TRAKA TOUCH PRO GETTING STARTED GUIDE

UD0259

23/10/24

VERSION 1.3

CONTENTS

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

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:	**+31 10 2570010**
Support Tel:	**+44 (0)1234 943900**
Contact Email	**info@traka.nl**

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. PRODUCT DETAILS

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

3.1 ELECTRICAL RATING

3.1.1 TRAKA TOUCH PRO SERIES

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

3.2 BATTERY BACKUP:

- Touch Pro V, M, S & L – DC12v 7Ah

3.3 WEIGHT:

- Touch Pro V:
  20Kg (this weight includes 5 iFobs with no keys)
- Touch Pro M:
  25Kg (this weight includes all the receptor strip and 40 iFobs with no keys)
  20Kg (this weight is when the receptor frame, frame side and top covers removed) *****
- Touch Pro S:
  42Kg (this weight includes all the receptor strip and 120 iFobs with no keys)
  30Kg (this weight is when the receptor frame, frame side and top covers removed) *****
- Touch Pro L:
  99Kg (this weight includes all the receptor strips and 360 iFobs with no keys)
  58Kg (this weight is when all three receptor frames, frame side and top covers removed) *****

* Please refer to the TD0213 - Traka Touch Pro Key Cabinet Installation Guide for the instructions on how to remove these parts

3.4 ENVIRONMENTAL RATING

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

3.5 APPROVALS & COMPLIANCE LEVEL

3.5.1 PRODUCT COMPLIANCE

UK – UKCA

Europe - CE

USA – MET NRTL, FCC

Canada – MET NRTL, ICES

3.5.2 BUSINESS COMPLIANCE

Quality – ISO9001

Environmental – ISO14001

Information Security – ISO27001

4. 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 Pro Key Cabinet Systems. Please keep this guide handy for those times when you need to remember how to **Add a user**, **Replace an iFob** or simply refresh your memory on how to restrict access to a key in the user details form.

NOTE: **Please note that any misuse or damage to the equipment caused by the incorrect installation or use of the product, such as misuse or damage to doors, hinges and locks will cause a reduction in performance of the key cabinet(s). Misuse includes (but not limited to) blocking hinges and doors, overriding locks or over filling with keys.**

NOTE: **For information on the previous range of Traka Touch Key Cabinets please refer to UD0011 - Traka Touch User Guide.**

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 Pro. 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.
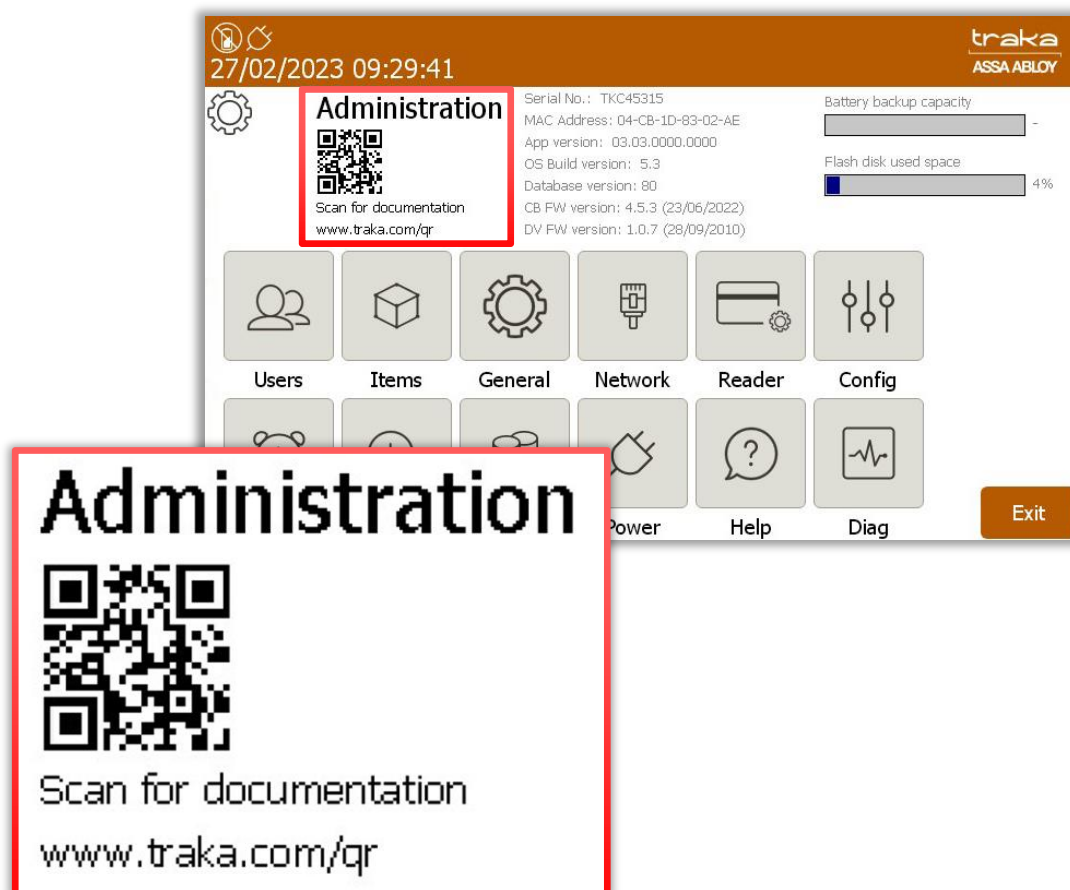

Figure 1 – QR code in the Traka Touch Pro Administration menu

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

5. TRAKA TOUCH DETAILS AND DIAGRAMS

5.1 CABINET TYPES

Traka Touch Pro Key Cabinets are now available in four variants:

The Traka Touch Pro V, M, S & L, as shown in the diagram below from left to right.

Like our previous range of Capacitive Touch Screen models, the Traka Touch Pro Key Cabinet Range are equipped with a Capacitive Touch screen and the Traka Mk3 Control Board. The Traka Touch Application software is the same for all models and should be at a minimum version of V3.2.3

5.1.1 TRAKA TOUCH PRO KEY CABINET MODELS

Figure 2 – Traka Touch Pro Series units

Figure 3 – Traka Touch Pro M

The Touch Pro M Key cabinet is perfect for smaller applications. Accommodate up to 20 keys (40 double density) with this innovative key cabinet system putting keys where they are needed most.

The Touch Pro M is a sophisticated key management system that has intelligence built in. It can operate as a standalone solution that requires no IT network or server to manage the database. Alternatively, it can be networked with our enterprise solution TrakaWEB.

A full audit trail of all key transactions is retained within the system by the internal solid-state memory. Management of keys has never been so easy,

Securely store and manage up to 20 keys (up to 40 keys if double density)

- 24/7 access to keys

- Control access to authorised users only

- View a full audit trail of all users and key transactions

- Easy access via PIN code, card reader and biometric fingerprint reader

- Battery backup

- Soft close-down with no data loss in the event of long-term power failure

5.1.3 TRAKA TOUCH PRO S KEY CABINET MODEL

Figure 4 – Traka Touch Pro S

The Touch Pro S Key cabinets are a versatile solution allowing for system scalability. Accommodate up to 60 keys (120 in double density) with this innovative key cabinet system.

The Touch Pro S is a sophisticated key management system that has intelligence built in. It can operate as a standalone solution that requires no IT network or server to manage the database. Alternatively, it can be networked with our enterprise solution TrakaWEB.

A full audit trail of all key transactions is retained within the system by the internal solid-state memory. Management of the system has never been so easy.

Securely store and manage up to 60 keys (up to 120 keys if double density)

- 24/7 access to keys

- Control access to authorized users only

- View a full audit trail of all users and key transactions

- Easy access via PIN code, card reader and biometric fingerprint reader

- Battery backup

- Soft close-down with no data loss in the event of long-term power failure

5.1.4 TRAKA TOUCH PRO L KEY CABINET MODEL

Figure 5 – Traka Touch Pro L

The Touch Pro L Key cabinet system is designed especially for larger organizations with a high key turnover. Accommodate up to 180 keys (360 in double density) with this innovative key cabinet system.

The Touch Pro L is a sophisticated key management system that has intelligence built in. It can operate as a standalone solution that requires no IT network or server to manage the database. Alternatively, it can be networked with our enterprise solution TrakaWEB.

A full audit trail of all key transactions is retained within the system by the internal solid-state memory. Management of the system has never been so easy.

Securely store and manage up to 180 keys (up to 360 keys in double density)

- 24/7 access to keys

- Control access to authorized users only

- View a full audit trail of all users and key transactions

- Easy access via PIN code, card reader and biometric fingerprint reader

- Battery backup

- Soft close-down with no data loss in the event of long-term power failure

Figure 6 – Traka Touch Pro V

The Touch Pro V Key management system by Traka brings all the traditional benefits of our core Touch systems in a neat compact design for up to 5 sets of keys.

The Touch Pro V has been designed to manage critical keys at multiple locations where space is at a premium and only a few keys need to be managed at each location. This could include ships and remote locations requiring maintenance. There is a minimum order quantity for this product.

Securely store up to 5 sets of keys at multiple locations.

- 24/7 access to keys

- Control access to authorized users only

- View a full audit trail of all users and key transactions

- Card reader and biometric options available

- Optional battery backup

- Can be networked with other Traka solutions to provide centralized control of your keys
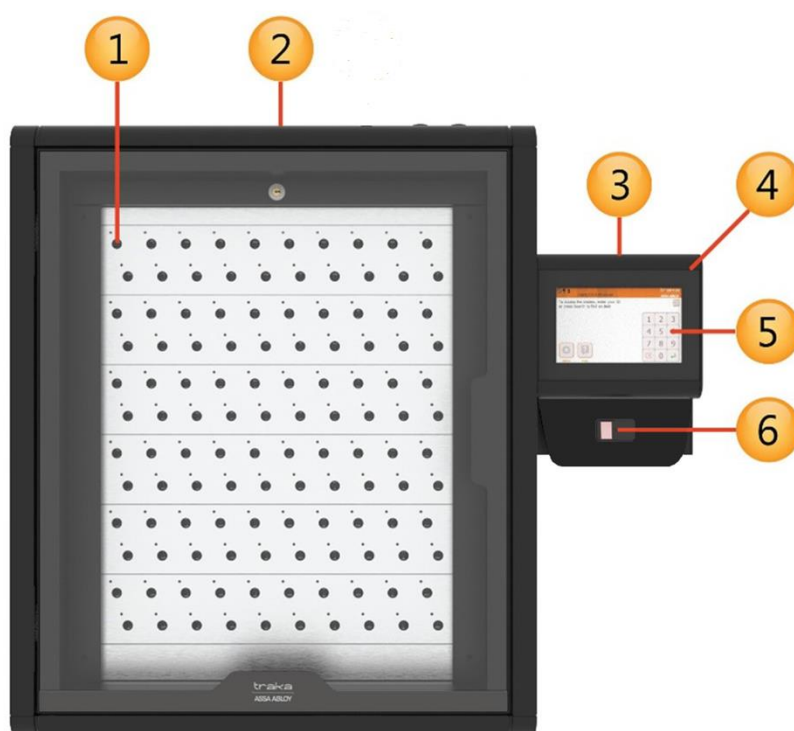
Figure 7 – Traka Touch Pro Cabinet diagram

5.2.1 SYSTEM KEY

1. Receptor Slot Cabinet

The Receptor Slot holds the item. A Receptor Slot is defined as Locking or Non-Locking depending upon the type of Receptor Strip. For a locking slot, the user is required to push an 'on screen' touch sensitive button to release the item.

