

TRAKA TOUCH PRO KEY CABINET USER GUIDE

UD0258

23/10/24

VERSION 1.6

CONTENTS

Contents	1
GDPR Compliance Information	7
1. Introducing Traka.....	8
2. Traka Contact Details	9
3. Product Details	10
3.1 Electrical Rating	10
3.1.1 Traka Touch Pro Series	10
3.2 Battery backup:	10
3.3 Weight:.....	10
3.4 Environmental Rating	10
3.5 Approvals & Compliance Level	10
3.5.1 Product Compliance	10
3.5.2 Business Compliance.....	10
4. What and Whom is this Guide For?	11
5. Traka Cabinet and item Diagrams	12
5.1 Cabinet Types.....	12
5.1.1 Traka Touch Pro Key Cabinet Models.....	12
5.1.2 Traka Touch Pro M Key Cabinet Model.....	13
5.1.3 Traka Touch Pro S Key Cabinet Model	14
5.1.2 Traka Touch Pro L Key Cabinet Model.....	15
5.1.4 Traka Touch Pro V Key Cabinet Model	16
5.2 Cabinet Diagram Touch Pro M, S & L.....	17
5.2.1 System Key	17
5.3 Cabinet Diagram Touch Pro V	18
5.3.1 System Key	18
5.4 iFob (Intelligent fob) & Key Bunch Diagram	19
5.4.1 iFob Diagram Key	19
5.5 USB Memory Sticks	20
6. Overview	21
6.1 TrakaWEB	21
6.2 The Touch Screen.....	21
6.2.1 Screen Saver	21
6.2.2 Touch Commands.....	21

6.2.3	Top Bar Icons	22
7.	Types of Identification	23
7.1	Other Types of Identification.....	23
7.1.1	Keypad ID Only Access	23
7.1.2	Keypad and PIN Access	23
7.1.3	Credential ID Only Access.....	23
7.1.4	Credential ID and Pin Access.....	24
7.1.5	Fingerprint Access	24
7.1.6	Fingerprint and PIN Access	24
7.2	Granular User Permissions.....	25
7.3	Multiple ID & PIN Attempts.....	31
8.	Users.....	33
8.1	Creating the First Admin User	33
8.2	Adding more Users	38
8.3	Editing Users	43
8.4	Deleting users.....	44
8.5	Supporting a Large Number of Users	45
8.6	User Enrolment ID.....	47
9.	Item Administration.....	50
9.1	Initial Setup	50
9.2	Deallocating an iFob	52
9.3	Allocating an iFob.....	54
9.4	Replacing an iFob	55
9.5	Relocating an iFob Within The Same System.....	58
9.6	Relocating an iFob From One System to Another	61
9.6.1	Relocating Items within a Common Item Access Group	64
9.6.2	Relocating Items within an Item Access Group	64
9.6.3	Relocating Items With an Associated Booking.....	64
9.6.4	Relocating Paired Items.....	64
9.6.5	Relocating Items With an Associated Access Schedule.....	64
10.	Changing the Clock Settings	65
11.	System Operation	66
11.1	Removing an Item.....	66
11.2	Override of an Empty Slot	68
11.3	Returning an Item	68

11.4	Item in Wrong Slot	68
11.5	No Door Systems	68
11.6	Non-Locking Receptor Strips.....	69
11.7	Auto Open All Doors on Login	69
11.8	Attaching Keys to iFobs.....	69
11.8.1	Keyrings.....	69
11.8.2	Security Seals	69
12.	Reports.....	70
12.1	Generating and Exporting Reports	70
12.2	Exporting Reports.....	73
13.	Advanced User Guide.....	75
13.1	Item Release Screen.....	75
13.1.1	Searching for Items	75
13.1.2	I Know What I Want.....	77
13.2	New PIN.....	77
13.3	Search Report.....	78
13.4	Item Authorisation	80
13.4.1	Setting up the Items	80
13.4.2	User Process	81
13.4.3	Authoriser from a Different Group on Removal & Return	82
13.5	Exporting & Importing	86
13.5.1	Exporting Users	87
13.5.2	Importing Users	88
13.6	General Options	92
13.7	Network Administration.....	95
13.7.1	Enforce TLS 1.2.....	96
13.7.2	NIC (Network Interface Controller) Settings	96
13.7.3	Simple Network Management Protocol (SNMP)	98
13.7.4	802.1X Support.....	100
13.7.5	Communication Status	104
13.7.6	Add the New CA Certificate into the Traka Touch 'Root Store' (V2.3.0 & Later)	105
13.7.7	Add the new CA Certificate into the Traka Touch 'Root Store' (Pre V2.3.0).....	108
13.8	Reader Administration	109
13.9	Search Facility	110
13.10	Languages.....	111

