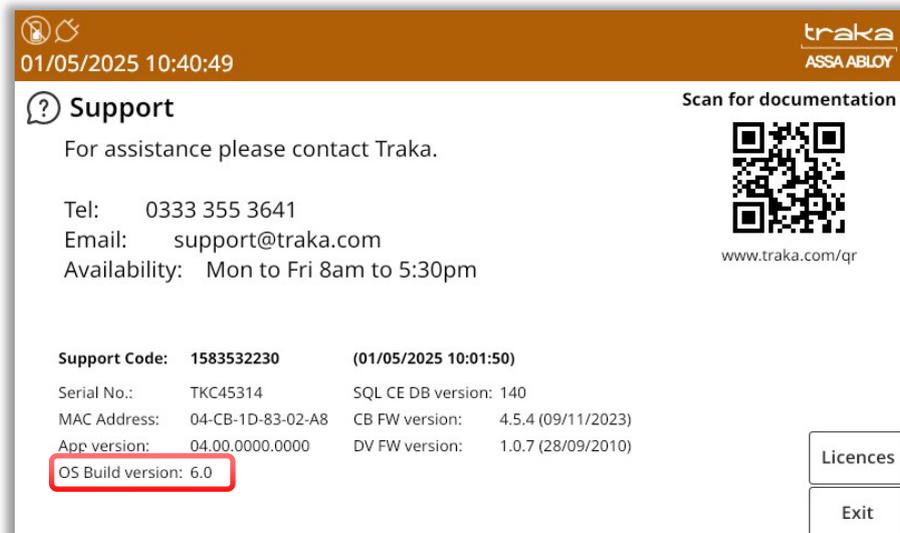
NOTE: If a Traka Touch PCB must be replaced for any reason, replacements might not have version Windows CE 1.9installed by default, therefore please specify version Windows CE 1.9 or later when raising an RMA request. If you connect a Sagem MorphoSmart Fingerprint Reader to a version of Windows CE less than 1.9, when you plug the reader in, you get a Windows CE dialog pop up requesting the Driver Name.

15.2.3 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.

15.3   ACCESS METHODS

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's simply plug & play.

In addition, it's possible to use a Keypad ID or a Credential ID as an alternative method of access or a backup method of access in case of issues with the fingerprint reader. For users to access the system via the alternative method the associated user record must have a Keypad ID or Credential ID defined.

Mode	Keypad Only	Card Reader
No fingers enrolled	Enter Keypad ID on keypad	Swipe Card
Fingers enrolled	Touch finger	Touch finger **OR** Swipe Card

In keypad-only mode, any user may opt out of using a fingerprint by not enrolling a template and by defining a Keypad ID in their user record. The user will then be able to login using a normal Keypad ID. This is useful for users who have poor fingerprints.

PIN functions as normal and the system will ask for it if the PIN is defined in the user record.

15.4   READER DISCONNECTION / RECONNECTION

If the Sagem MorphoSmart Fingerprint Reader is disconnected at any point, the system will revert back to the alternative method of access (i.e., Keypad Only or Card Reader).

TIP: It's worth setting up at least one administrator with a Keypad ID or Credential ID so that they can still access the system in case of reader issues.

At application start-up or whenever a (new) reader is attached to the system while the application is running, the application will initialise the Reader and will send down all templates from the Traka Touch SQL CE Database to the reader – this may take some time when there are a lot of users enrolled. A message will appear at the top of the display saying 'Initialising Biometrics...' whilst this is in progress.

There is no need for any 'Sync' or 'Reset' function as the reader is updated dynamically as each user record is changed. Fingerprint templates cannot be taken from one Traka Touch to another by moving the reader.

NOTE: If the reader is disconnected whilst in the middle of identifying or enrolling a user, this will invalidate the whole communication process and so if you try to reconnect the reader it will no longer work until you power cycle the whole system.

15.5   HOW TO ENROL A USER

Organisations using a Traka Touch system within any jurisdiction where GDPR applies should ensure they have put measures in place to fulfil their obligations under that legislation relating to biometric (finger) data, before inviting users to enrol this data into the Traka Touch system. In particular:

- The organisation may have decided that use of users Personal Data within its Traka system is based on "legitimate interest" or some other basis that does not require "consent" but must be mindful that this does not normally extend to biometric data, which normally can only be used with explicit, recorded "consent".

- The organisation must ensure that its management actions and its working practices do not accidentally or intentionally restrict the genuine freedom of choice of the employee to use the Traka system without using the biometric reader.

- The organisation must obtain the consent of the user (employee), in some form that can be kept as proof, for the user's biometric data to be put into the system (via the enrolment process) and used within the system (for the purpose of identifying the user to the Traka system). The user must give this consent (if they wish to enrol their finger), and the consent must show that they have genuine freedom of choice about giving this

consent (or not doing so). The consent must also show that the user knows they can withdraw this consent in future, if they wish to, and that they know how to do so.

When a user decides to enrol their finger (biometric data) as a method of accessing the Traka systems, they should not normally also have a Keypad ID Number held within the system.

There are 2 ways of enrolling users' fingerprints on the Traka Touch system:

- Manually enrolled by an admin
- Via an Enrolment ID

15.5.1 MANUAL ENROLMENT BY ADMIN

This method requires both an Admin user and the user to be enrolled to be present at the Traka Touch System.

1. The Admin user must access the system and navigate to the User List, and then edit/add the required user.

2. On the User Details screen, click **Access**->**Options->Next->Enrol** and you will be presented with the enrol screen. This button cycles round the various screens i.e., Access->Options->Enrol->Details->Access etc.

3. When you get to the enrol screen, it will display how many fingers are enrolled for the user, 0, 1 or 2.

4. To clear enrolled templates for a user, click the **Clear** button.

To enrol 1 or 2 fingers, use the up/down buttons to select the required number of fingers to enrol and press the **Enrol** button.

Simply follow the on-screen instructions. The system will prompt the user to place each finder to be enrolled on the reader **3** times.

 Place finger   Capture Ok   Remove finger

When placing a finger, if the finger is not located correctly on the reader the following icons will be displayed:

 Press harder

 Move finger up

 Move finger down

 Move finger right

 Move finger left

When complete, the screen will display how many fingers are enrolled for the user, 1 or 2. To cancel the Enrol process, click the central Cancel button. Once the Enrolment is complete click **Save**.

NOTE: The template will not be written to or cleared from the reader until Save is clicked.

NOTE: When enrolling the first administrator, please ensure you enter a Keypad ID or Credential ID. This is essential so that they can still access the system in case of reader issues. You will not be able to save the user record unless this is supplied. If you have the system configured as Keypad Only, there is no restriction on the Keypad ID length and so for added security you could for example enter a 6 or 10 digit PIN.

15.5.2 ENROLMENT ID

An Enrolment ID is a number assigned to each user to enable them to enrol their fingerprints the first/next time they access the system. This allows the User to enrol without the need to have an Admin User present. The Enrolment ID must be entered into the correct field in the User Import Spreadsheet. For more information on Exporting and Importing users please refer to the 'Exporting and Importing' section. It is possible to force a single finger enrolment or 2 finger enrolments; this choice is controlled by the 'configuration file' loaded into the Touch unit – if you wish to swap from single finger to 2 finger enrolments, contact Traka for a new 'configuration file'.

1. Export the User spreadsheet and enter an Enrolment ID into the appropriate filed for each user you wish to enrol. The maximum length allowed for the Enrolment ID is 30 characters.

2. Import the User spreadsheet to the Traka Touch system.

3. From the login screen the user must select the Enrol button.
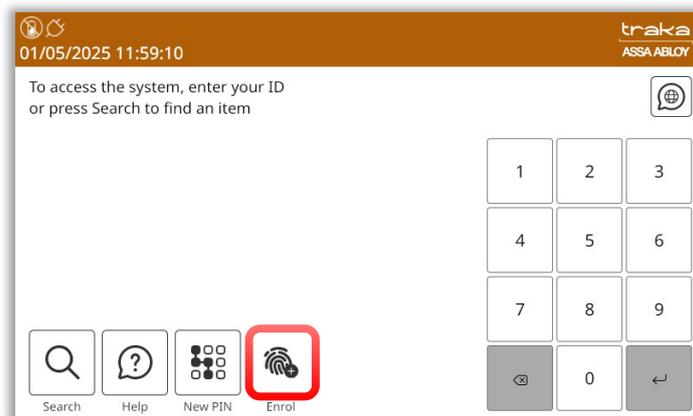
4. The user can now enter their assigned Enrolment ID and press ⏎ (enter).
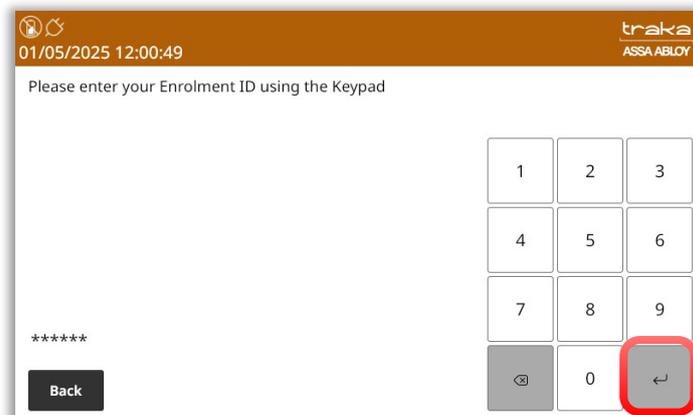
5. Follow the on-screen instructions to take 3 captures of the users' fingerprint. This process is the same as shown in the previous section 'Manual Enrolment by Admin'. The image to the right shows the screen for 2 finger enrolment with "**Enrol Finger 1 of 2**" visible.

6. If the fingerprint captures are successful, you will be presented with the following screen. The User can now access the system by the method explained in the next section.
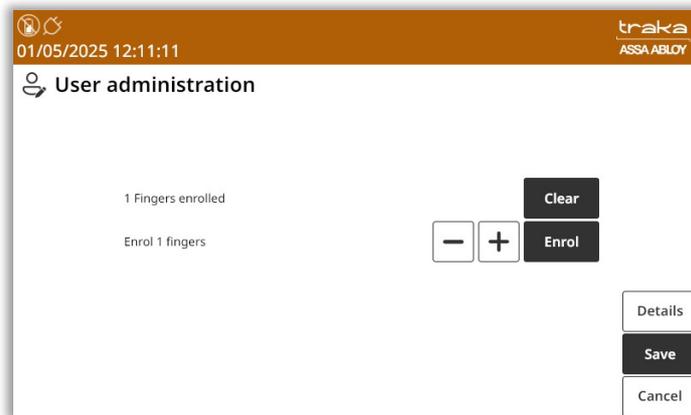
15.6   HOW TO ACCESS THE SYSTEM

When the login screen is displayed, simply place your enrolled finger on the reader. If recognised, the system will log you in.
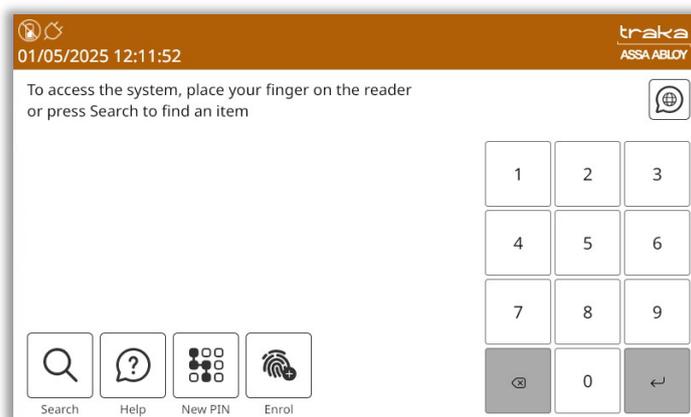
NOTE: When the main login screen is shown, the red light on the reader will NOT illuminate if no users have been enrolled in the database.