2. Cam Lock

This cam lock is a manual override for the cabinet door. 2 keys are supplied with your Traka system. We ask that you do not keep these keys in the Traka cabinet. In case of system failure, you will be required to access those keys and use this cam lock as a manual override to open the cabinet door.

3. Control Pod Cam Lock

This cam lock provides access to the cabinet's electronics during servicing and maintenance. The keys used for the pod are the same keys used as a manual override for the cabinet door.

4. Control Pod

Incorporates the LCD (Liquid Crystal Display) and Card Reader as well as the Cam Lock providing access to the systems electronics.

5. 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.

6. Card Reader/Biometrics Reader

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.

Figure 8 – Traka Touch Pro Cabinet diagram

5.3.1 SYSTEM KEY

1. **Touch Screen**

   The Touch sensitive screen 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.

2. **Control Panel Cam Lock**

   2 master keys are supplied with your system. The master key can be used for gaining access to the system electronics during service and maintenance. It is important that the Master Keys are **not** stored inside the Traka system.

3. **Manual Door Release Cam Lock**

   2 Master Keys are supplied with your Traka system. The Master Key can be used for gaining access to the keys in the system in an emergency situation. It can also be used during servicing and maintenance.

4. **Card / Proximity / Biometrics Reader Plate**

   Traka supports a wide array of access devices, which will be mounted onto this plate. 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 keys accordingly.

5. **Receptor Slot**

The Receptor Slot holds the iFob in place.

5.4 SERIAL NUMBER/RATING PLATE LOCATION

5.4.1 TRAKA TOUCH PRO V

1. The Rating plate can be found on the side of the Touch system.

Figure 9 – Location of the Rating Plate in V-Touch

5.4.2 TRAKA TOUCH PRO M, S & L

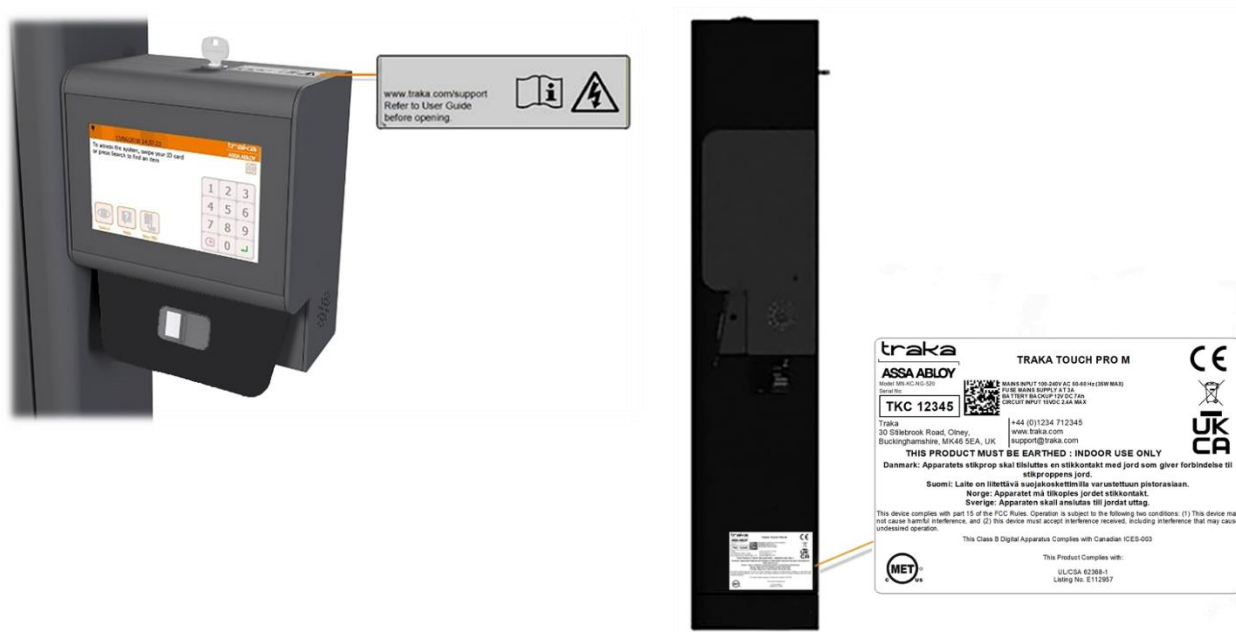1. The Rating plate can be found on the side of the Touch System.

Figure 10 – Location of the Serial Number & Rating Plate

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

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.

5.5   IFOB (INTELLIGENT FOB) & KEY BUNCH DIAGRAM
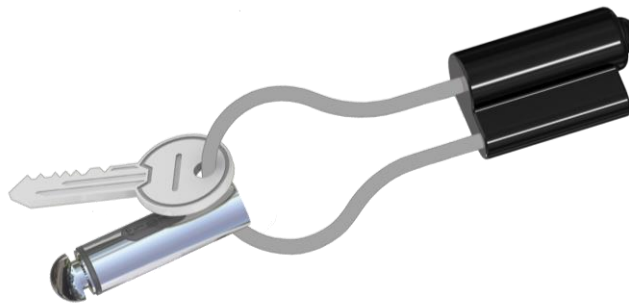
Figure 11 – Key bunch diagram

5.5.1 IFOB DIAGRAM

1. iFob

The item is at the heart of any Traka Key Management system. It is a bullet shaped device made from nickel plated brass. It contains a microchip with a unique identification number allowing the Traka system to identify the key(s) attached.

2. **Identification Tag**

The identification tag displays the cabinet position number to which the item belongs. The tags can be provided in a variety of colours which is useful when managing multiple Traka systems. For example, tag "101 yellow" would belong to position 101 in the "Yellow" cabinet and tag "101 blue" would belong to position 101 in the "blue" cabinet. This makes it nice and simple for system administrators and users.

3. **Security Seal**

The Security Seal is used to attach the key(s) to the iFob using the special tool from the kit provided. Once the seal is locked, the only way to detach the keys from the item is to cut the security seal using the provided tool. Traka can provide various types of security seal, please enquire with your Traka Account Manager or Distributor for more details. Alternatively, a less secure method would be to use a G-ring or a simple Keyring.

5.6   USB MEMORY STICKS

Figure 12 – USB memory stick

NOTE: USB memory sticks should be formatted to FAT32 and not NTFS when used in a Traka Touch Pro system as NTFS is not supported by the Windows 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 Pro 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. For Traka Touch Pro Key Cabinets, the USB port will be located behind the door and also the Traka Mk3 Control Board located behind the control panel door using.

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

6. THE TOUCH SCREEN

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

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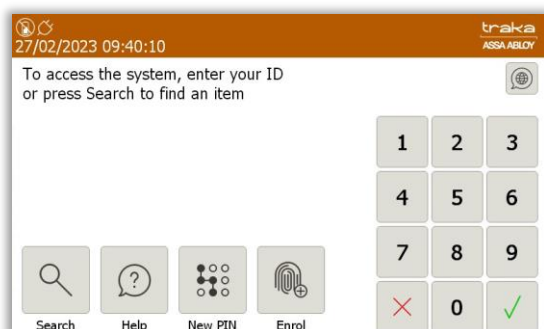
If the Traka Touch Pro system is not used for user definable period of time, then the system will go into 'idle' mode. To use the system again simply press anywhere on the touch screen or swipe your card to wake the system up.

6.2 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.
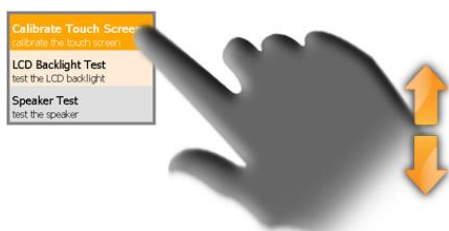
Scroll – Swiping up and down on a list in will scroll through the menu.

7.1 CREATING THE ADMIN USER

When using Traka Touch Pro 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.
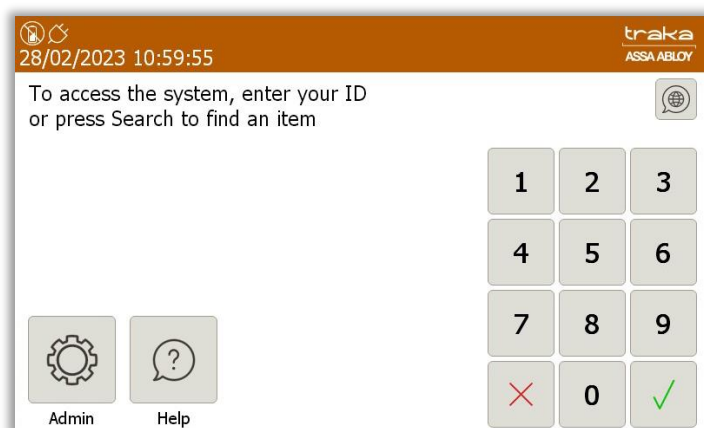
1. From the login screen, select **Admin**.
2. When the Admin screen appears select **Users**.
3. The User list will currently be empty. Select the **Add** button.
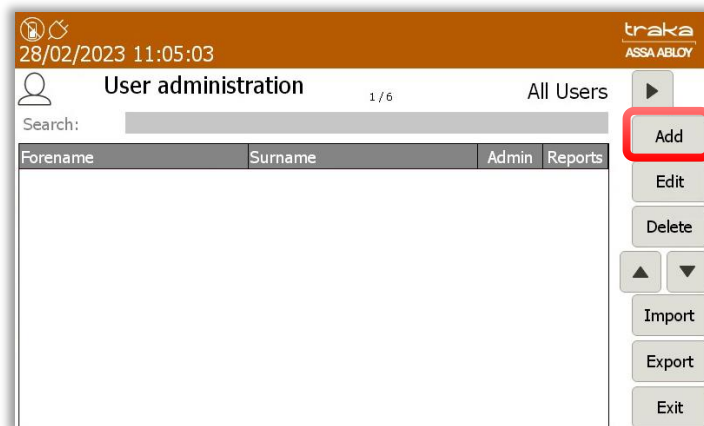
NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

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.

Access Method	User Will Require
Primary Access	
Keypad ID	Enter a Keypad ID – This is an ID number minimum of four digits long.
Reader Access	Enter the Card details into the Credential ID field or Swipe ID Card at reader
Fingerprint Access	Select Access > Options > Enrol and follow-on screen instructions. **NOTE: Please see separate Sagem section on how to enrol a user**
Secondary Access	
PIN	Enter a PIN - This is also an ID number minimum of four digits long that can be used in addition to a Keypad ID, Credential ID or Fingerprint ID. Please refer to the main Traka Touch Pro User Guide UD0258 for details on PIN.

NOTE: Systems with Multiple Credentials enabled 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 Pro 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 as 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.
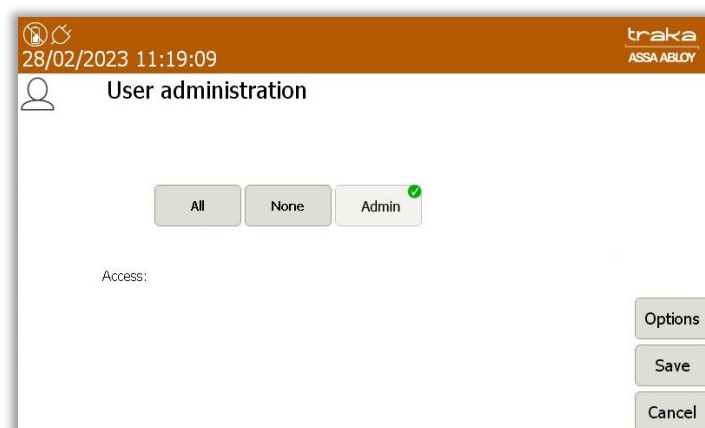
Credential ID

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

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

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 Pro 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:

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.