13.10.1	Changing the Language for a Single Login	111
13.10.2	Changing Languages for a User	112
13.10.3	Changing the Default Language of the System	113
13.11	Alarms	113
13.11.1	Multiple Alarm Outputs Per Relay	114
13.11.2	Table of Alarm Events	116
13.12	Curfews.....	117
13.12.1	Items with a 'Specific Time of the Day' Curfew	117
13.12.2	Items with a 'Number of Days, Hours and Minutes' Curfew	119
13.12.3	Users with a 'Specific Time of the Day' Curfew	120
13.12.4	Users with a 'Number of Days, Hours and Minutes' Curfew	121
13.12.5	All Curfews	122
13.12.6	Supress Curfew Acknowledgement.....	123
13.13	Data Settings.....	124
13.14	Power Settings	126
13.15	Configuration	127
13.16	Help.....	129
13.16.1	Viewing the Help Section	129
13.16.2	Changing the Help Section.....	129
13.17	Backing Up The Traka Touch Database.....	130
14.	Sagem MorphoSmart Reader	132
14.1	Introduction	132
14.2	System Requirements.....	132
14.2.1	Sagem Reader Models.....	132
14.2.2	Traka Touch Operating System.....	132
14.2.3	Traka Touch Application	132
14.3	Access Methods.....	133
14.4	Reader Disconnection / Reconnection	133
14.5	How to Enrol a User.....	133
14.5.1	Manual Enrolment by Admin	134
14.5.2	Enrolment ID	136
14.6	How to Access The System	137
14.7	Removing a Fingerprint Template	138
14.8	Tips on Enrolling	139
14.9	FAR	140

15.	Remote System Lockdown.....	141
15.1	Requirements	141
15.2	Using the System	141
15.2.1	Events.....	142
16.	RRSS (Random Return to Single System).....	143
16.1	System Requirements.....	143
16.2	RRSS Overview	143
16.3	Item Setup.....	143
16.4	Item Replacement.....	144
16.5	Granting Access to Items	145
17.	Tamper Switches	146
18.	Feature Options	147
18.1	Feature Options Overview	147
18.2	Fault Logging.....	147
18.3	Reason Logging	147
18.4	Notes Logging.....	147
18.5	Custom Messages.....	147
18.6	Email Notifications.....	148
18.7	Item Booking.....	148
18.8	Fuel, Distance & Location Logging	148
18.9	Item Handover.....	148
18.10	Random Return to Multiple Systems (RRMS).....	149
18.11	Advanced FIFO.....	149
18.12	Access Schedules	149
18.13	Real-Time Update Service.....	150
18.14	Temporary Key Store (TKS).....	150
18.15	Item Pairing & Locker Pairing	150
18.16	Allowance Across Systems (AAS).....	151
18.17	Multiple Credentials	151
19.	General Maintenance	152
19.1	Cleaning Guidance.....	152
19.1.1	Cleaning Procedure for Traka Cabinet.....	152
19.1.2	Cleaning the Touch Screen.....	152
19.1.3	Ifobs.....	152
19.1.4	Warranty Statement	152
19.2	Powering On/Off the System.....	153