NOTE: To save energy, the fingerprint reader is disabled when the Screen Saver comes on. To activate it again, just touch the screen to close the Screen Saver.

15.7 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.
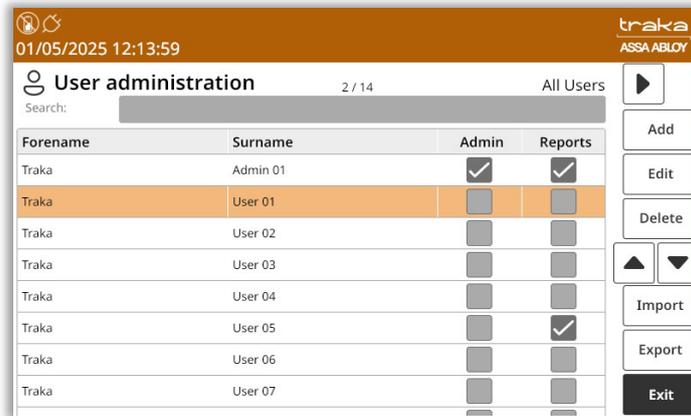
2. Select the enrolled user you wish to edit and navigate to the User Administration Enrolment page.

The User Administration page will now display an additional **Clear** button for an enrolled user.
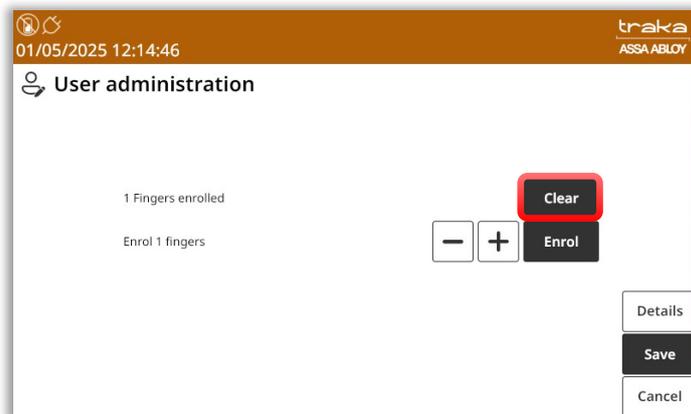
3. Select the **Clear** button.

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.
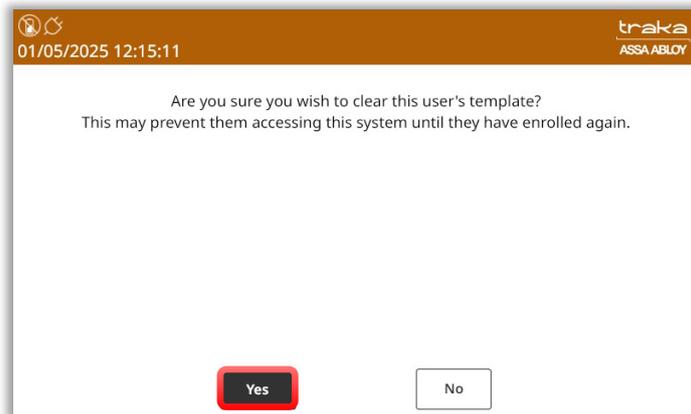
The users' template is now removed from the database. The User Administration page will remain visible should the user require re-enrolling.

5. Once completed, select the **Save** button.
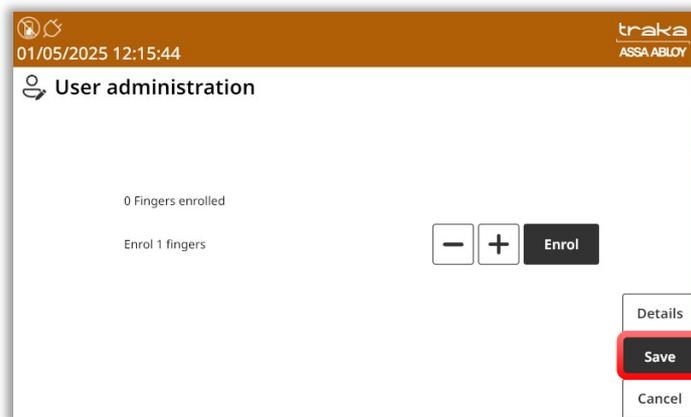
To get the best quality image, one needs to:

- Maximise the finger/sensor contact
- Position the centre of the fingertip in the centre of the sensor
- Ensure a good quality contact
    - Leave your finger on the sensor at least 2 seconds or wait until the sensor light goes out
    - Do not press too hard
    - Do not move during image acquisition
    - Do not slide nor roll your finger across the sensor
- Try to avoid dry finger or cold fingers!

VERY USEFUL TIP: If you are having issues, brush the fingertip along the side of your nose – this adds a fine layer of natural grease to your finger and will get you a much better read!

How to position your finger correctly on the sensor:

Finger Height

Finger Angle

Ideal Position

Ideal Position

Finger Inclination

Finger Rotation

Ideal Position

Ideal Position
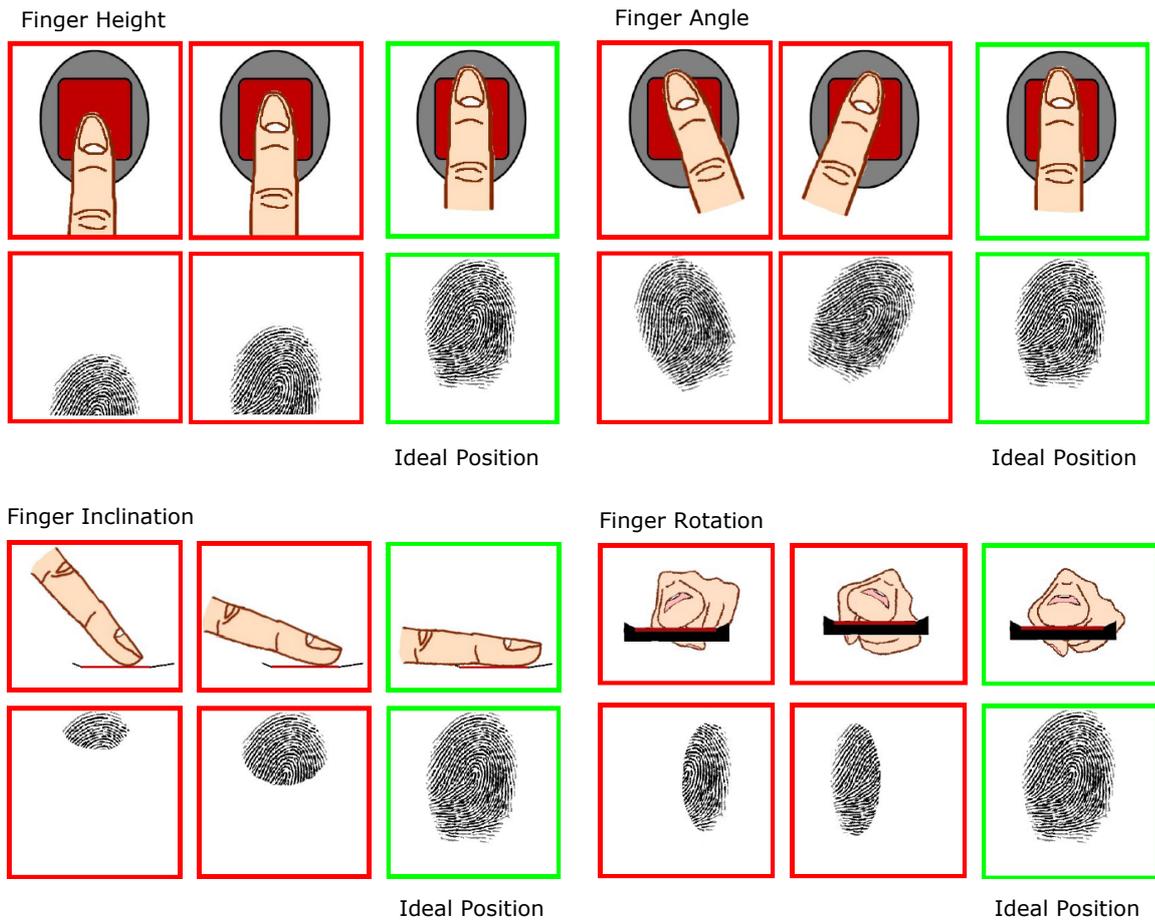
15.9   FAR

The False Acceptance Rate is set to < 0.01 % and currently cannot be altered.

If the application keeps saying 'Press harder' without a finger placed on the reader, it's likely that the glass needs to be cleaned or that there's a bright light shining on the reader. This is not usually a problem unless used in sunlight or the reader is horizontal with a light above which is highlighting tiny bits of dirt on the glass. Although this is not a common issue, in either case, a quick firm wipe down the glass with a finger will usually solve the problem.

16. REMOTE SYSTEM LOCKDOWN

Remote System Lockdown is an optional feature that restricts the user from interacting with the system when an external alarm is triggered. A third-party alarm is wired into the Traka Touch and when triggered, will put the system into 'lockdown'.

This is a standalone Traka Touch feature i.e., does not require TrakaWEB. When in lockdown mode, the system will refuse automated remote login/item release requests from TrakaWEB. No users will be able to gain access to items or system functions until the lockdown has been lifted.

16.1   REQUIREMENTS

- To use the remote system lockdown feature you will require the additional Traka CAN Relay Interface PCB. This additional hardware can be added to your system by a Traka engineer after your initial installation. The feature may then be enabled through Traka Touch. No further software configuration is required.

- An alarm that can be wired into the Traka CAN Relay Interface PCB.

- The alarm must be non-voltage contact.

NOTE: Refer to document TD0083, 'CAN Relay PCB Wiring Guide' for details on pinouts and wiring specifications.

16.2   USING THE SYSTEM

The system can be used as normal until the alarm is activated. On alarm activation, the user interface will display a message informing that system access is currently blocked, preventing the user from logging in.

NOTE: The system will come out of the screensaver or 'idle' mode to go into lockdown.

'System in lockdown mode' is displayed in the default system language and cycles in all other supported languages. This will continue to stay onscreen if the system is in lockdown.

Internal

A message will be present at the top of the screen inside the banner whilst the system is in the state. The message reads 'System Blocked'. This will also be onscreen if the system is in lockdown.

Users already logged in during an alarm condition will still be able to navigate to the admin menu if they have the correct permissions, however when the system lockdown begins item access is instantly removed, therefore if a user is currently at the item selection screen, they will immediately be prevented from removing items, even if they have access to them.