Start Date
The user active date defines when a user becomes able to use the Traka Touch Pro 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 Pro 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:
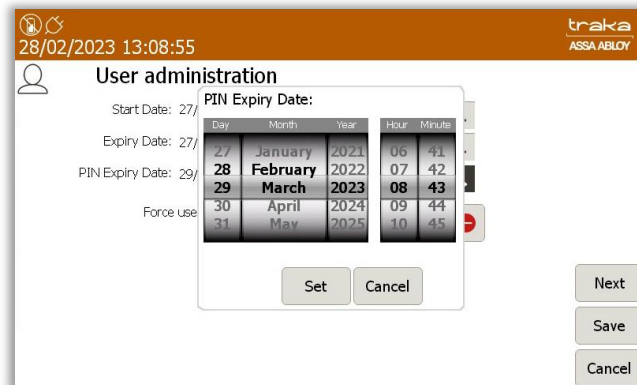
PIN Expiry Date

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:

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.
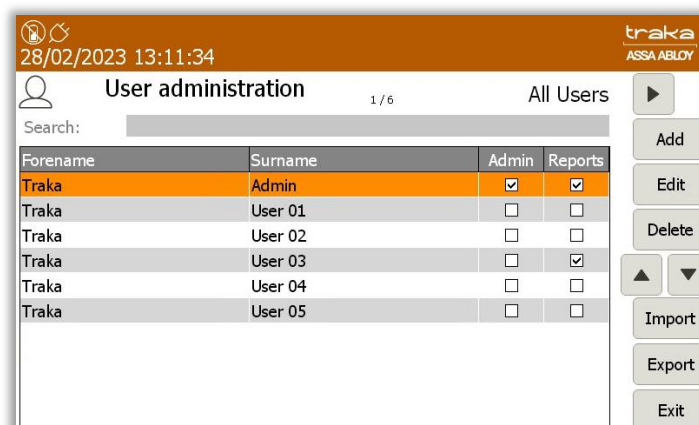
User Curfew Type

Here, you will be able to select from None, Specific time of day and Days/Hours Minutes.

9. 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.

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

11. To add more users simply click the **Add** button and repeat this process.

12. 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:

13. 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.

14. 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.

7.2   ACCESSING THE SYSTEM

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.

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.
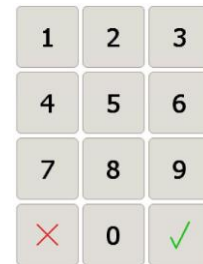
7.2.1 KEYPAD ID ONLY ACCESS

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

2. Enter your Keypad ID.

3. Press ↵ (enter) to confirm your Keypad ID.
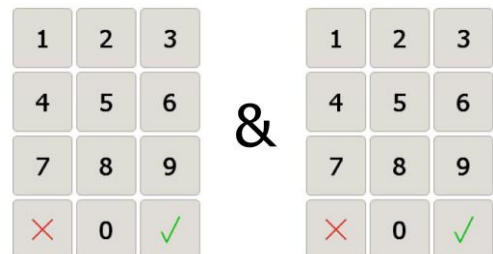
4. Verify your username on the touch screen.

7.2.2 KEYPAD ID 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.

7.2.3 CREDENTIAL ID ONLY ACCESS
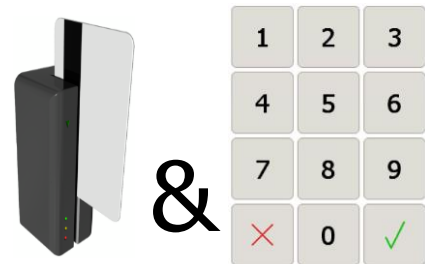
1. Swipe/present your card/token to the reader.

2. Verify your username on the touch screen.

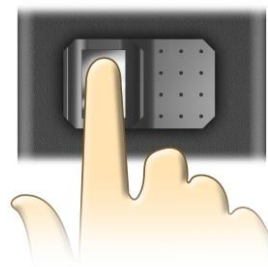### 7.2.4 CREDENTIAL & PIN ACCESS

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.
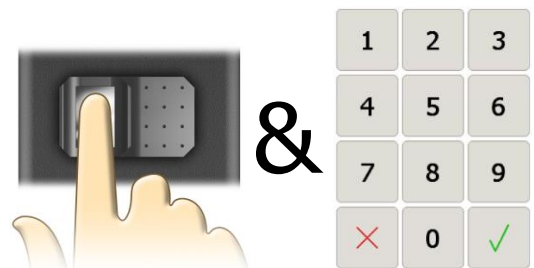
7.2.5 FINGERPRINT ACCESS

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.

7.2.6 FINGERPRINT & 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.

NOTE: There is an event within Traka Touch Pro 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.

7.3 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. 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 Pro system. The Roles are assigned within the User Administration screen by selecting the Roles button.
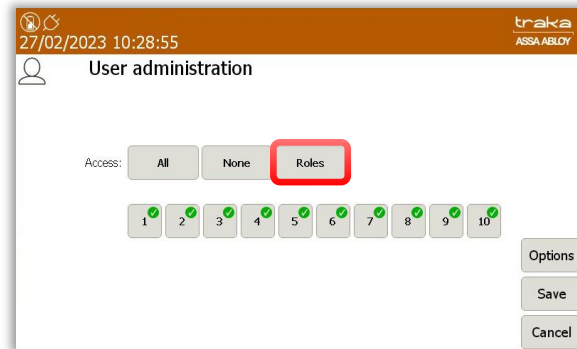
Admin roles can be selected individually from the User Roles list. They may also be assigned from the system access grid in TrakaWEB. For more information, please refer to TrakaWEB User Guide.

NOTE: Roles not applicable to Traka Touch Pro may only be assigned from TrakaWEB, these will include many of the cost option override features.
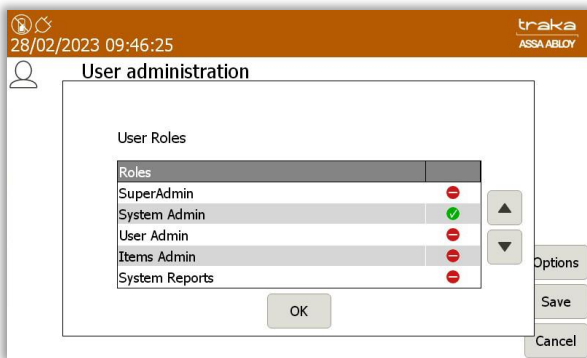
Super Admin Role

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

The Super Admin role will allow 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.
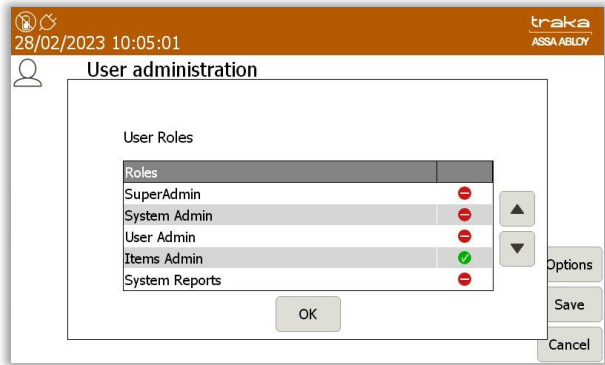
User Admin Only Role

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.
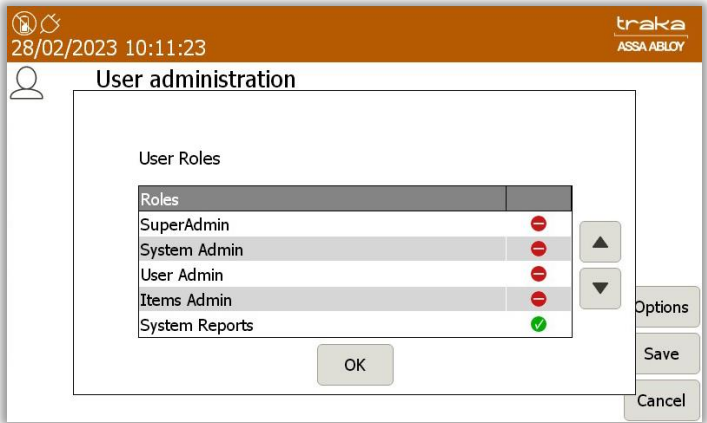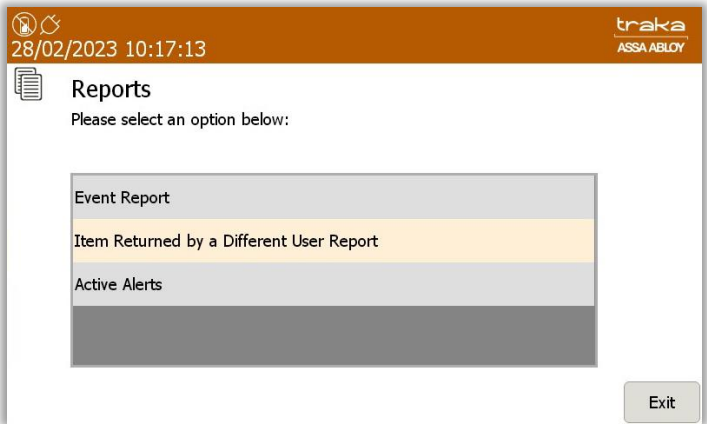

Items Admin Only Role

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 or replace damaged or broken iFobs.

System Reports Only

Selecting this option will allow the user to view & run reports at the Traka Touch Pro 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.

This Document is uncontrolled when printed unless over stamped "CONTROLLED DOCUMENT"
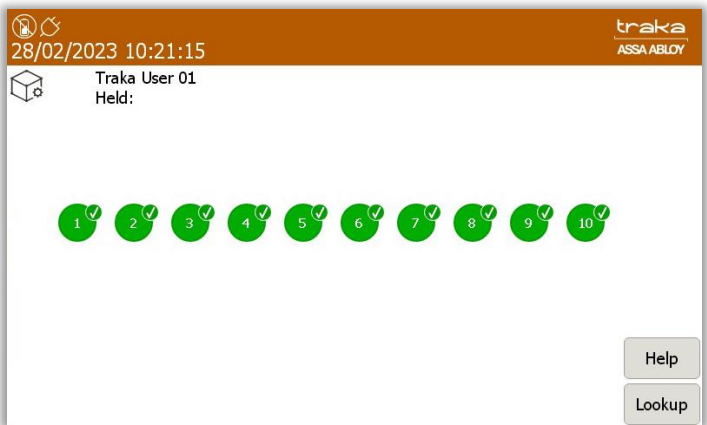
Users with System Admin & Items

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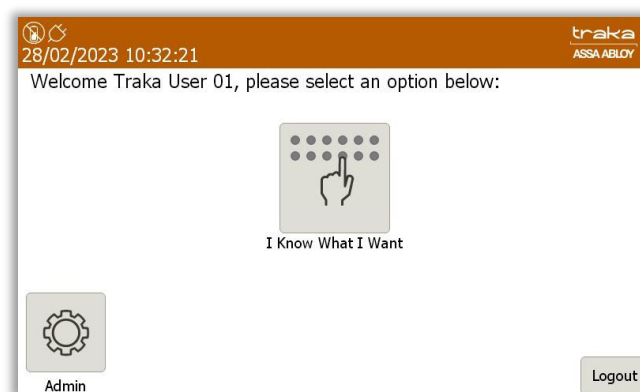

Users with User Admin & Items

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.
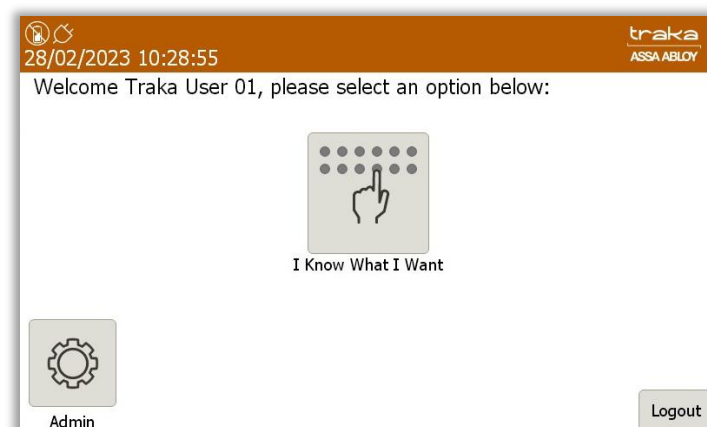

Users with Item Admin & Items

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.