19.3	Manually Opening the Door For Emergency Access	154
19.3.1	Traka Touch Pro V	154
19.3.2	Traka Touch Pro M, S & L	154
19.3.3	Opening the Receptor Strip Frame(s)	154
19.4	Replacing iFobs.....	157
19.5	Accessing The System	159
19.6	Serial Number/Rating Plate Location	160
19.6.1	Traka Touch Pro V	160
19.6.2	Traka Touch Pro M, S & L	160
19.7	Battery Connection/Disconnection	161
19.7.1	Traka Touch Pro V Battery Location	161
19.7.2	Traka Touch Pro M, S & L Battery Location.....	162
19.7.3	Battery Connection Details.....	163
19.8	Zip and Export All Log Files and SQL CE Database to USB.....	164
20.	Product Disconnection	166
20.1	Mains Disconnection	166
20.2	Battery Disconnection	166
21.	Technical Support	167
22.	End User Licence Agreement – Embedded Software.....	168

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 as 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. 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 WHOM 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 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 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. 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.

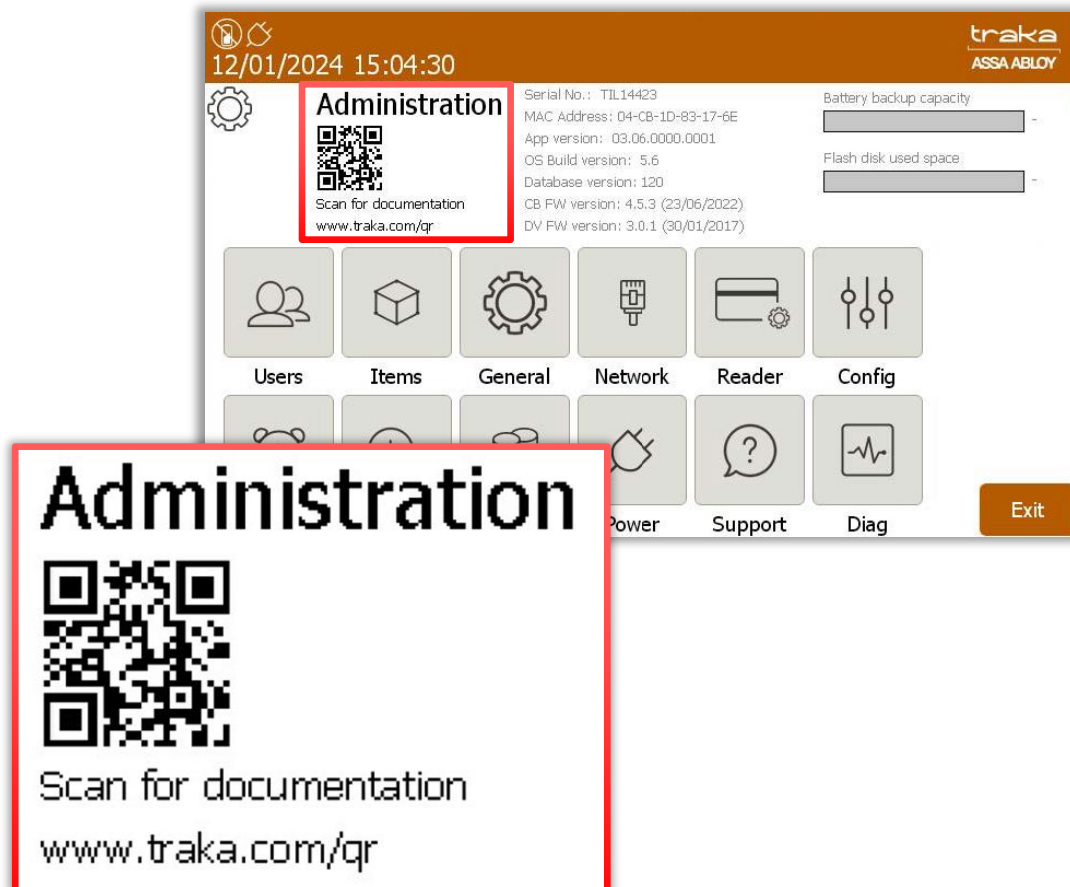


Figure 1 – QR code in the Traka Touch Administration menu

5. TRAKA CABINET AND ITEM 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 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