16.2.1 EVENTS

The system will log the appropriate events that can be viewed when running activity reports. The lockdown events will appear as 'System Block Mode' once the alarm has been triggered and 'System Block Mode End' when the alarm has ended.

17. TAMPER SWITCH

A tamper switch is fitted to a Traka Touch Locker System that when activated will display a message on the touch screen and log an event. The message will be displayed in the orange bar at the top of the screen. The system will also sound an alarm whilst the switch is activated.
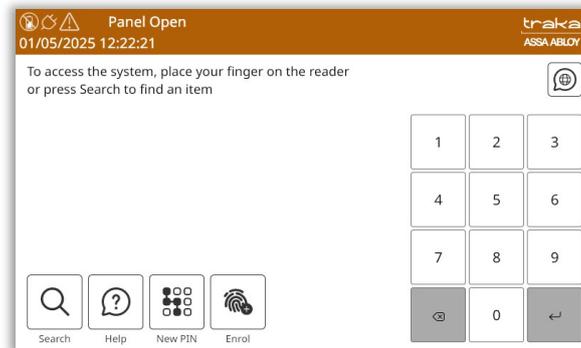
The tamper switch is fitted to the rear of the Control Panel and is activated when the Control Panel is opened. This will return a 'Panel Opened' event and a 'Panel Closed' event once the Control Panel has been closed.

Internal

18. FEATURE OPTIONS

18.1 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 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

18.2 FAULT LOGGING

Fault Logging is a cost option 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, for example 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.

NOTE: For a comprehensive guide to the functionality of the Fault Logging Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

18.3 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.

NOTE: For a comprehensive guide to the functionality of the Reason Logging Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

18.4 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.

NOTE: For a comprehensive guide to the functionality of the Notes Logging Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

18.5   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.

NOTE: For a comprehensive guide to the functionality of the Custom Messages Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

18.6   EMAIL NOTIFICATIONS

The Email Notification System is a cost option feature which 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.

NOTE: For a comprehensive guide to the functionality of the Email Notification Feature Option, please refer to UD0018 – TrakaWEB User Guide.

18.7   ITEM BOOKING

Item Booking is a cost option feature that is created and used within TrakaWEB. Its functionality is derived from the TrakaWEB front end software.

The purpose of Item Booking is to allow items to be reserved for defined periods of time to specific individuals. Typical examples of its functionality could 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 Curfews and Email Notifications. Booking Confirmation Emails are created within TrakaWEB Admin.

NOTE: For a comprehensive guide to the functionality of the Item Booking Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

NOTE: A Traka Touch System will record items as late if a System Lock Out has prevented the return of these items on time.

18.8   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 other staff members throughout the business, but don't want the secondary staff member to have access to the system.

NOTE: For a comprehensive guide to the functionality of the Item Handover Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

18.9   ACCESS SCHEDULES

Access Schedules is a cost option that is used within TrakaWEB to impose time restrictions on Items or Users 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 Items when the schedule is active. Outside of this time, they will have access to no 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 Items in separate Access Schedules to avoid potential confusion.

NOTE: For a comprehensive guide to the functionality of the Access Schedules Feature Option, please refer to UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.

NOTE: If a System Lock Out overruns into the end of an Access Schedule, Traka Touch will allow a User to log in to the system to return an item but will prevent the removal of further items.

18.10 REAL-TIME UPDATE SERVICE

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.

NOTE: For more information regarding the installation and configuration of RTUS, please refer to TD0165 – Real time Update Service Installation Guide.

18.11 ADVANCED FIFO

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 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.**

18.12 ITEM PAIRING & LOCKER PAIRING

Item Pairing and Locker Pairing are powerful security features 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.

Item Pairing 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:

Locker Pairing can be used on Touch systems working in the Fixed Return to Single System (FRSS) mode. It can be setup to function with locker systems as RFID and or non-RFID. This will allow a user to take one or more primary items from separate compartments and automatically be given an item from a secondary compartment. The reverse of this process however is not the case.

For a full overview of Item Pairing & Locker Pairing, please refer to **UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.**

18.13 ALLOWANCE ACROSS SYSTEMS (AAS)

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 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. The feature will also be dependent on the Advanced First in/First Out functionality for fixed return systems.

A configuration will be required to enable the Allowance Across Systems feature which can be obtained from Traka.

For a full overview of Allowance Across Systems, refer to **UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.**

18.14 MULTIPLE CREDENTIALS

Multiple Credentials is a non-cost feature, which was created to provide organisations with the ability to assign multiple/different types of credentials against single users. Multiple Credentials was designed to work alongside an Access Control System (PACS) where credentials in different forms can be accepted, i.e. Cardholder and Mobile Credential, or multiple different cards where PACS controls access to different areas.

A configuration will be required to enable the Multiple Credentials feature which can be obtained from Traka.

For a full overview of Multiple Credentials, refer to **UD0260 – TrakaWEB Version 4 User Guide.**

NOTE: Multiple Credentials is not supported directly on 16bit systems. However, it is possible to mix a single credential system with a multiple credentials system via TrakaWEB.

19. MULTIPLE USER LOCKER ACCESS

The Multiple User Locker Access functionality enables more than one user to access a locker compartment without having to wait for a previous user to complete their activity and log out to allow another user to access the system. This allows the locker system to be used more quickly and efficiently but will only function for users who have only been granted access to a single locker compartment. A configuration change will be required to enable the feature which can be obtained from Traka.

Multiple User Locker Access is not compatible with the following:

- Reason Logging
- Custom Messages
- Notes Logging
- Fault Logging
- Fuel Logging
- Distance Logging
- Location Logging
- Item Booking
- First In First Out Mode
- Advanced FIFO
- Docksafe
- Temporary Deposit Lockers
- Item Handover
- Item Booking Type
- Random Return to Multiple Systems
- Random Return to Single Systems
- Faulty Item Exchange
- Item Release Default Screen: Always Use Menu Screen
- Item Release Default Screen: Always Use 'I Need to Search' Screen

NOTE: Multiple User Locker Access will not support RFID Lockers

NOTE: This feature will be available on Linux systems running future versions of the Traka Touch Application.

Internal

19.1.1 USING MULTIPLE USER LOCKER ACCESS

1. Log into the system using either card reader, keypad, or fingerprint.
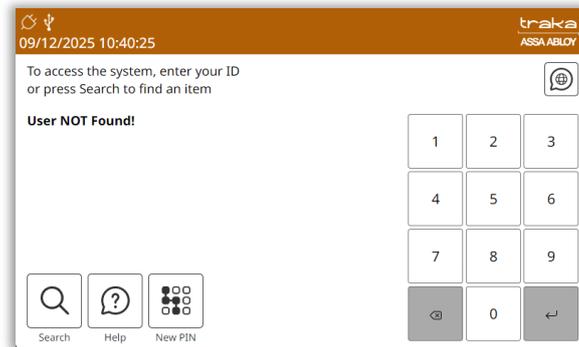
A message will appear on the screen, and the locker door will automatically open.
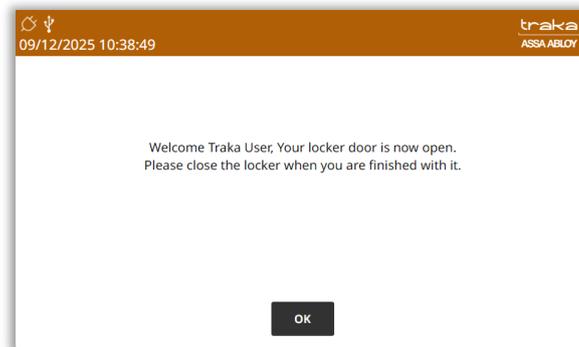
NOTE: This will only apply to users that have been granted access to a single locker compartment. There is no behavior change for a user with multiple door access, and they will be presented with the 'I Know What I Want' option.

2. Select the **OK** button to clear the message and remove or return the item as required.

NOTE: A user with single door access will be automatically logged out after 5 seconds regardless of the door status.

If another user logs into the system with access to the same compartment whilst the door is open, they will be presented with the following message:
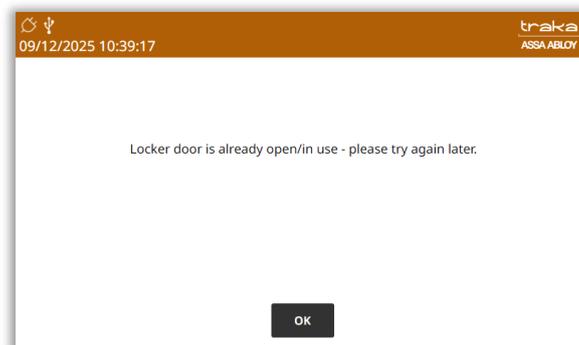
A door open/closed event will be generated as normal in TrakaWEB and the logged in username will be recorded for these events. If a locker door is left open and the door timer elapses, then no username will be recorded as it is possible that another user may close the door.

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.

Should the Emergency Open option be activated and 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.

For more information on email notifications and enabling the Emergency Open option in TrakaWEB, please refer to **UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.**

NOTE: The Emergency Open feature can still be used during a System Lock Out, but App functionality will not be available until the System Lock Out has ended.

20.1   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:
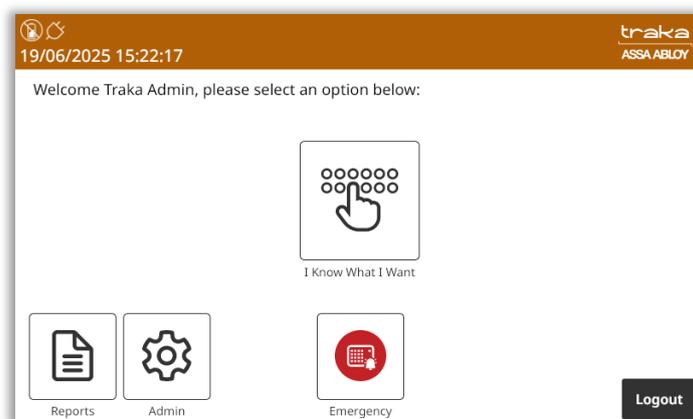
1.   Next, select the Emergency icon- on the Touch screen. All the doors to the Locker system will now open sequentially.

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.
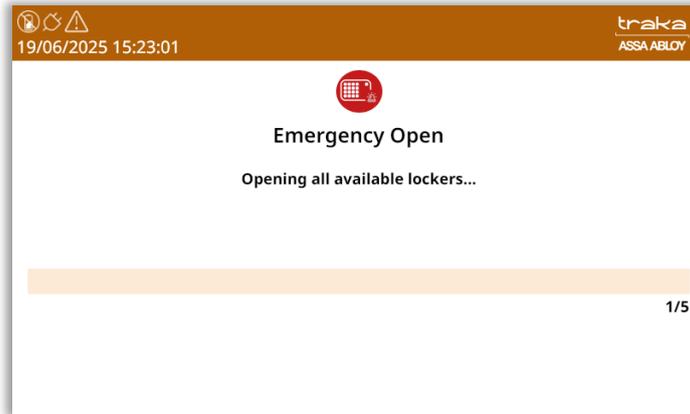
You will now be taken to the 'I Know What I Want' screen. Here you will be shown all the items currently in the system and their status. The item icons will change as the items are removed from the system.