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

<u>**Users with System Reports & Items**</u>

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.
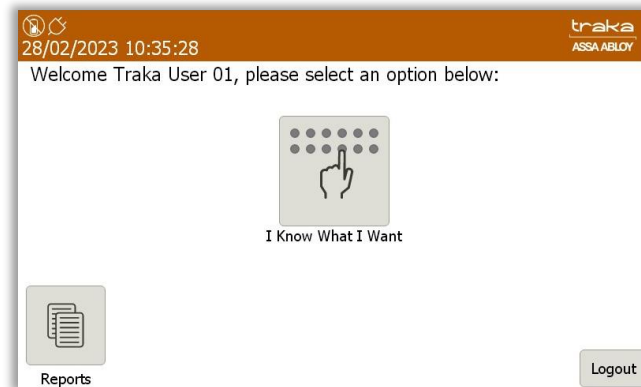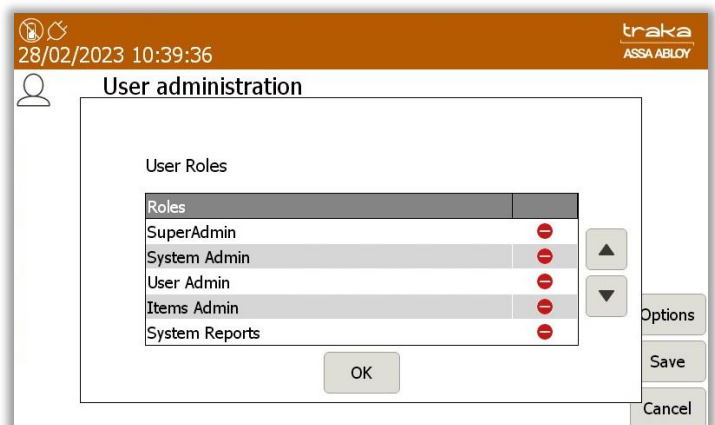

From the User Roles screen, it is also possible to create different combinations of roles that can be assigned to specific users. These can be applied to users with access to both admin roles and items or admin roles only.

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

NOTE: If your Traka Touch Pro has RRMS enabled, you will not be able to configure iFobs.

NOTE: This procedure will have already been carried out at Traka, however it is a good idea to configure the iFobs to ensure they are being detected and the system is operating correctly after delivery and installation.

1. An administrator needs to identify themselves to the Traka system.

2. Click **Admin**.

3. From the admin menu, select **Items**.

4. The item list will currently be populated with recognised iFobs. Click the **Setup** button.
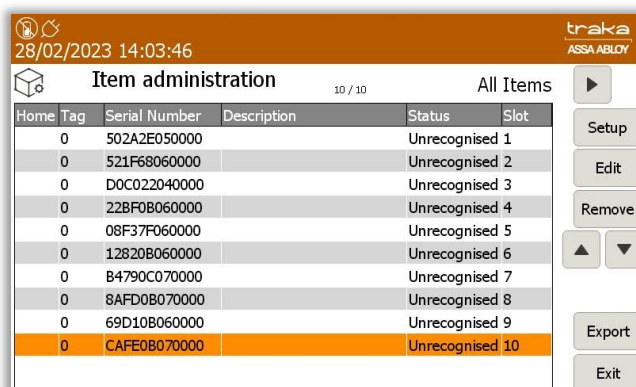
5. You will be asked if you wish to setup all items, click **Yes**.
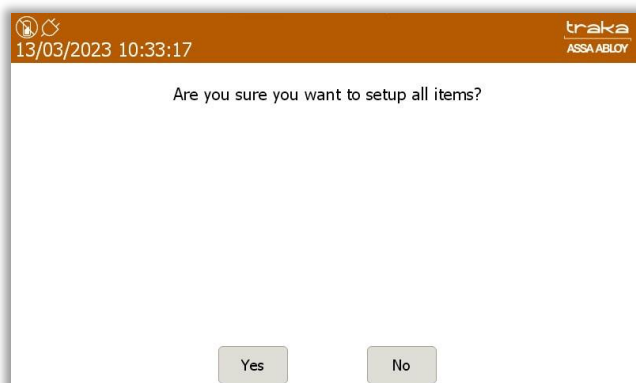
6. The item list will now begin to populate, showing all the iFobs that are being recognized. This process is displayed via the small blue progress bar in the top right corner of the window.
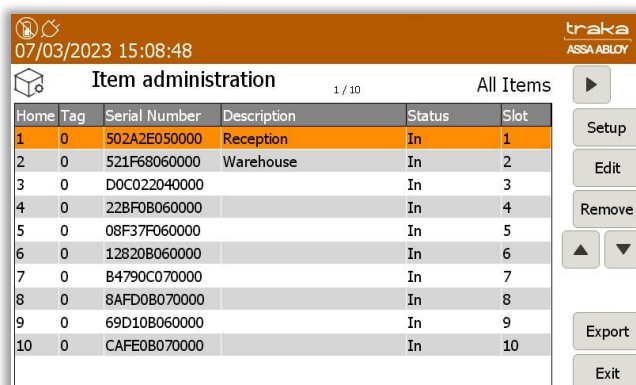
7. Once this is complete, you can choose to give each item a description. To do so simply highlight the desired item in the list and click the **Edit** button.

8. Enter a description into the provided field.

NOTE: From the Options page you can configure various advanced fetaures for the item. For more details please refer to UD0258 - Traka Touch Pro User Guide.

9. Click **Save** and you will be taken back to the Item Administration page. To edit more items simply highlight the item and click the **Edit** button.

10. When you have finished editing items, click **Exit** and you will be taken back to the Admin menu. Click **Exit** again to return to the login screen.

7.5   USERS

7.5.1   ADDING USERS

NOTE: Adding, editing, and deleting users must be carried out by an administrator.

1. Identify yourself to the system via Keypad ID, Credential ID or Fingerprint.

2. Click Admin.

3. From the admin menu, select Users.

4. The current user list will then be displayed.

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.

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

5. Click the Add button.

6. The user details window will then be displayed. Simply enter the user's information in the same way as described in Section **Creating the Admin User**.

NOTE: Systems with Multiple Credentials enabled 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'. Refer to UD0260 – TrakaWEB Version 4 User Guide for further details.

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.

7.5.2 EDITING USERS

NOTE: Adding, editing, and deleting users must be carried out by an administrator.

1. Identify yourself to the system via Keypad ID, Credential ID or Fingerprint.

2. Click **Admin**.

3. From the admin menu, select **Users**.

4. The current user list will then be displayed.

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.

NOTE: If you are currently using card readers and are searching for a particular user, swipe their ID card when the user list is showing to quickly navigate to the user. This is particularly helpful when you have a large user list as it will save time scrolling though different users.

5. Click the **Edit** button.

6. The user details window will then be displayed. Simply enter the user's information in the same way as described in the Creating the Admin User section.

NOTE: Systems with Multiple Credentials enabled 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'. Refer to UD0260 – TrakaWEB Version 4 User Guide for further details.

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.

7.5.3 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. The preferred option to remove a User from a Traka system is as follows:

- Define the user as in-active 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 back-up 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: Adding, editing, and deleting users must be carried out by an administrator.

1. Identify yourself to the system via Keypad ID, Credential ID or Fingerprint and click Admin, Users, then select the desired user from the list 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. Select Yes to permanently delete the user from the system. The users name will no longer appear on the User list.

NOTE: If you are deleting all users, the last user to be deleted must be an admin user.

3. Select Exit and then Exit again to be taken back to the login screen.

7.5.4 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 Pro to handle a large number of users.

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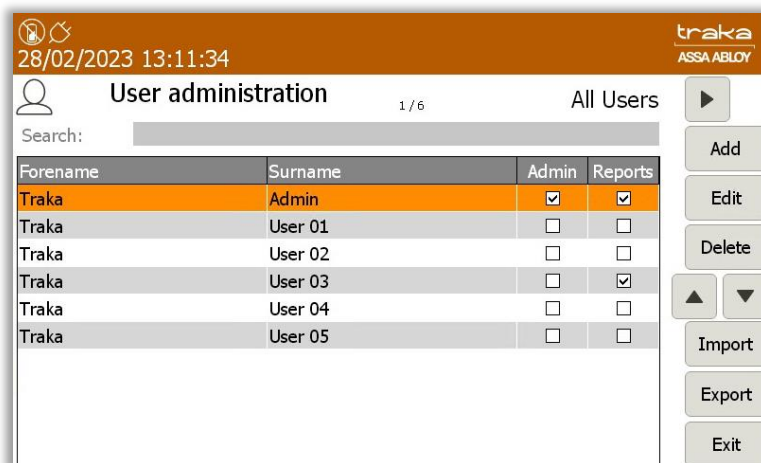
NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

Less than 500 users

If there are 500 or less users within the system, the option to 'show all' will be displayed.

Clicking on 'show all' will display all the users within the grid.

NOTE: **A username can also be entered in the search bar. Clicking on '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.
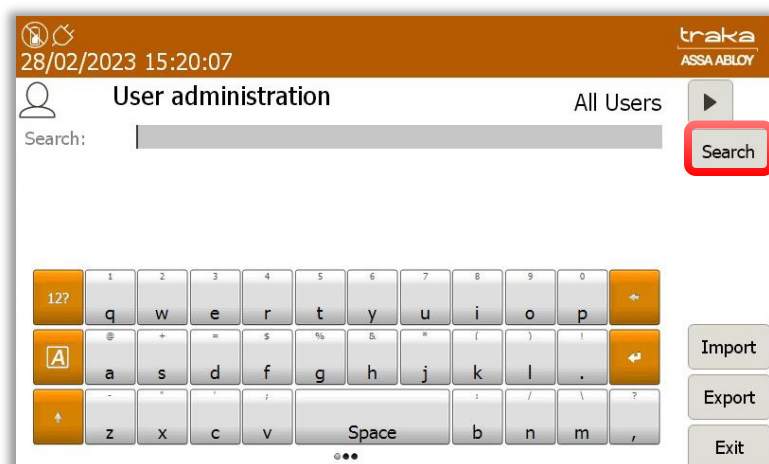
A username can be entered in the search bar. However, a minimum of 2 characters may be entered. Clicking on **Search** will display all matching results.
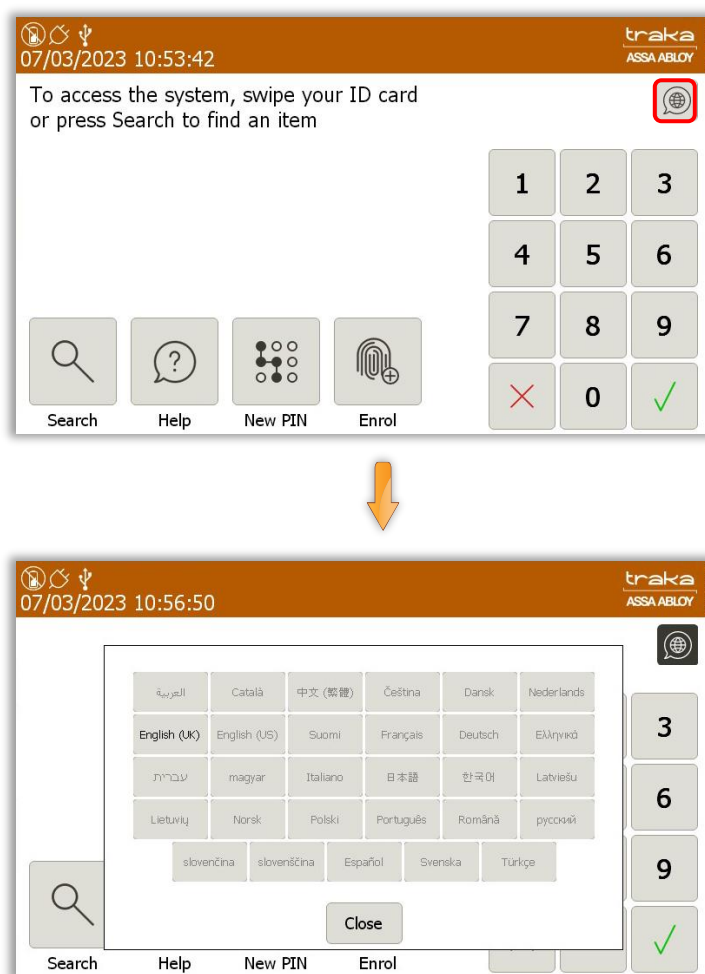
7.6 LANGUAGES