Figure 4 – Traka S-Touch

The Touch Pro S Key cabinets are a versatile solution allowing for system scalability. Accommodate up to 60 keys (120 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



Figure 5 – Traka L-Touch

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



Figure 6 – Traka V-Touch

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

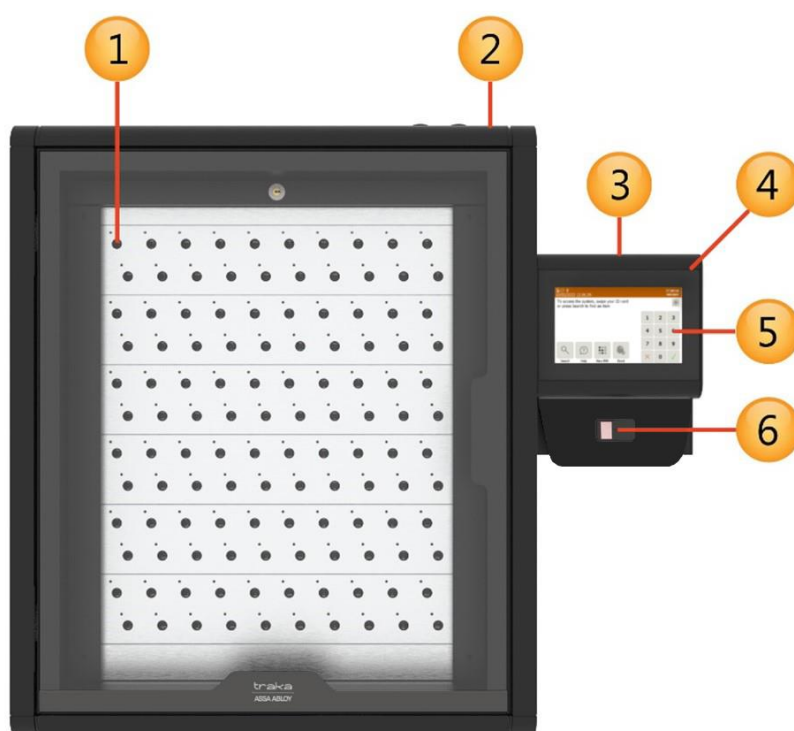


Figure 7 – Traka Touch Pro Key Cabinet diagram

5.2.1 SYSTEM KEY

1. Cabinet 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.

2. 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.

3. Control Pod

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

4. 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.

5. Card/Proximity 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.

6. Receptor Slot

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.



Figure 8 – Traka Touch Pro Key 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 IFOB (INTELLIGENT FOB) & KEY BUNCH DIAGRAM

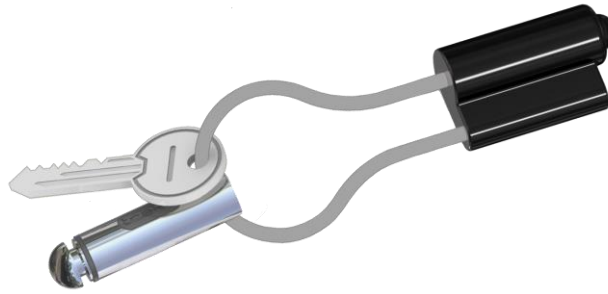


Figure 9 – Key bunch diagram

5.4.1 IFOB DIAGRAM KEY

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.



Figure 10 – USB memory stick

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. For Traka Touch Key Cabinets with doors, the USB port will be located behind the door. Some Locker systems and Rack Management 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.

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.