NOTE: Closing all the doors at this stage will automatically log you out and return to the main login screen.
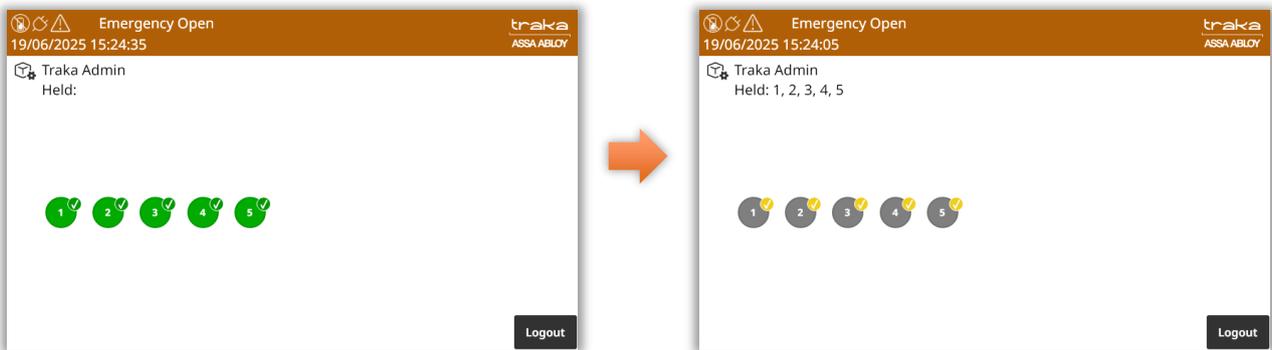
If you choose to select the Logout button on the screen without first closing all the doors, you will still remain logged in until all the doors have been closed as detailed below.

2. Select the **Logout** button to exit.

Internal
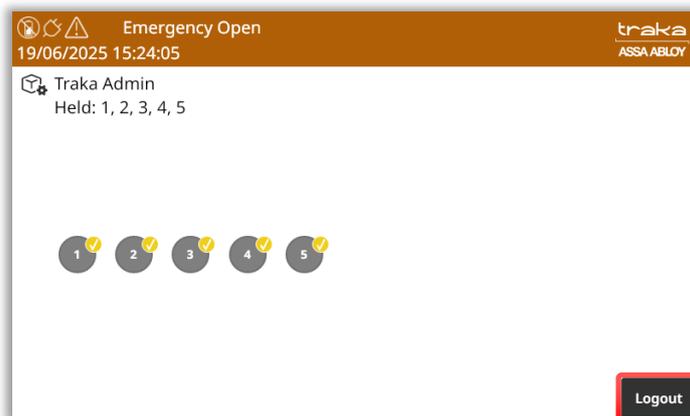
If 1 or more doors remain open, you will not be fully logged out and you will see the following screen indicating which doors remain open:
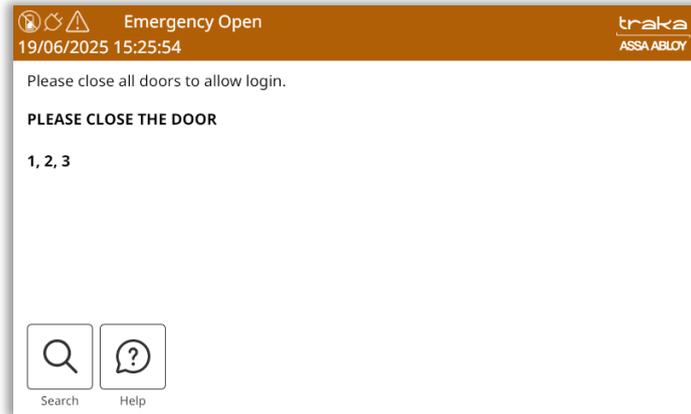
NOTE: The Emergency Open message will continue to display on the screen if one or more doors remain open and the configured auto-logout timeout will not apply.

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.
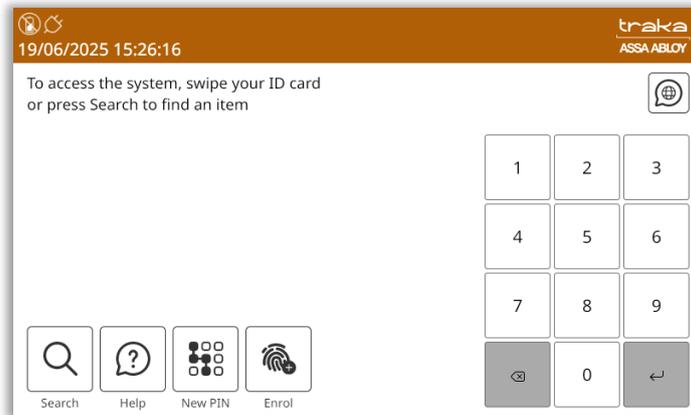
20.2 EMERGENCY OPEN WITH FAULT LOGGING

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.	Description	Status
🚫	1		In System
ⓘ	2		Out Of System
✏️	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.

Internal

2. Select the **Emergency** icon on the Touch screen.
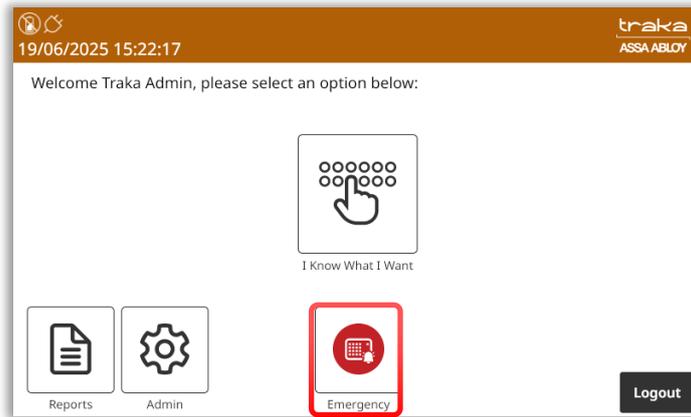
The doors will now open sequentially as described previously except any doors to compartments containing items with critical faults.

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.
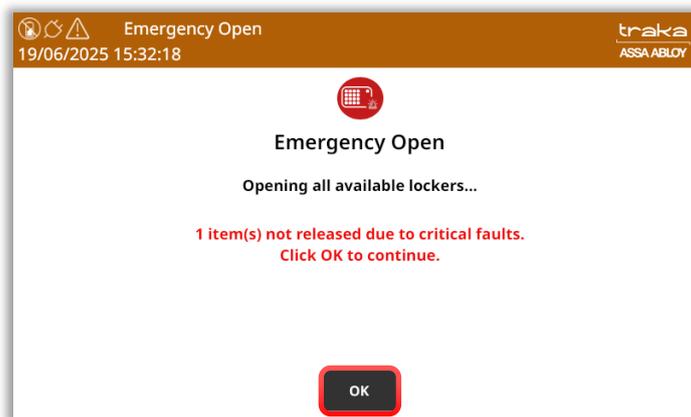
A user with the Fault Logging Admin role will be able to select the item from the touch screen.

4. Select the item with the critical fault.
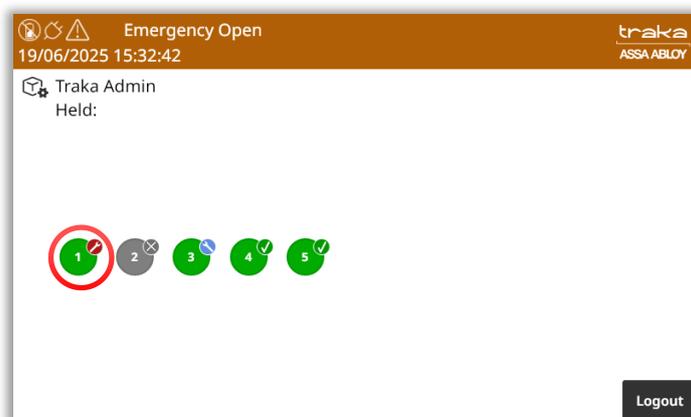
At the next screen, you will be required to acknowledge that the item has a critical fault.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

5. Select the **Continue** button to accept the critical fault.
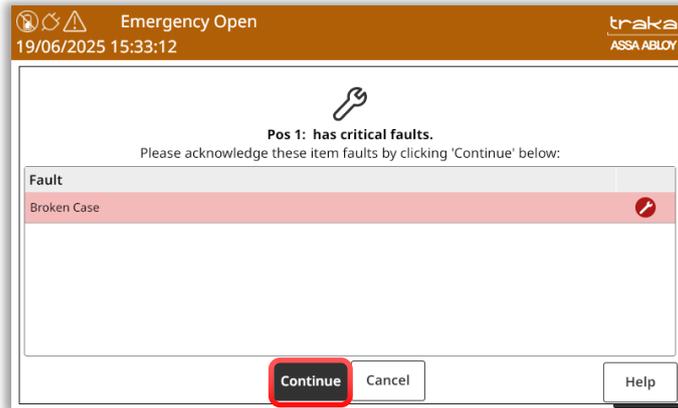
The door will now open allowing access to the item with the critical fault.

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.

20.3   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.**
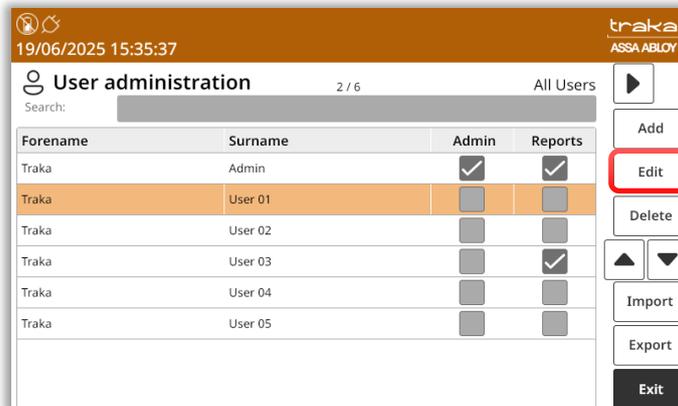
2. At the next screen, select the **Roles** button.
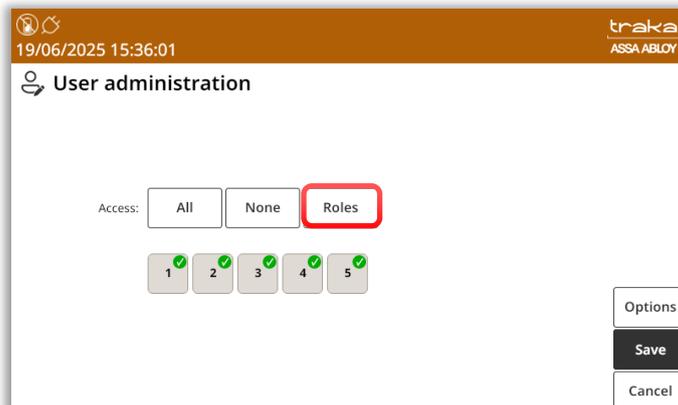
A new window will appear displaying a list of roles.