The Traka Touch Pro 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.

7.6.1 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 back to its default language.

7.6.2 CHANGING LANGUAGES FOR A USER

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

1. Click **Admin.**

2. Click **Users.**

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

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.

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

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

7.6.3 CHANGING THE DEFAULT LANGUAGE OF THE SYSTEM

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

1. Click **Admin.**

2. Click **General.**

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 Pro 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.
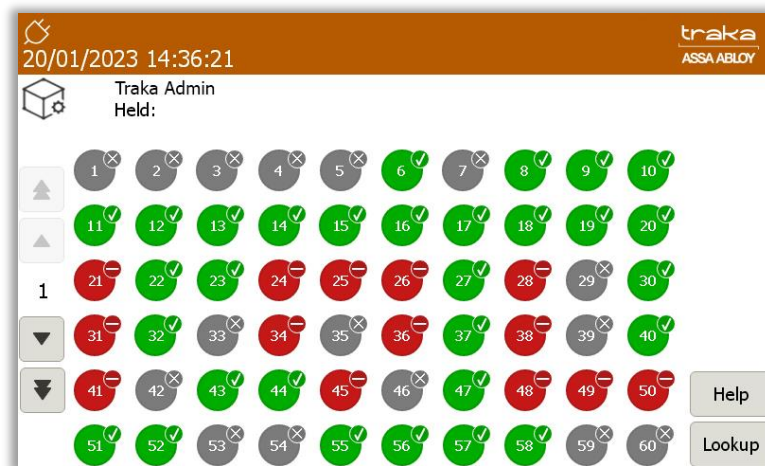
8.1   REMOVING / RETURNING ITEMS

NOTE: Systems with RRMS enabled do not have the following restrictions applied.

8.1.1   REMOVING AN ITEM

1. Identify yourself to the system via Keypad ID, Credential ID or Fingerprint.

2. The door will open.

3. Select which item you wish to remove by selecting the graphic on screen.

- 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.

- Single arrow – scroll through pages of position numbers using this button. The display will show a maximum of 60 positions on each page.

- Double arrow (systems with extensions only) – pressing this button will scroll through all available cabinets/doors. The cabinet door number is displayed between the arrows on the left of the screen.
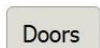
- (Systems with extension cabinets only) – pressing the Doors button will return you to the Door Selection screen.
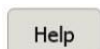
- Pressing the Help button will present you with a screen that has instructions on how to remove/return keys.

- 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.

1. **Press** the button on the touch screen of the item you wish to remove.

2. You will hear a beep.

3. **Wait** for the "**click**" (unlocking item).

4. **Remove** the iFob.

8.1.2 RETURNING AN ITEM

You **must** return the iFob to the correct position.

1. Identify yourself to the system via Keypad ID, Credential ID or Fingerprint.

2. The door will open.

3. Check the tag number on the key bunch.

4. Insert the iFob into the matching position.

8.1.3 ITEM IN WRONG POSITION

When an iFob is returned to the incorrect position, the system will prompt you to remove the iFob and return it to the correct position.
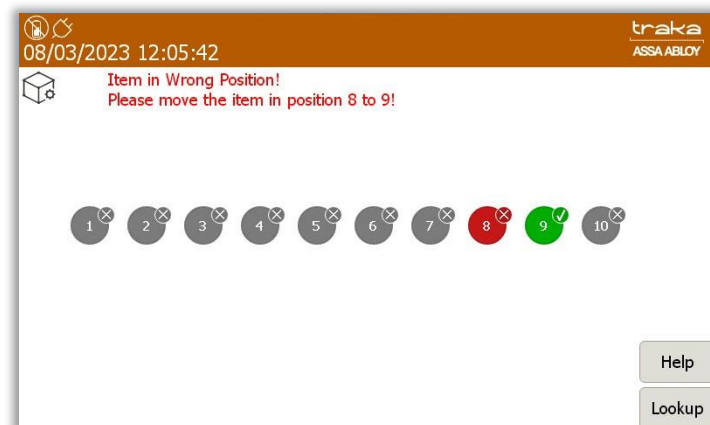
In addition to the touch screen giving you instructions, the receptor strip LED's will illuminate and guide you to the correct slot.

8.2 GENERATING REPORTS

Traka Touch Pro 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.

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.
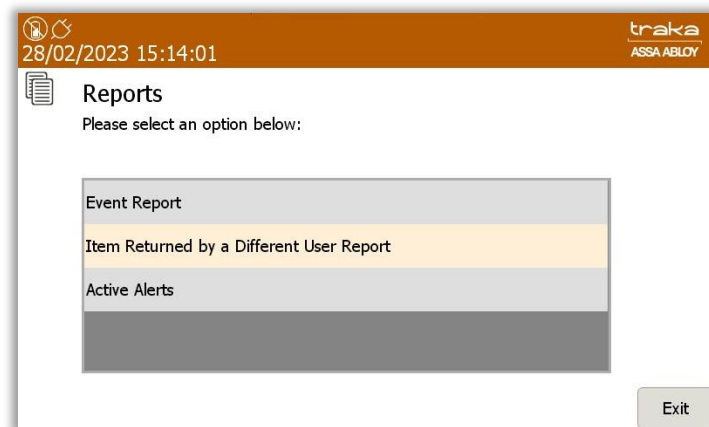
The Reports options will provide you with a number of set ways to filter the report as required. Alternatively, you can choose to set more specific dates.

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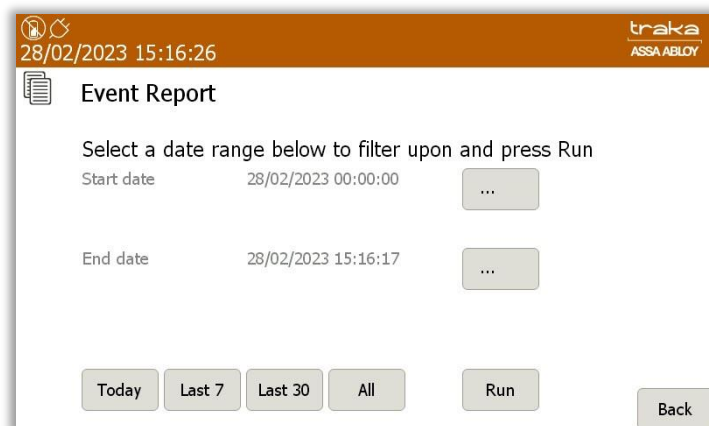
- The [Today] button will provide all the reports for today.

- 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 scroll function that will enable you to navigate up or down to select and set the required start date.

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

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

2. 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 scroll 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 scroll function that will enable you to select and set the required end date.

1. Select one of the filtering options above and click the Run button.

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

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

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

8.2.1 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, refer to the USB Memory Sticks section in this document.

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.
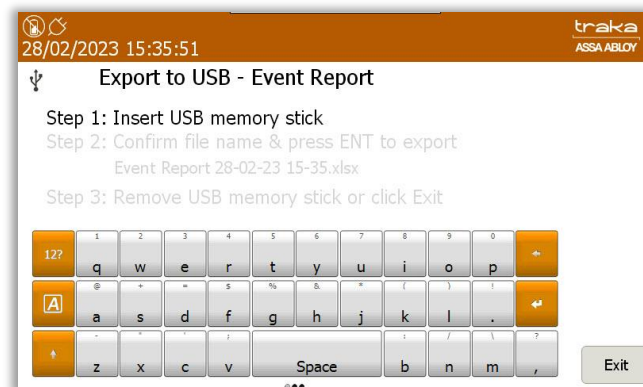
3. Enter the desired file name for the report and press [↵] (enter).
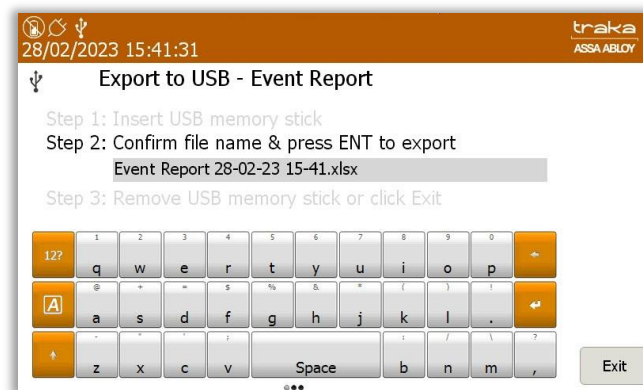
4. The report will now begin to export to the USB device.
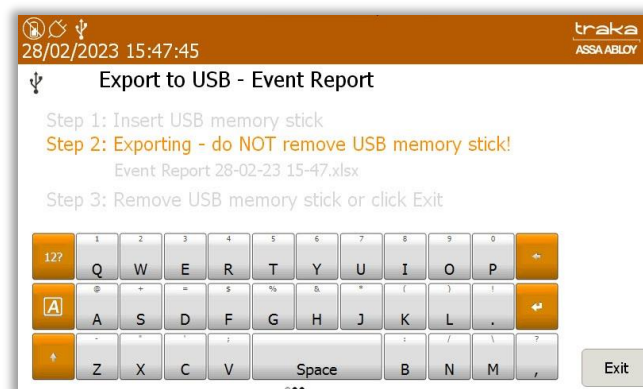
5. When the report has finished exporting, remove the memory stick and close the door (if applicable).
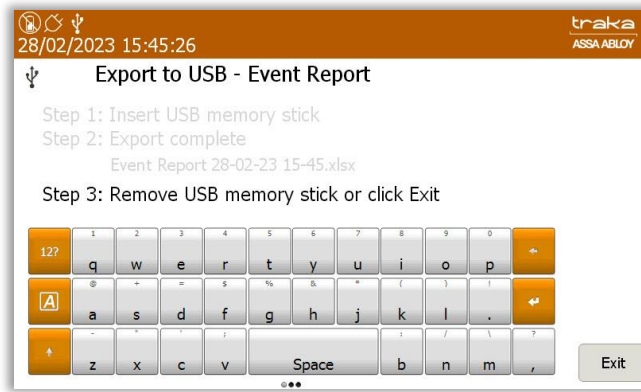
6. You will be taken back to the event report screen. Click the [Exit] button to be taken back to the login screen.