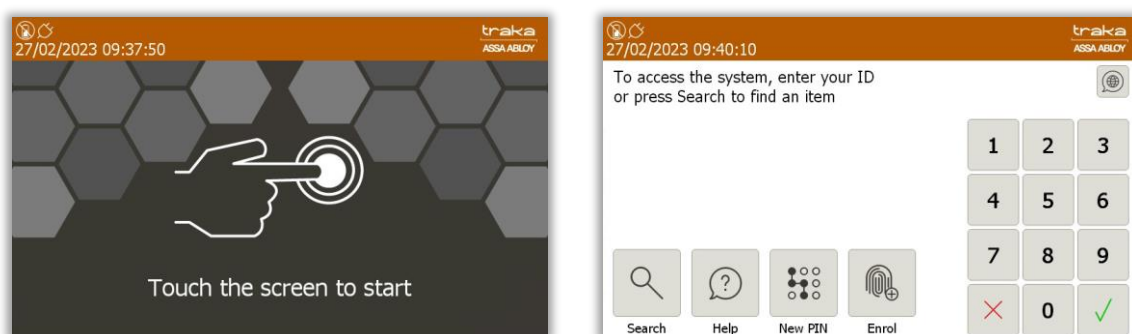
6.1 TRAKAWEB

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.

6.2.2 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 will scroll through the various options.

6.2.3 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.



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 themselves to the Traka Touch system is able to use a Keypad ID (as described below).

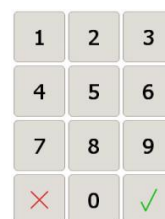
7.1 OTHER TYPES OF IDENTIFICATION

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.

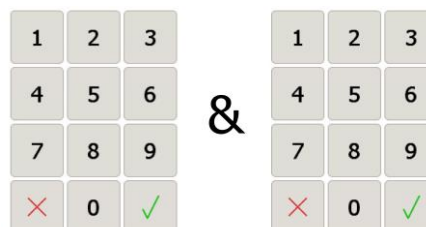
7.1.1 KEYPAD ID ONLY ACCESS

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.



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.



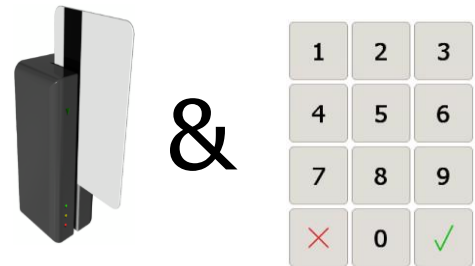
7.1.3 CREDENTIAL ID ONLY ACCESS

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



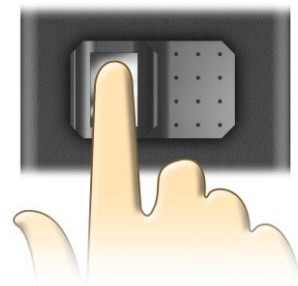
7.1.4 CREDENTIAL ID AND PIN ACCESS

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.



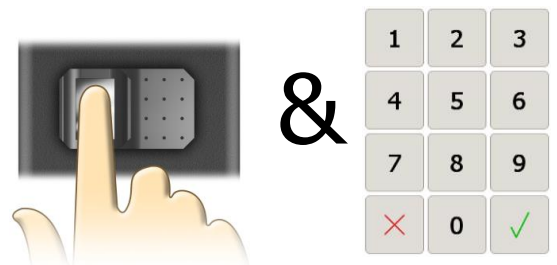
7.1.5 FINGERPRINT ACCESS

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.

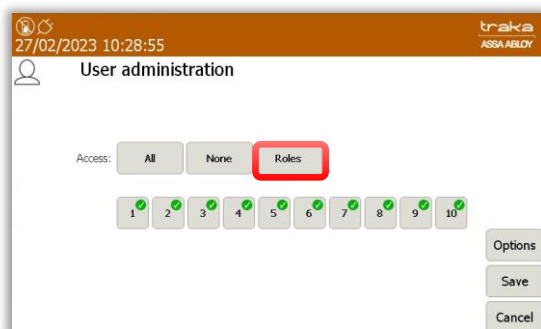


NOTE: There is an event within Traka Touch called 'Duress via PIN +/-1'. This is triggered to notify a duress situation. After a user has accessed the system either by Credential ID or fingerprint, they must input their PIN number + or - 1 digit of their actual PIN number to activate the event. For example, 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.