3. Navigate through the list and select the **Emergency Open** role. The icon will change to a tick as shown below.
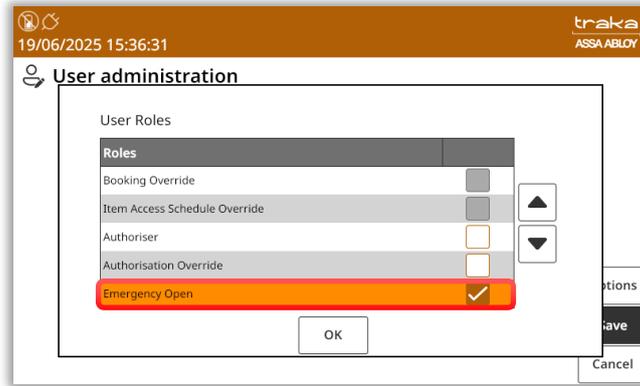
4. Once completed, select **OK** and then **Save** and **Exit.**

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.
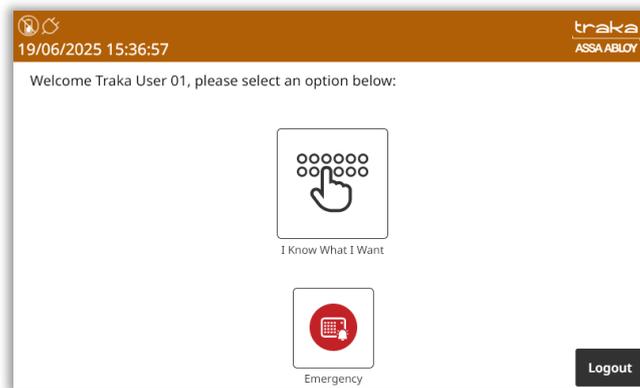
20.4 REPORTS

Events will be recorded anytime the Emergency Open feature is activated and deactivated. Events can be seen in Reports within TrakaWEB. For more information, refer to **UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.**

21. REMOTE EMERGENCY OPEN ALL DOORS ON ALL LOCKERS.

The Remote Emergency Open All Doors on All Lockers feature will enable all the doors on all lockers to be opened by toggling the trigger input on and off on the iMX6 Control Board.

The corresponding trigger points for each system are located in the Operations Room which when pressed will give the signal to release all the doors of each system respectively.

21.1   OPERATION

Once the trigger input has been toggled on, the Traka Touch system will wake up.
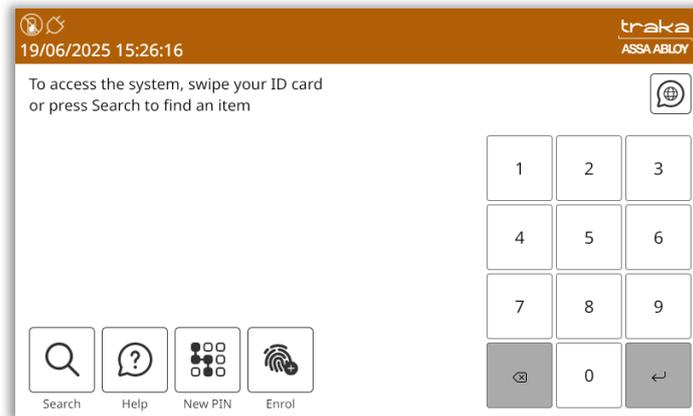
The Emergency Open screen will then be displayed and all the doors to the chosen locker system will automatically open. A Flashing **Emergency Open** message will also be displayed at the top of the screen.
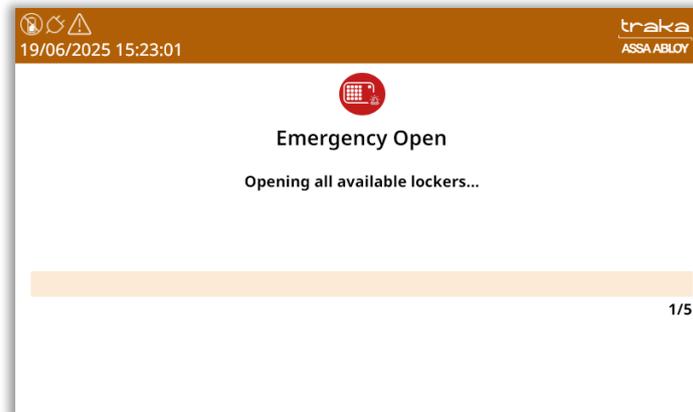
Once all the doors have opened, you will be taken to the **I Know What I Want** screen. Here you will see all the items available in the system and their current status.
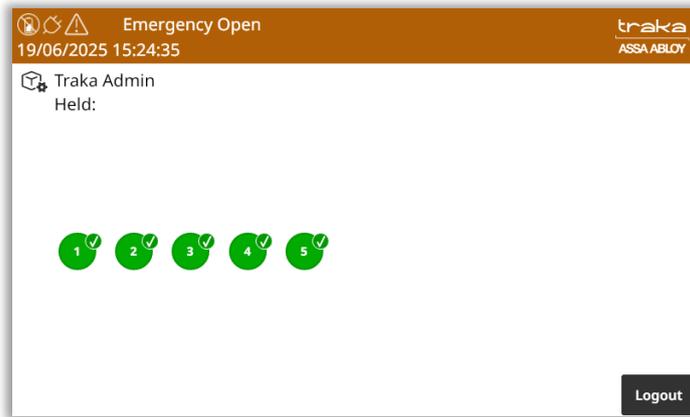
The item icons will change as items are removed from the system.
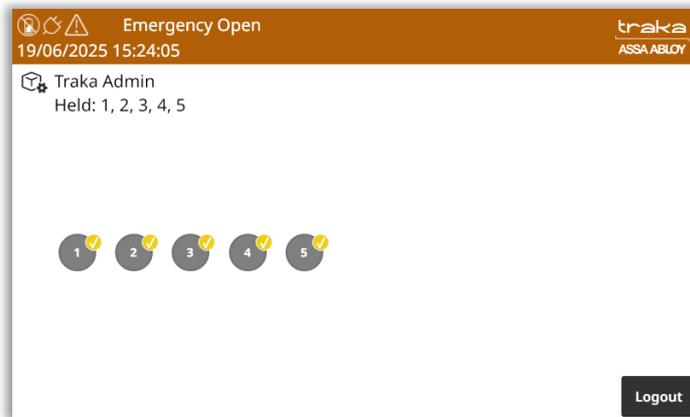
Once all the doors have been closed the system will still remain in Emergency Open mode, and any doors may be reopened by selecting a locker position from the Traka Touch screen.

The system will remain in Emergency Open until all the doors have been closed and the trigger input is toggled off. The system will then return to the login screen.
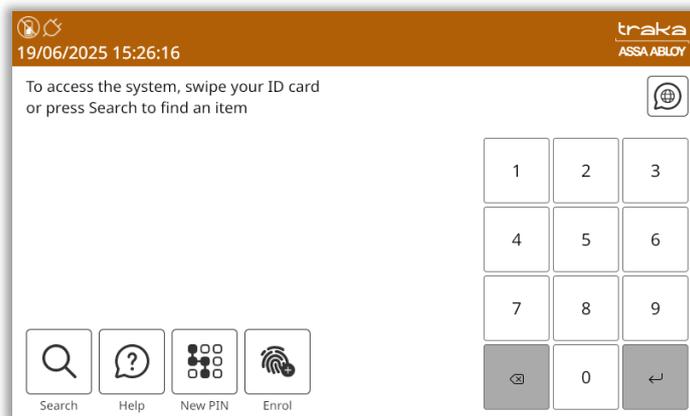
NOTE: Any user logged into the system when Emergency Open is activated will be automatically logged out.

21.2 EMERGENCY OPEN WITH FAULT LOGGING

When Fault Logging is enabled on the Locker system and the Emergency Open has been activated, the compartment doors to any items that have critical faults against them will not automatically open.

A message will appear on the screen informing you of how many items were not released due to having critical faults.
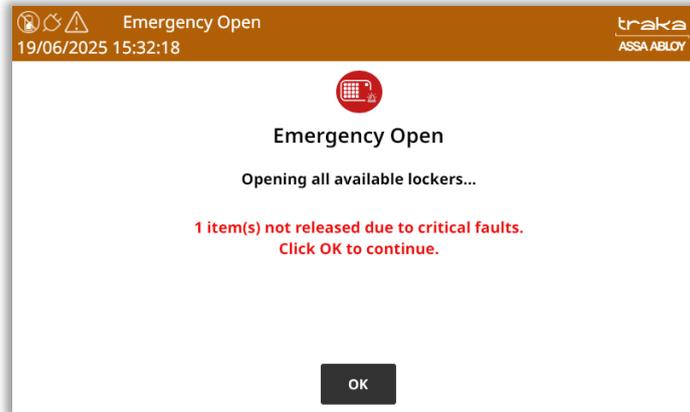
After selecting **OK**, you will be taken to the **I Know What I Want** screen where you will see all the available items and their current status including items with critical and non-critical faults and any items currently out of the system.
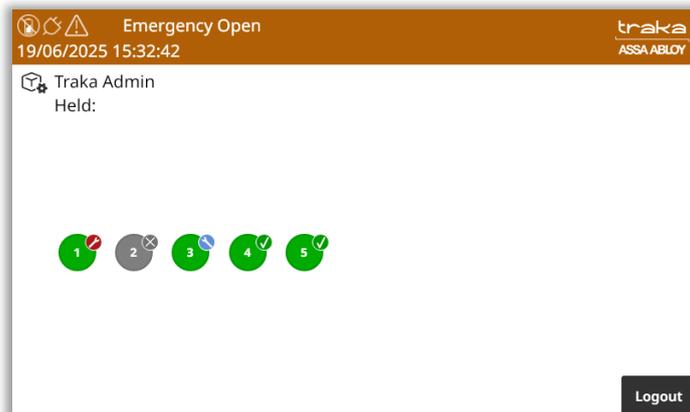
A predefined user is assigned by default who will be able to select items with critical faults from the touch screen. As the user is predefined, they cannot be changed.

At the next screen, you will be required to acknowledge that the item has a critical fault.

Internal
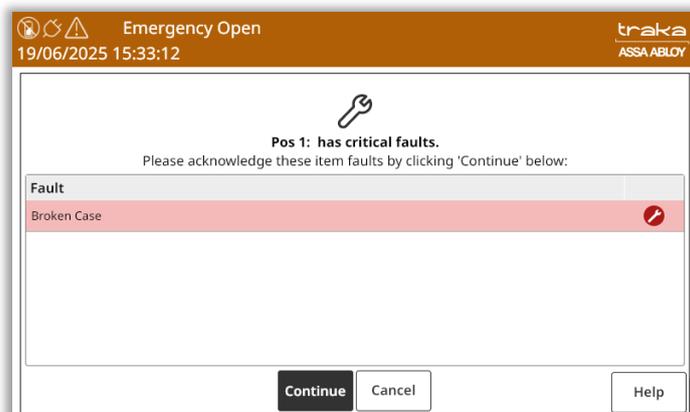
Select **Continue** and the item will be released. The system will remain in Emergency Open mode, and you may choose to reopen any doors that have been closed.

The system will remain in Emergency Open until all the doors have been closed and the trigger input is toggled off. The system will then return to the login screen.

NOTE: Any events during a remote release will not be logged against a user due to the nature of the Remote Release functionality.