9. SAGEM FINGERPRINT READER

9.1 INTRODUCTION

This section has been prepared to assist you when enrolling users on the Sagem Fingerprint reader. This is the Getting Started Guide and does not contain as much detail as the full Traka Touch User Guide. For more details, please see UD0258 – Traka Touch Pro User Guide.

9.2 HOW TO ENROL

NOTE: An admin user must be present to manually enrol a user at the Traka Touch Pro system. Alternatively, enrolment can be carried out by the user via an Enrolment ID. For more details on Enrolment ID please refer to the main Traka Touch Pro User Guide UD0258.

1. Identify yourself to the system via Keypad ID, Credential ID or Fingerprint.

2. Click Admin.

3. From the admin menu select the Users button.

4. From the user details select the **Options** button until you get to the enrol screen. This button cycles round the various screens i.e. Access->Options->Enrol->Details->Access etc.
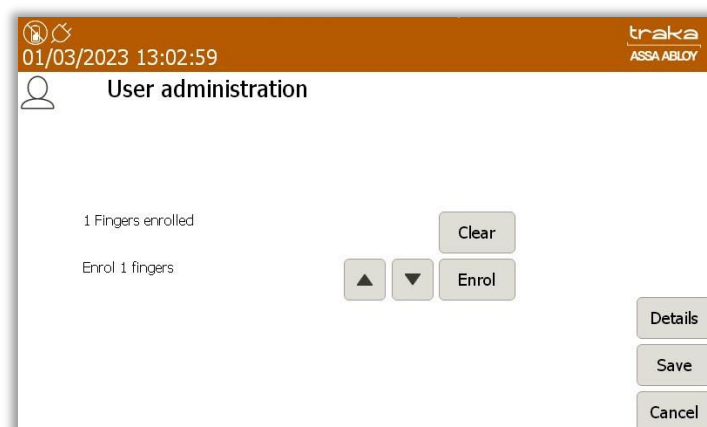
5. Click the **Enrol** button.

6. The system will prompt the user to place their finger on the reader. They will have to do this 3 times for each finger they wish to enrol.

Place finger   Capture Ok   Remove finger

7. When placing a finger, if it is not located correctly on the reader the following icons will be displayed to help with positioning:

 Press Harder   Move Finger Up   Move Finger Down

 Move Finger Right   Move Finger Left
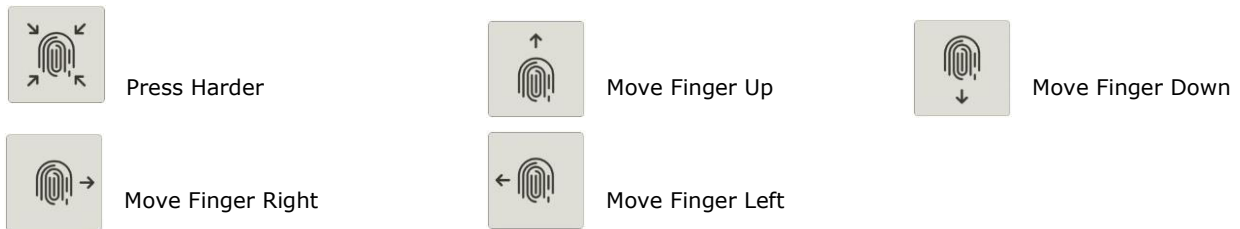
8. When complete, the screen will display how many fingers were enrolled for the user, 1 or 2.

NOTE: To cancel the Enrol process, click the central Cancel button.

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

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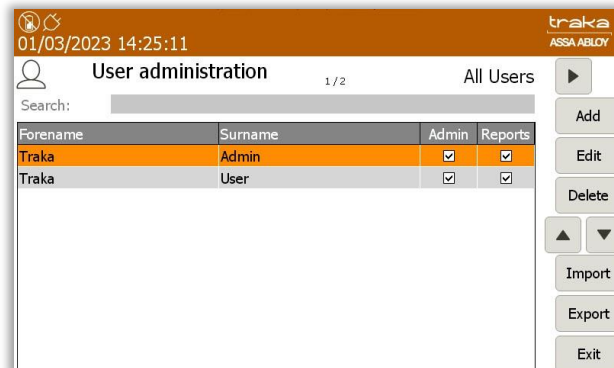
NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

2. 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.
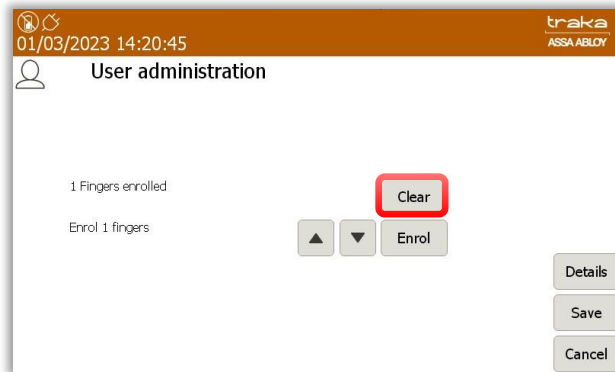
3. Select the **Clear** button.

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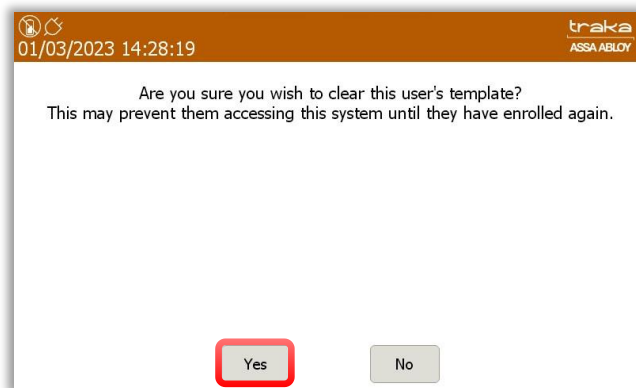
The users' template is now removed from the database. The User Administration page will remain visible should the user require re-enrolling.

5. Once completed, select the **Save** button.
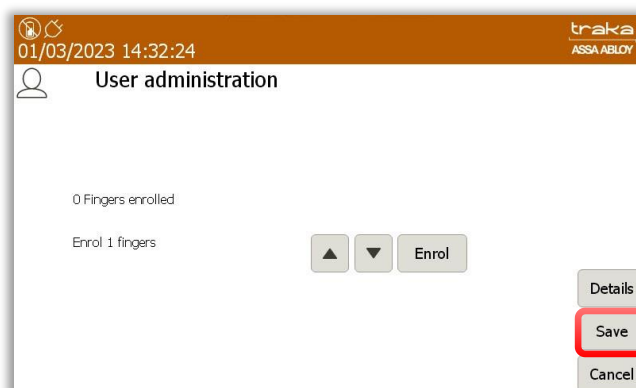
9.4   TIPS ON ENROLLING

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**

Finger Angle   **Ideal Position**

Finger Inclination   **Finger Rotation**

Ideal Position   **Ideal Position**
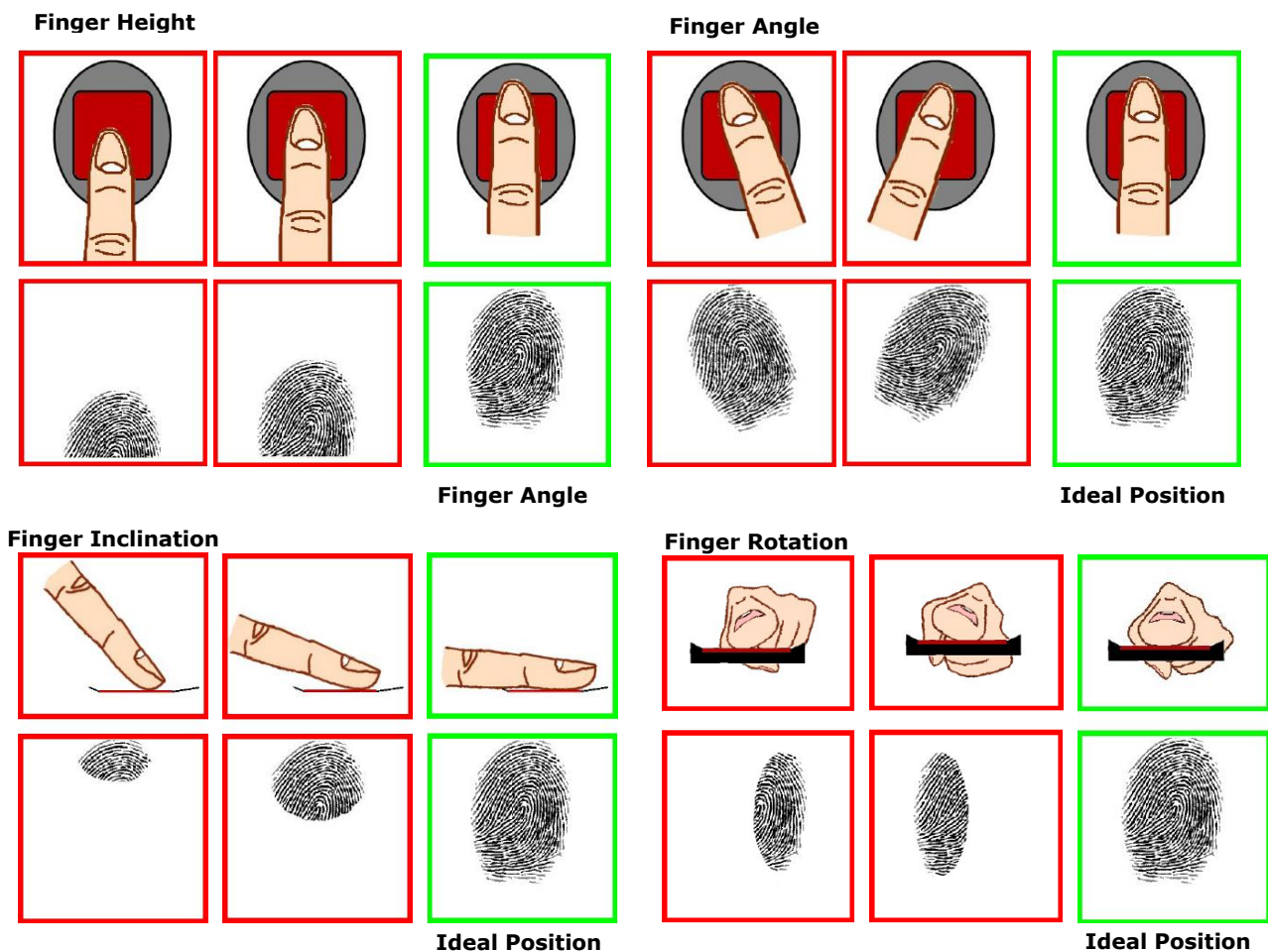
9. Once you have finished enrolling click the Save button.

10. You will then be taken back to the user list. From there click Exit to be taken back to the Admin menu, and click Exit again to be taken back to the Login screen.

10.1 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 Cabinet with wet hands as this may damage the touch screen.

10.1.1 CLEANING PROCEDURE FOR TRAKA CABINET

- 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.

10.1.2 CLEANING THE TOUCH SCREEN

The Traka Touch Pro 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.

10.1.3 IFOBS

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

10.1.4 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.