Internal

22.1   CLEANING GUIDANCE

With the current situation regarding the Coronavirus (Covid-19) outbreak, it is important to take precautionary measures focused on sanitisation. Where contact with multi-user systems is unavoidable, always wash hands thoroughly after use with antibacterial soap, handwash, gel or wipes. Ensure that wipes are disposed of accordingly and avoid contact of your face with your hands during operation.

This guide will assist you with the necessary requirements for cleaning your Traka systems to help reduce the spread of any viruses and ensure that they continue to function correctly.

NOTE: Do not use the Traka Locker with wet hands as this may damage the touch screen.

22.1.1 CLEANING PROCEDURE FOR TRAKA LOCKER

- Use a soft lint-free or microfibre cloth
- The cloth may be lightly dampened with a mild cleaner and water or Ethanol
- Never use acidic or alkaline cleaners
- Use of incorrect cleaners may result in damage to the surface
- Be sure the cloth is only lightly dampened and not wet
- Never apply cleaner directly to any surface
- Wipe surfaces gently. If there is a directional surface texture, wipe in the same direction as the texture
- Soak up any spilled or excess cleaner with an absorbent cloth immediately

NOTE: Ensure that users wash their hands thoroughly after use.

22.1.2 CLEANING THE TOUCH SCREEN

The Traka Touch screen by design, is a sensitive electronic device and therefore, extra care should be taken when cleaning.

- Never apply cleaning solution to the Touch screen directly
- Use a soft lint-free or microfibre cloth
- The cloth may be lightly dampened with a mild cleaner or Ethanol
- Never use acidic or alkaline cleaners
- Use of incorrect cleaners may result in damage to the Touch screen
- Lightly dampen the cloth and then apply the cloth to the screen
- Be sure the cloth is only lightly dampened and not wet
- Do not allow excess liquid to seep into the edges of the Touch screen
- If cleaner is spilled onto the screen, soak it up immediately with an absorbent cloth

NOTE: Ensure that users wash their hands thoroughly after use.

22.1.3 ITEMS

Generally, Items will be handled by many users. Whilst this is unavoidable, it is strongly advised that all users wash their hands thoroughly after use.

22.1.4 WARRANTY STATEMENT

Failure to comply with these cleaning instructions could damage the Traka unit and may invalidate the product warranty with any resolution of issues being chargeable.

NOTE: Traka cannot make a determination of the effectiveness of a given disinfectant product in fighting pathogens, such as COVID-19. Please refer to your local public health authority's guidance on how to stay safe from potential infection.

22.2 POWERING ON/OFF THE SYSTEM

Disconnecting the system directly from the mains could result in data loss and should only be done in an emergency. Therefore, to safely switch off the system and prevent any data loss follow the steps below:

To power on/off the system you will need to gain access to the Traka Touch PCB located on the back of the Control Panel. For information on accessing the Control Panel please refer to the section **Opening the Control Panel**.

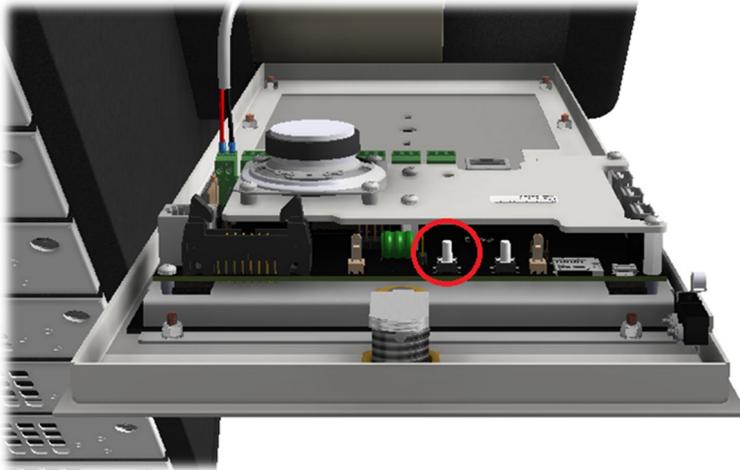1. To power **Off** the system press and hold the button highlighted below for 5 seconds.

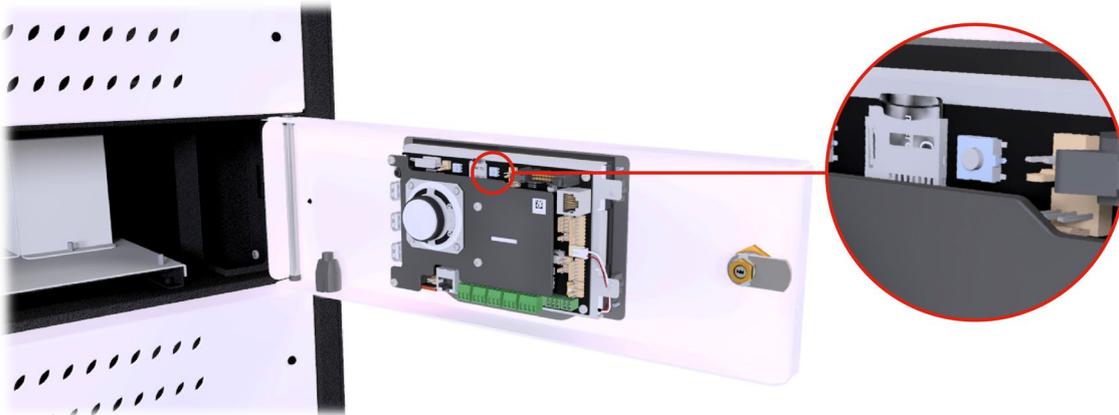**Figure 4 – Power Button on iMX28 in the Traka Touch Modular Locker**

Figure 5 – Power Button on iMX6 in the Traka Touch Capacitive Screen Laptop Locker

2. To power **On** the system simply press this button once.

22.3 MANUALLY OPENING DOORS

In the case of a total power failure including the backup battery, you may need to manually open the locker compartment doors to access the items. Each Traka Touch Locker System is supplied with a manual override key to enable you to open each locker compartment. Simply insert the key into the lock of the desired compartment and turn anti-clockwise and the door will pop open.

NOTE: Traka recommends that override keys are not stored inside a locker compartment.

22.4 REPLACING ITEMS

From time to time, you will be required to replace an item that may have become lost or damaged. If your system is a Non-RFID system, simply remove the item from the compartment and replace it.

If your system is an RFID system, each item will have been fitted with an RFID tag. In most cases this tag will not be removable from the existing item and therefore a new tag will need to be fitted to the replacement item before it can be allocated to the compartment. For more information on RFID tagging see the 'RFID Tagging' section.

The Traka Touch RFID Locker System works on fixed item replacement basis which means items must be returned to the compartments from where they were taken. By default, the system will not know where an item should go therefore the serial number of the RFID tag must be associated with the position in the system.

1. Identify yourself to the Traka System by entering your PIN or swiping your Card.

NOTE: The user must be an administrator and have access to the required compartment.

2. Select the '**I Know What I Want'** button (if applicable).

3. The touch screen will now show you all the items in the system. Select the appropriate compartment number on the screen by clicking the green symbol and the compartment door will open.

Internal

4. Insert the new item into the compartment. The system will start to alarm warning you that the item is not recognised, ignore this message, and close the door.

NOTE: If you have multiple items that need to be replaced then repeat steps 1 to 4 for each of them before moving on to step 5.

5. Identify yourself once again at the Traka System by entering your PIN or swiping your Card and then select the **Admin** button.

6. You will then be taken to the Administration screen. Click the **Items** button.

7. The item list will then display the new item(s) status as 'unrecognised'. Select the **Setup** button.

8. You will be asked if you wish to setup all items, click the **Yes** button.

Internal
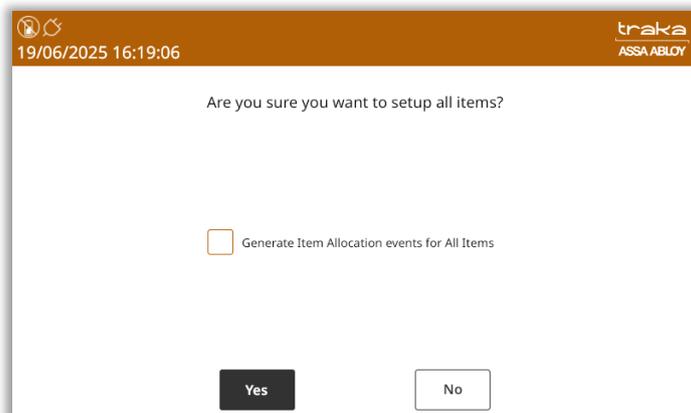
9. A message will appear asking you whether you wish to setup or replace the item(s) you removed with the new item(s), click the **Replace** button.
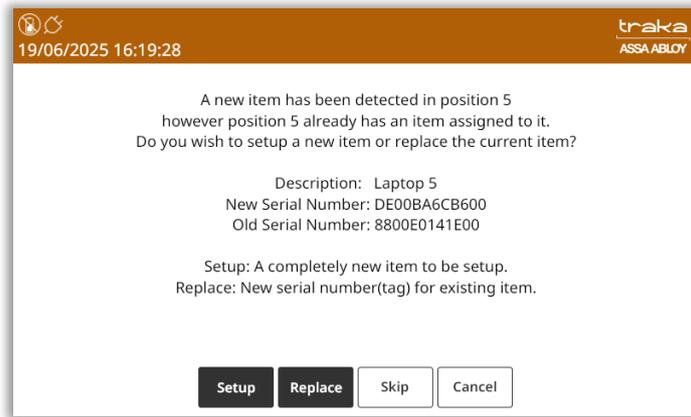
10. The item list will now begin to re-populate adding the new item(s). This progress is displayed via the small orange progress bar in the top right corner of the window.

11. Click the **Exit** button to be taken back to the administration menu, and from there click the **Exit** button again to return back to the regular login screen.

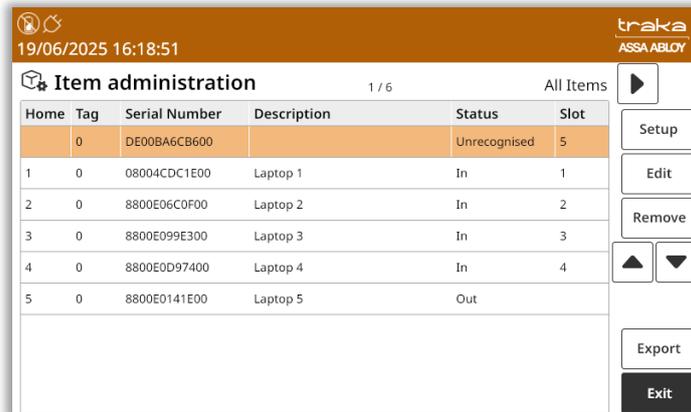12. Identify yourself once again at the Traka System by entering your Keypad ID or swiping your Card.

13. Select the '**I Know What I Want**' button if applicable.

14. The Touch Screen will now show you all the items in the system. Ensure the item(s) you replaced now have the 'Item in System' symbol and can be removed.

Internal

Traka Lockers can be designed in various ways to suit the customers' requirements. As a result, the process for opening the control panel may differ slightly between systems. However, the Control Electronics will always be locked behind the panel containing the touch screen. The following describes the process for opening the Control Panel on the most common Control Pod design.

NOTE: If your system design is different to the one described below and you are unsure of how to open the Control Panel, please contact Traka using the contact details on the last page of this document.

Every Traka Touch Locker System is supplied with 2 Master keys used for accessing the Control Panel.

1.   Insert the Master key into the Cam Lock on the Control Panel.

2.   Whilst supporting the Control Panel, turn the key 90° clockwise. Take care at this point as the control panel will start to tilt forward.

3.   Carefully tilt the Control Panel forward and it will rest on the restraining cable.

Internal

Other types of Lockers might have the Control Panel located in one of the locker compartments. If that is the case, you will only need to insert the Master key in that compartment's lock and open the door.

Opening the Control Panel gains access to the Control Electronics for the system. This may be required for various reasons including accessing the USB ports, and locating the Serial Number/Rating Plate. To locate the position of the USB ports and other features on the PCB see the 'Traka Touch PCB' section.

22.6   SERIAL NUMBER/RATING PLATE LOCATION

Every Traka System has a Serial Number/Rating Plate label attached. This label contains not only the unique serial number of the system but also electrical information.

In some scenarios it may be necessary to access this label. Traka Lockers can be designed in various ways which means the exact location of the rating plate may differ between systems.

Please note, that the following graphical symbols, that are found on or inside the Touch system, have the following meanings:

   Indicates that caution is needed when operating or performing any work on the Touch system.

   Indicates that there is a risk of electric shock.

   Indicates that the operating instructions should be considered when operating the Touch system.

Internal

22.6.1 RESISTIVE SCREEN LOCKERS

In principle, the location of the rating plate will be behind the Control Panel. For more details on opening the Control Panel see the previous section 'Opening the Control Panel'.

22.6.2 CAPACITIVE SCREEN LOCKERS

In all the locker models equipped with the Capacitive Screen, the rating plate is located on top of a locker, near its back edge.

22.7 REPLACING THE BACKUP BATTERY

Traka provide a backup battery already connected with every Touch System supplied in the UK. The backup battery is kept charged by the system when running from the mains so that it is ready to be used should the power fail.

The service life of the battery is typically 5 years. Should the battery require replacing, then it is important that it is replaced with the correct type.

22.7.1 BATTERY SPECIFICATION

Traka recommends the following battery for the Traka Touch Locker System:

- 12V, 7AH Valve Regulated Lead Acid Battery approved for IEC 61056-1 or equivalent.

22.7.2 BATTERY LOCATION

The location of the battery can vary depending on the design of your system, however in most cases it will be located inside the Control Pod. Please consult your system drawing or installation document for more details. If you are unsure, please contact Traka or your distributor using the technical support details on the last page of this document.

The following process explains how to access the Battery if it is located inside the Control Pod.

1. Open the Control Panel using the Master Key. For more details on how to open the Control Panel refer to the section **Opening the Control Panel**.

2. The Battery will be located in the bottom of the control Pod.

Internal

Other types of Lockers might have the Battery located behind the Control Panel in one of the locker compartments. If that is the case, you will only need to insert the Master key in that compartment's lock and open the door.

The battery will be secured with a bracket. You will need a 7mm nut spinner / Ratchet to remove the bracket.
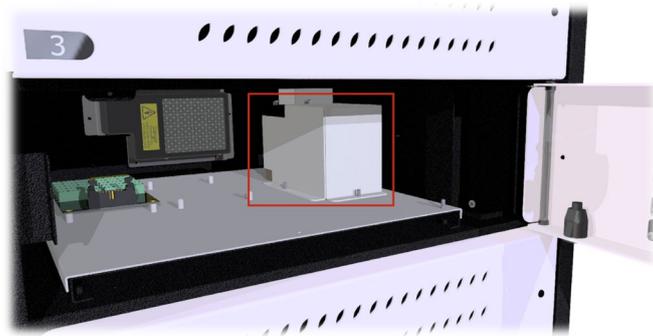

For connection/disconnection of the Battery please refer to the **Battery Connection Details** section below.

22.7.3 BATTERY CONNECTION DETAILS

The following diagram shows the connection details for the Traka Touch Backup Battery.

For Battery disconnection, carefully disconnect the spade connectors from the battery.

WARNING: Never disconnect the wires from the green connector whilst the cable is still connected to the battery terminals.

Red wire to **Red** Battery Terminal (+)
Black wire to **Black** Battery Terminal (-)

Black wire to (-)
Red wire to (+)

(-)
(+)
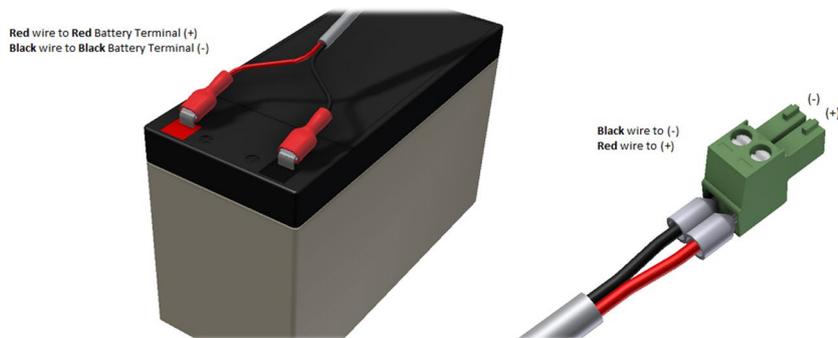
NOTE: Ensure that the spade connectors are pushed fully onto the battery terminals. It is recommended that insulation tape is wrapped around the battery to fully cover any exposed parts of the battery terminals.

22.8   TRAKA TOUCH SOUND MASKING LOCKER – CALIBRATION

The level of sound masking is governed by the controller which is located in the compartment behind the touch screen.

Level 15 has been pre-set at the factory, but as different environments can impact on the effectiveness of the system, we recommend that the system is re-calibrated before putting into service.

The arrow indicator on the left (**C**) when pressed enables control of the sound masking volumes for the 12 compartments to the left of the controller and the 1 compartment immediately above.

The arrow indicator on the right (**D**) when pressed enables control of the sound masking volumes for the 12 compartments to the right of the controller and the 4 compartments immediately below.

The arrow indicators top and bottom will increase (**A**) or decrease (**B**) the sound masking volume for whichever of the two compartment groups selected from above.

Either one of the compartment groups (**C**) or (**D**) can have their sound masking volumes increased or decreased, or even switched of (0 volume selected) without effecting the other group.

22.8.1 SOUND MASKING CALIBRATION CHECK

1. Turn the sound masking system **ON.**

2. Place a recording device in any compartment in compartment group (**C**) by opening a compartment via the touch screen. Make sure that the microphone does not make contact with compartment sides or door. Also ensure that the microphone is not obstructed or covered in any way.

3. Activate the record function on the device and close the compartment door.

As a general rule, stand 1-2 metres from the compartment door and speak normally for about 10 seconds.

The effectiveness of the sound masking can be improved by standing closer to the Sound Masking Locker whilst talking and calibrating the system by increasing the up arrow (**A**) value until no talking can be heard on the recording device.

4. Open the compartment door, remove the device and play the recording.

If the recording is audible press the Up arrow (**A**) on the controller to a higher value.

NOTE: Traka suggest a value increase of 2 between checks.

5. Repeat the above process until an inaudible recording is made.

IMPORTANT: Changing the sound masking volume for compartment group (C) DOES NOT automatically change the sound masking in compartment group (D). The same calibration process will need to be applied to the compartment group (D).

22.8.2 DAY-TO-DAY FUNCTIONALITY

To activate the sound masking functionality, simply turn the key operated switch, which has a white surround, that is mounted on the control pod door, to the **ON** position and then remove the key*.*

Once the switch has been activated all the selected individual sound masking speakers, one in each compartment, will be activated.

When the sound masking functionality is not required, its **ON/OFF** switch should be turned to the **OFF** position.

The day-to-day functionality of the SML will not be affected by the sound masking function being turned ON or OFF.
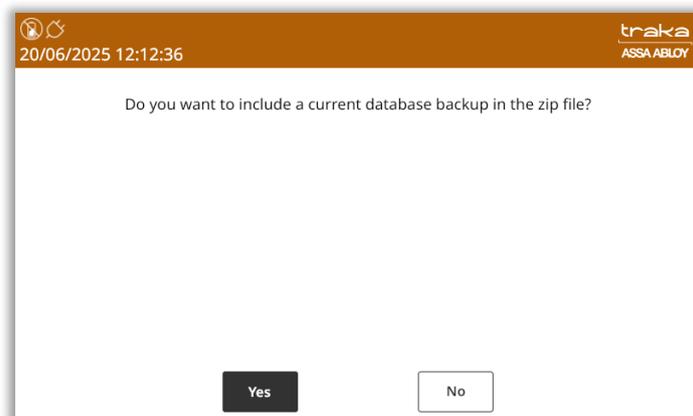
NOTE: Traka would strongly recommend that a responsible person holds and manages the key to the sound masking ON/OFF control switch.

1.   From the Admin menu select the Application diagnostic followed by **Export App Log File to USB**.
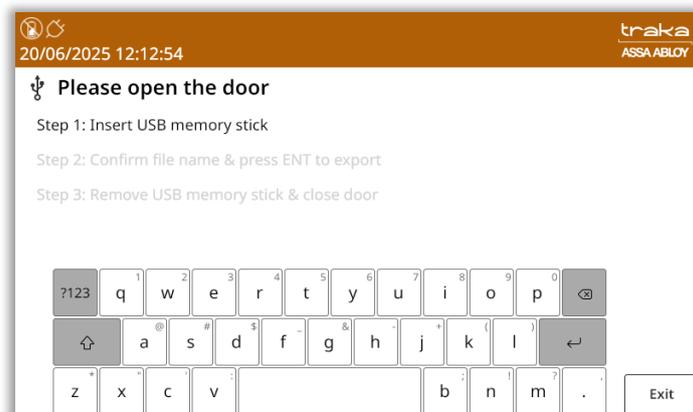

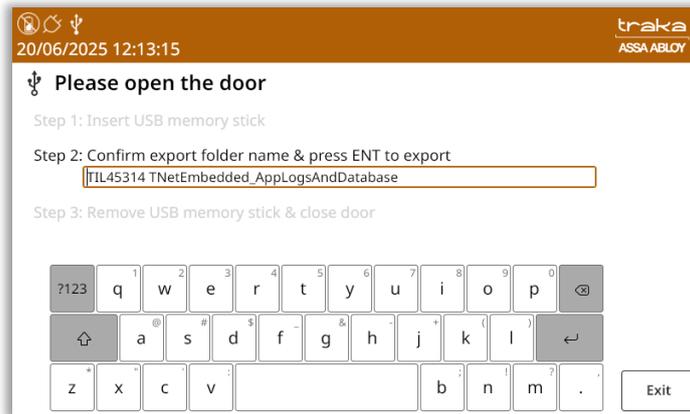You will then be asked if you want to include a current database backup in the zip file.

2.   Select **Yes** to continue.

The door will then pop open, and you will be required to insert a USB memory stick.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

You can rename the database file if required, by using the provided keyboard.

If required, you can then enter an optional password to protect the archive.

Once complete, press the Ent button to export the files.