10.2 MANUALLY OPENING THE DOOR

10.2.1 TRAKA TOUCH PRO V

1. Insert your Master override key into the cam lock and turn until the lock fires and the door opens.

Figure 13 – Opening Control Panel in V-Touch

10.2.2   TRAKA TOUCH PRO M, S & L

1. Insert your Master override key into the cam lock and turn until the lock fires and the door opens.

Figure 14 – Opening Cabinet Door

NOTE: **If your Traka Touch Pro system is set to RRMS then this section is not applicable.**

You will occasionally be required to replace an iFob that may have become lost or damaged. If the damaged iFob is in the system, you will need to remove it from the system before allocating a new iFob to the same position.

The Traka Touch Pro system works on a fixed item replacement basis, which means iFobs, must be returned to the positions from where they were taken. By default, the system will not know where an iFob should go therefore the iFob serial number must be associated with the position in the system.
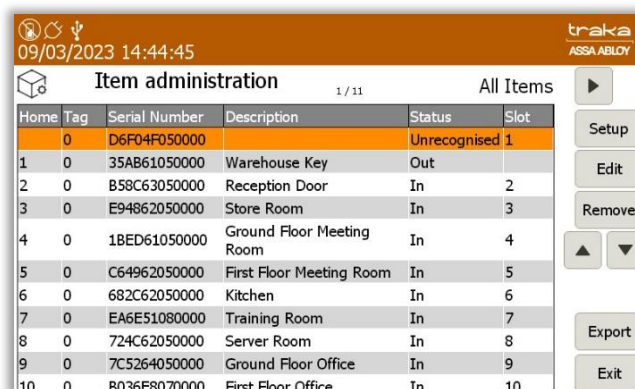
1. Identify yourself to the Traka System by entering your Keypad ID or swiping your Card.

NOTE: **The user must be an administrator and have access to all the iFobs in the system.**

2. Select the items button.

3. The touch screen will now show you all the iFobs in the system. Select the appropriate iFob on screen by clicking the green symbol and the iFob will be released. Remove the iFob.

4. Insert the new iFob into the vacant position. The system will start to alarm warning you that the iFob is not recognised, ignore this message, and close the door.
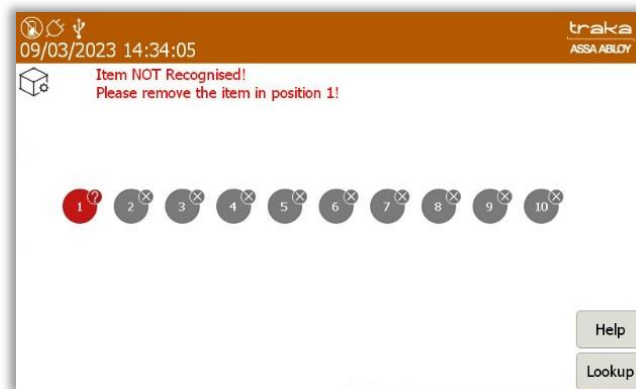
5. Identify yourself once again at the Traka System by entering your Keypad ID or swiping your Card.

6. Select the Admin button.

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

8. The item list will then display the new items status as 'unrecognised'. Select the Setup button.

9. You will be asked if you wish to setup all items, click the Yes button.
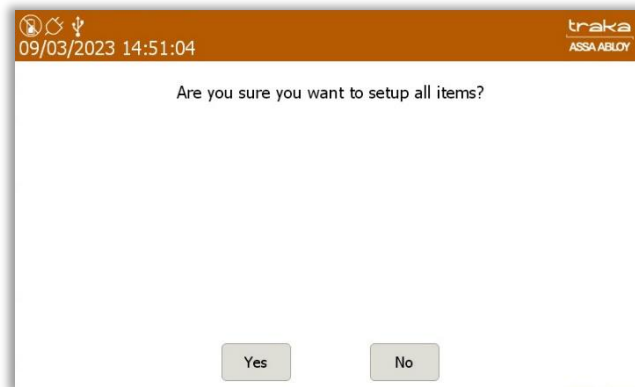
10. A message will appear asking you whether you wish to replace the item you removed with the new item, click the Yes button.
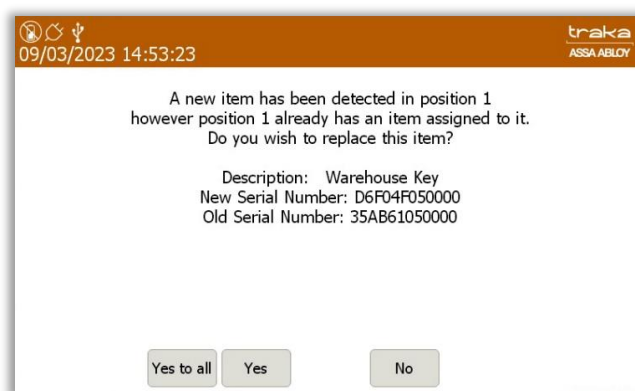
11. The item list will now begin to re-populate adding the new item. This progress is displayed via the small blue progress bar in the top right corner of the window.
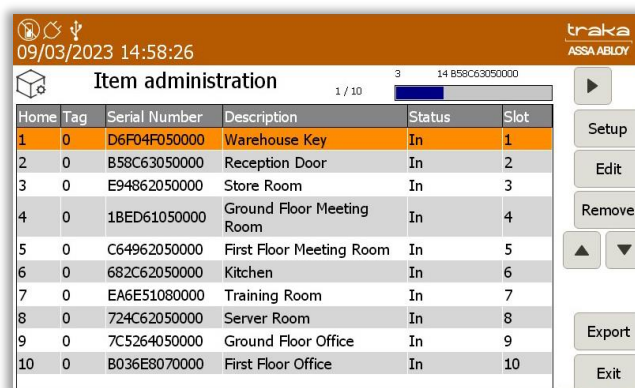
12. Click the Exit button to be taken back to the administration menu. From there click the Exit button again to return to the login screen.

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

14. Select the Keys button.

15. The LCD will now show you all the items in the cabinet. Ensure the item you replaced now has the 'item in System' symbol and can be removed.

11. 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
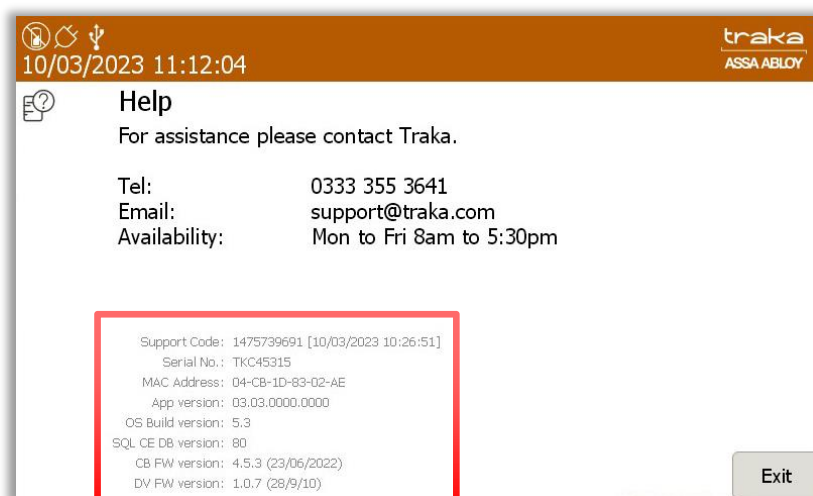
Technical Support Information

Please refer to the 'Traka Contact Details' on the next page of this guide.

The Embedded Software supplied under this End User Licence Agreement (EULA) shall be subject to the following terms and conditions:

1.   Definitions

"Applicable Law" means any: (i) law including any statute, statutory instrument, bye-law, order, regulation, directive, treaty, decree, decision (as referred to in Article 288 of the Treaty on the Functioning of the European Union) (including any judgment, order or decision of any court, regulator or tribunal); (ii) rule, policy, guidance or recommendation issued by any governmental, statutory or regulatory body; and/or (iii) industry code of conduct or guideline in force from time to time which relates to this EULA and/or the Hardware.

"Commercial Terms" means any legally binding document relating to the sale or supply of the Hardware to the Customer or dealing with the subject matter of this EULA, including under which payment is made for the Hardware by the Customer.

"Company" means ASSA ABLOY Global Solutions UK Ltd trading as Traka and shall include the Company's successors and assigns.

"Customer" means the person, firm or company with whom this EULA is made.

"Data Protection Laws" means all Applicable Laws relating to data protection, the processing of personal data and privacy, including: (i) the Data Protection Act 1998; (ii) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679; and (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and references to "Data Processor", "Data Subjects", "Personal Data", "Process", "Processed", "Processing" "Processor" and "Supervisory Authority" have the meanings set out in, and will be interpreted in accordance with, such Applicable Laws.

"Documentation" means materials such as manuals, user guides or similar materials associated with or related to the Hardware.

"Embedded Software" means all software including firmware on or embedded in the Hardware at the date of manufacture together with any updates or newer versions made available by the Company from time to time.

"Hardware" means the product acquired from the Company or its authorised partner, including all Embedded Software and Documentation.

"Intellectual Property Rights" means all intellectual and industrial property rights of any kind whatsoever including, but not limited to, patents, supplementary protection certificates, registered trademarks, unregistered trademarks, rights in know-how, registered designs, models, unregistered design rights, rights to prevent passing off or unfair competition and copyright (whether in drawings, plans, specifications, designs and computer software or otherwise), database rights, topography rights, any rights in any invention, discovery or process and applications for and rights to apply for any of the foregoing, in each case in the United Kingdom and all other countries in the world and together with all renewals, extensions, continuations, divisions reissues, re-examinations and substitutions.

"Supplier" means the entity from which the Hardware was purchased by the Customer being the Company or one of its authorised partners.

"Warranty Period" means the 12 months following the date of sale by the Company of the Hardware to which the Embedded Software relates.

2.   Licence

2.1   In consideration of the payment of the price for the Hardware to the Company or its authorised partner, the Company hereby grants a perpetual, non-exclusive, non-transferable licence for the use of the Embedded Software solely for use with the Hardware.

2.2   By installing and/or operating the Hardware, the Customer agrees to the terms of this EULA.

3.   Patents, Designs and Copyright

The Embedded Software is licensed, not sold, to the Customer by the Company for use only under the terms of this EULA. The Company and its licensors retain all proprietary interests and rights in and over the Embedded Software and reserve all rights not expressly granted to the Customer under this EULA including all Intellectual Property Rights which shall remain the exclusive property of the Company or its licensors.

4. Restrictions

4.1 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to disclose the contents or code of the Embedded Software to any third party. The Customer may take such copies of the Embedded Software as is necessary for the purpose of back-up security and agrees that all copies shall be kept confidential and subject to the terms of this EULA.

4.2 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to lease, rent, sub-license, loan, sell or otherwise redistribute the whole or any part of the Embedded Software. The Customer may, however, rent, lease or sell the Hardware, provided that: (a) any rental, leasing or sale must include the Hardware and all of the Embedded Software, including all its component parts, original media, printed materials and this EULA; (b) the Customer does not retain any copies of the Embedded Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the Hardware reads and agrees to accept the terms and conditions of this EULA.

4.3 The Customer agrees not to modify, disassemble, reverse engineer, derive the source code of, decrypt, create derivative works or decompile the whole or any part of the Embedded Software nor attempt to do so save to the extent expressly permitted by law.

4.4 The Customer will not attempt to ascertain or list the source programs or source code relating to the Embedded Software.

4.5 The Customer will notify the Company as soon as it becomes aware of any unauthorised use of the Embedded Software by any person.

5. Warranty

5.1 The Company believes that to the best of its knowledge the Embedded Software has been thoroughly tested for freedom from arithmetic or logical defects in the Embedded Software and that it will function and perform substantially in accordance with the functions described in the Documentation.