22.10 REPLACING THE USB CHARGING CABLE

If your system has fly lead charging it is possible to replace the charging lead should a fault occur or if a different charging lead is required. The compartment is designed in a way that makes the replacement of a charger lead possible from the inside.

Internal

1. Power off the Locker system before starting any work. Open the compartment door, refer to Section 20.3 for more information. Disconnect the charger lead and remove the tablet device inside.
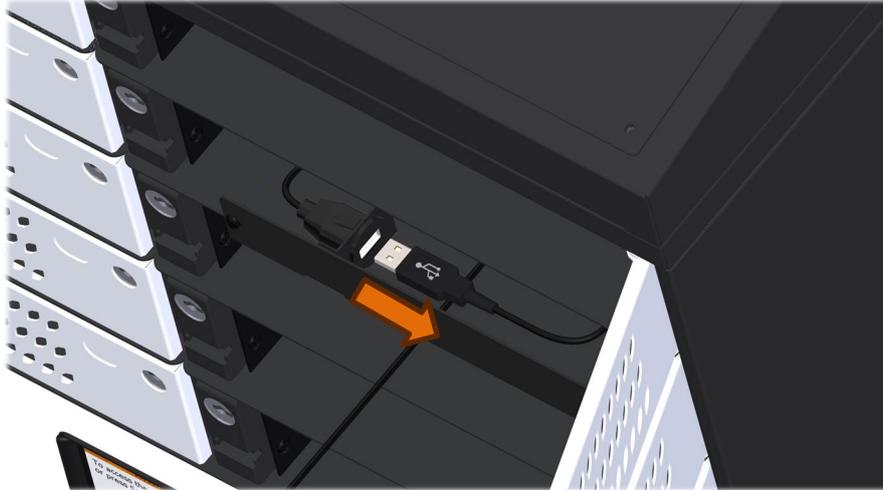

2. The charger lead is connected to a USB socket mounted on the rear of the access panel on the front face of the tablet shelf. Remove the 2 screws securing the access panel.
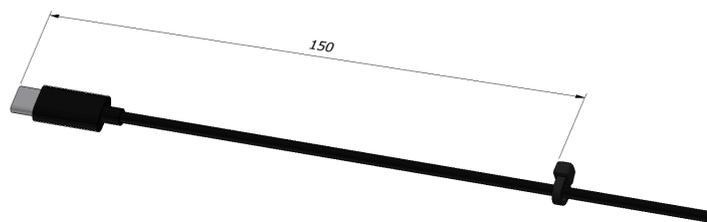

3. Remove the access panel together with the USB socket from the front of the shelf. Be careful not to damage the USB socket or its cable.
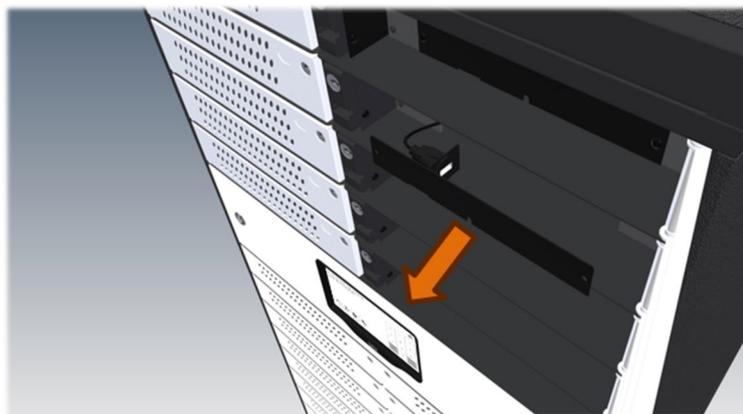
4. Disconnect the old charging lead from the USB socket.

5. Attach a cable tie onto the new USB cable to prevent the cable from being pulled out, when on place.

6. Replace the USB cable with the new one, with the cable tie sitting behind the access panel.
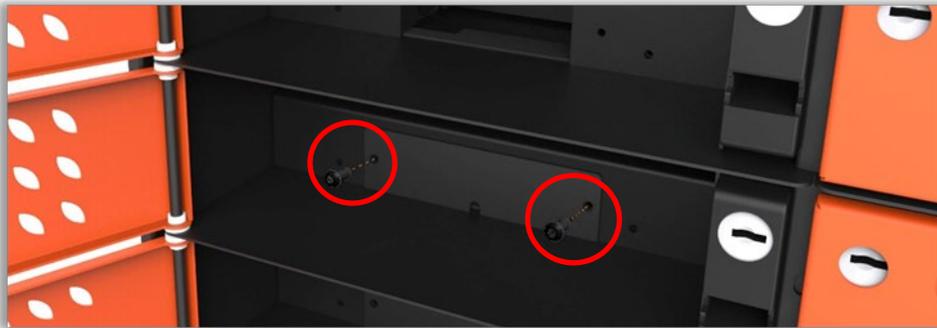

7. Re install all parts removed.

8. Return the tablet to the compartment and connect the charging lead. Power on the Locker and ensure that the tablet begins to charge and then close the compartment door.

22.10.2 REPLACING THE USB CHARGING CABLE WITH A SERIAL NUMBER OF TIL18686 OR LOWER
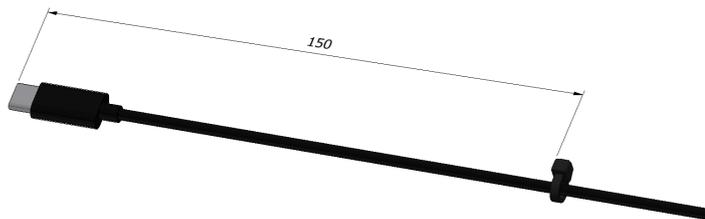
1. Power off the Locker system before starting any work. Open the compartment door, refer to the Manually Opening Doors Section for more information. Disconnect the charger lead and remove the tablet device inside.
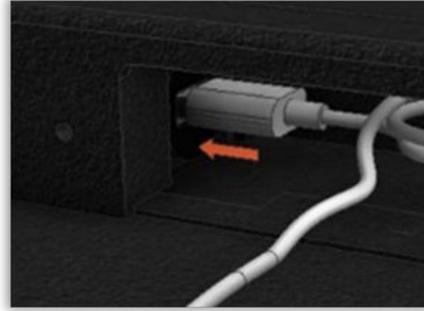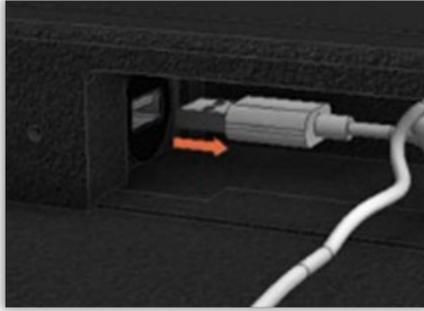

2. The charger lead is connected to a USB socket situated behind the access panel on the front face of the tablet shelf. Remove the 2 screws and remove the access panel.

9. Attach a cable tie onto the new USB cable to prevent the cable from being pulled out, when in place.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"

Internal

10. Disconnect the charger lead from the USB socket and replace with the new one.

11. Coil up and cable-tie any excess cable, making sure enough length remains to connect to the tablet once in position.

12. Refit the access panel and replace the 2 screws, making sure the cable tie is sitting behind the access panel.

13. Return the tablet to the compartment and connect the charging lead. Power on the locker and ensure that the tablet begins to charge and then close the compartment door.

Internal

23. PRODUCT DISCONNECTION

23.1   MAINS DISCONNECTION

To completely disconnect the system from the mains supply, follow the steps below:

- If the Traka Power Supply is connected to a non-switched fused spur, remove the fuse from the spur.
- If the Traka Power Supply is wired to a plug and connected to a power outlet outside of the system, disconnect the plug from the power outlet.
- If the Traka Power Supply is wired to a plug and connected to a socket in a power bar inside the lockers, disconnect the power bar as explained in the following points.
- If the system is fitted with a single or multiple power bars and wired to a BS60309-2 'Commando' plug, disconnect all commando plugs from the sockets.
- If the system is fitted with a single or multiple power bars and connected to non-switched fused spurs, remove the fuses from the spurs.
- If the system is fitted with a single or multiple power bars that are wired to plugs and connected to power outlets, disconnect the plugs from the power outlets.
- In the case of a battery being fitted there are two power sources to disconnect before any service or maintenance work is carried out.

NOTE: To safely power down and prevent the risk of data loss the system must be switched off as described in the Powering On/Off the System section. Only disconnect directly from the mains in an emergency.

23.2   BATTERY DISCONNECTION

The battery is connected to the Traka Touch PCB on the back of the control panel.

For Battery disconnection, carefully disconnect the connector from the Traka Touch PCB.

WARNING: Never disconnect the wires from the green connector whilst the cable is still connected to the battery terminals.
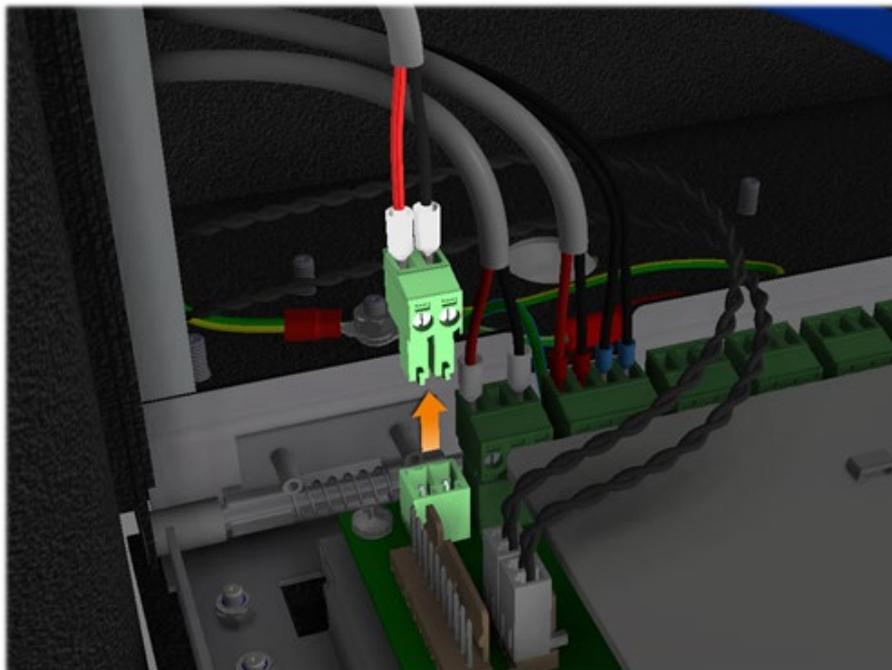
24. TECHNICAL SUPPORT

If you need to contact Traka/distributor for technical support, navigate to the Help section at the main screen and provide the following details:-

- Support Code

- Cabinet Serial Number

- App Version

- SQL CE DB Version

- CB FW Version

- DV FW Version

Technical Support Information

UK Telephone: **0333 355 3641**

International Telephone: **+44 333 355 3641**

Email: **support@traka.com**

Web: **support.traka.com**

25. END USER LICENCE AGREEMENT – SOFTWARE

Please refer to the policies section of the Traka web site for the most up-to-date information concerning Traka's software EULA:

https://www.traka.com/global/en/about/policies