5.2 If at any time during the Warranty Period, the Customer becomes aware of a breach of the warranty at Clause 5.1, the Customer will:

5.2.1 promptly notify the Supplier of any defect which it believes to exist, such notice to be given prior to the expiry of the Warranty Period, with all details and information which may assist in diagnosing and correcting the defect; and

5.2.2 provide any facilities, information and assistance which the Supplier may reasonably request to aid the diagnosis of the alleged defect and co-operate with the Supplier in these activities.

5.3 If the Supplier is unable to ascertain or correct the defect with the Embedded Software as notified by the Customer in accordance with Clause 5.2, the Supplier (if not the Company) shall notify the Company.

5.4 The Company reserves the right to charge the Customer at its prevailing rates for any effort expended in tracing apparent defects which prove not to be defects covered under this Clause 5.

5.5 In the event of a proven breach of the warranty in Clause 5.1 during the Warranty Period, the Supplier (or Company (as the case may be)) will either:

5.5.1 repair, or at its option replace, the Embedded Software (or the relevant part of it); or

5.5.2 correct the Documentation to reflect the proper performance of the Software where it is determined by the Company (acting reasonably) that the Software is functioning correctly but is not properly described in the Documentation.

5.6 The repair or replacement of the Embedded Software under Clause 5.5 will not be available to the Customer if:

5.6.1 the defect in the Embedded Software is attributable to failure or breakdown or interference of any third party, or software or hardware not supplied subject to this EULA;

5.6.2   the Customer is in breach of this EULA;

5.6.3   the Customer fails to operate the Hardware properly or fails to follow the instructions or recommendations of the Company as set out in the Documentation with respect to the Embedded Software;

5.6.4   the Customer interferes with, modifies, or fails to secure the Embedded Software otherwise than in accordance with the terms of this EULA;

6.   Training

Other than the supply of the Documentation included with the Embedded Software, no training is provided by the Company unless otherwise agreed by the Customer and the Company.

7.   Limit of Liability

7.1   Subject to Clause 7.2 and 7.3, the Company's maximum aggregate liability in connection with this EULA or the use of the Embedded Software will be limited to the lower of:

7.1.1   any applicable limitation of liability set out in the Commercial Terms; or

7.1.2   £100,000 or 100% of the price paid for the Hardware, whichever is lower.

7.2   Subject to Clause 7.3, the Company accepts no liability for any:

7.2.1   loss of business, loss of revenue, loss of profits, loss of goodwill, loss of use, loss of data or loss of any economic liability; or

7.2.2   indirect or consequential losses, however caused, arising in connection with this EULA or the use of the Embedded Software.

7.3   The Company makes no attempt to exclude liability relating to or arising from death or personal injury caused by the Company's negligence or the negligence of any employee, agent or contractor of the Company or liability for fraud or fraudulent misrepresentation, or for any other liability for which it would be unlawful to exclude or limit liability.

8.   Disposal

The Customer undertakes that, upon the cessation of the use of the Hardware for whatever cause, or upon termination of this EULA, it will promptly destroy all known copies of the Embedded Software on any media other than the copy embedded in the Hardware and, if required by the Company, certify that this has been done.

9.   Force Majeure

Neither party shall be liable for failure to perform its obligations under this EULA if such failure results from circumstance beyond the party's control.

10.   Termination

Either party shall have the right to terminate this EULA if the other party is in material or persistent breach of this EULA and fails to rectify such breach within 30 days of receipt of notification thereof in writing, from the injured party, or if a right to terminate the relevant Commercial Terms has arisen. Termination shall not affect any other rights of the injured party.

11.   Consequences of Termination

Upon termination of this EULA all rights and licences granted to the Customer under this EULA will cease immediately.

12.   Communications and Notices

12.1   All communications or notices that the Customer is required to provide to the Company under this EULA shall be sent to the following address:

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

Traka – ASSA ABLOY
30 Stilebrook Road, Olney,
Milton Keynes, MK46 5EA, United Kingdom

or such other address of which the Company makes the Customer aware from time to time.

12.2   Any notice given in accordance with Clause 12.1 will be deemed to have been served:

12.2.1   if delivered to or left at the Company's address, at the time the notice is delivered to or left; or

12.2.2   if delivered by pre-paid first class post or mail delivery service providing proof of delivery, at 9:00am on the second Business Day after the date of posting.

13.   Assignment

Except as expressly set out in this EULA or as permitted by law, the Customer will not be permitted to assign, transfer, charge, hold on trust for any person or deal in any other manner with any of its rights under this EULA without the prior written consent of the Company.

14.   Waiver

A delay in exercising or failure to exercise a right or remedy under or in connection with this EULA will not constitute a waiver of, or prevent or restrict future exercise of, that or any other right or remedy, nor will the single or partial exercise of a right or remedy prevent or restrict the further exercise of that or any other right or remedy.

15.   Severance

If any term of this EULA is found by any court or body or authority of competent jurisdiction to be illegal, unlawful, void or unenforceable, such term will be deemed to be severed from this EULA and this will not affect the remainder of this EULA which will continue in full force and effect.

16.   Rights of Third Parties

The parties do not intend that any term of this EULA will be enforceable under the Contracts (Rights of Third Parties) Act 1999 by any person.

17.   Law

17.1   This EULA (and any non-contractual obligations arising out of or in connection with it) is governed by the laws of England and Wales and the parties submit to the jurisdiction of the Courts of England and Wales.

Data Protection Laws

17.2   The Customer acknowledges that for the purposes of the Data Protection Laws, to the extent any Personal Data is involved in its use of the Hardware and Embedded Software, the Customer will be the Data Controller in respect of such Personal Data.

17.3   In limited circumstances, the Company may have access to data stored on the Hardware which may include user names or other Personal Data relating to the Customer's employees or authorized users ("Agreement Personal Data") where such access is required in order to provide support under the Warranty or any hardware maintenance agreement entered into by the Customer and the Company. The Customer authorises the Company to Process Agreement Personal Data during the term of this EULA as a Data Processor for the purposes of performing its obligations under this EULA only.

17.4   The Customer authorises the Company to appoint sub-processors of Agreement Personal Data and agrees to the use of the Company's existing sub-processors of Agreement Personal Data (each an "Authorised Sub-Processor").

17.5   The Customer shall:

17.5.1   comply with the Data Protection Laws;

17.5.2   ensure that only the Personal Data that the Company requires in order to perform its obligations under this EULA will be disclosed to, shared with and/or accessible by the Company; and

17.5.3 obtain all necessary consents and/or provide all fair processing notices required under the Data Protection Laws to enable the Company to lawfully receive, store, disclose and/or use all Agreement Personal Data (whether by itself or Authorised Sub-Processors) for the purpose of performing its obligations and exercising its rights under this EULA and as otherwise agreed by the parties from time to time.

17.6 The Company:

17.6.1 may appoint Authorised Sub-Processors in connection with the performance of its obligation under this EULA; and

17.6.2 shall provide notification of changes to Authorised Sub-Processors of Agreement Personal Data to the Customer at least 14 calendar days in advance to provide the Customer with the opportunity to object to the change. The Customer shall be deemed to accept the change if an objection is not received within 10 calendar days of notification. If an objection is received then the parties will work together in good faith to achieve an agreed outcome and any Authorised Sub-Processors appointed shall be appointed on terms the same as this EULA and the Company shall remain liable for the acts and omissions of such Authorised Sub-Processors.

17.7 The Company warrants that, if acting as a Data Processor, it shall:

17.7.1 Process the Agreement Personal Data only for the purpose of performing its obligations under this EULA and on such documented instructions received from the Customer from time to time as are reasonable, necessary and relevant to enable each party to perform its obligations under this EULA, save where required by Applicable Law and in such case the Company shall notify the Customer of the nature and extent of the Applicable Laws preventing such Processing (unless to do so would itself be a contravention of any Applicable Law); and

17.7.2 put in place appropriate technical and organisational security measures to the standard required under the Data Protection Law ("Security Measures") and shall provide reasonable assistance with any privacy impact assessment(s) that may be required of the Company under the Data Protection Laws which relate to the Processing of Agreement Personal Data under this Agreement.

17.8 From the 25 May 2018, the Company warrants that, if acting as a Data Processor, it shall:

17.8.1 notify the Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed ("Data Security Breach"). Where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay;

17.8.2 except to Authorised Sub-Processors, not disclose the Agreement Personal Data to a third party save as required for the performance of its obligations under this EULA, as otherwise provided under this EULA, or as required by Applicable Law;

17.8.3 notify the Customer without undue delay of any notice or communication from the Supervisory Authority which relates directly to the Processing of Agreement Personal Data;

17.8.4 ensure that any individual authorised to Process Agreement Personal Data on behalf of the Customer is subject to appropriate statutory or contractual obligation of confidentiality;

17.8.5 will upon reasonable notice, no more than once in any one calendar year, subject to appropriate confidentiality agreements being entered into, make available to the Customer all reasonable information relating to the Processing of Agreement Personal Data necessary to demonstrate compliance with the obligations set out in this EULA to the extent such information is not already available to the Customer; and allow for and contribute to one audit in any one calendar year, including inspection, conducted by the Customer or another auditor mandated by the Customer to that same extent solely to the extent relevant to the Processing of Agreement Personal Data;

17.8.6 to the extent required by Data Protection Laws, notify and provide reasonable assistance to the Customer on receiving any:

17.8.6.1 complaint by a Data Subject in respect of their Personal Data contained in the Agreement Personal Data or any request received from a Data Subject to have access to his Personal Data (or to exercise any other right(s) afforded to him under the Data Protection Laws) as contained in the Agreement Personal Data (including by appropriate technical and organisational measures, insofar as this is possible);

17.8.6.2 notice or communication from the Supervisory Authority which relates to the processing of Agreement Personal Data;

17.8.7   to the extent required by Data Protection Laws, reasonably assist the Customer in:

           17.8.7.1   taking measures to address any Data Security Breach; and

           17.8.7.2   conducting privacy impact assessments of any Processing operations and consulting with any applicable Supervisory Authority;

17.8.8   only share Agreement Personal Data with the Authorised Sub-Processors to carry out the services provided that, to the extent the Authorised Sub-Processor is located outside the UK or the European Union, the Company will implement measures to ensure an adequate level of protection for the rights and freedoms of the relevant individuals in relation to the transfer of any Personal Data, except to the extent that the transfer is (i) to a country that the European Commission has recognised as providing adequate protection for such transfer from time to time and/or (ii) otherwise expressly permitted by Data Protection Laws.

17.9   At the option of the Customer, the Company shall securely delete or return to the Customer all Agreement Personal Data promptly following termination of this EULA and shall securely delete any remaining copies.

18.   Entire Agreement

18.1   Subject to Clause 18.2, the parties agree that these terms and conditions (together with any Commercial Terms) represent the entire agreement between the parties relating to the licence of the Embedded Software, and that no statements or representations made by either party have been relied on by the other in agreeing to enter into the EULA and the parties shall have no remedy in respect of any such statement or representation which is not set out in this EULA.

18.2   Unless otherwise specified in the Commercial Terms, if the Customer also enters into a hardware maintenance agreement with the Company then the Customer's rights and obligations under Clause 5.5 and Clauses 17.2-17.9 (inclusive) will apply for the duration of the relevant hardware maintenance agreement by changing only those things which require to be changed in order to retain the meaning of those Clauses.

NOTE: v3.1 of this EULA, published on 1/Oct/2022 reflects the new legal entity, ASSA ABLOY Global Solutions UK Ltd, and contains no other changes from v3 published in 2018.