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 may only be assigned from TrakaWEB, these will include many of the cost option override features.

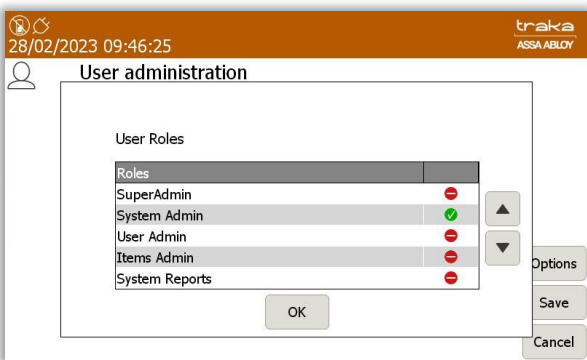
Super Admin Role



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



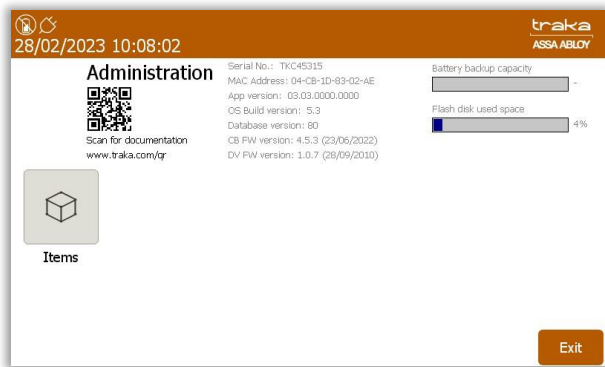
Selecting this option will provide an Admin role to grant/revoke the ability to edit User records such as adding or removing users or assigning items to users.



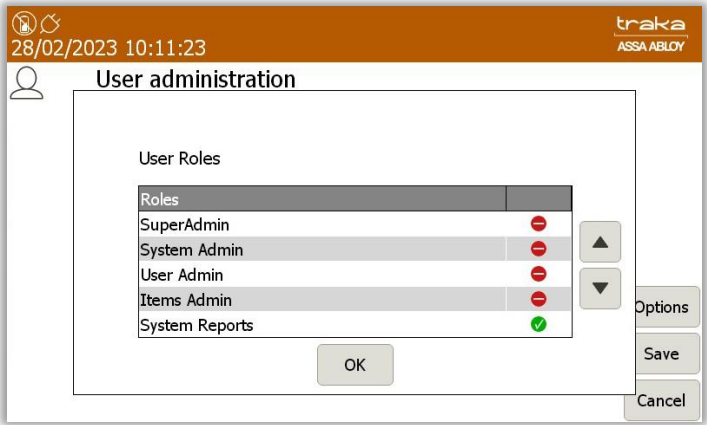
Items Admin Only Role



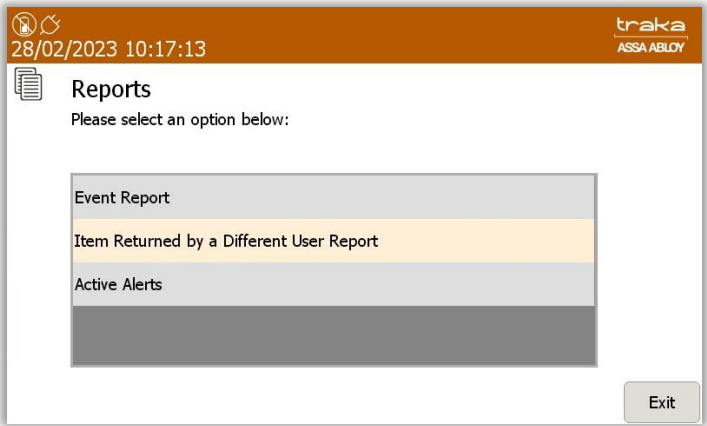
Selecting this option will add an Item admin role which will grant/revoke the ability to administer Item records, enabling a user to access items or replace damaged or broken iFobs.



System Reports Only

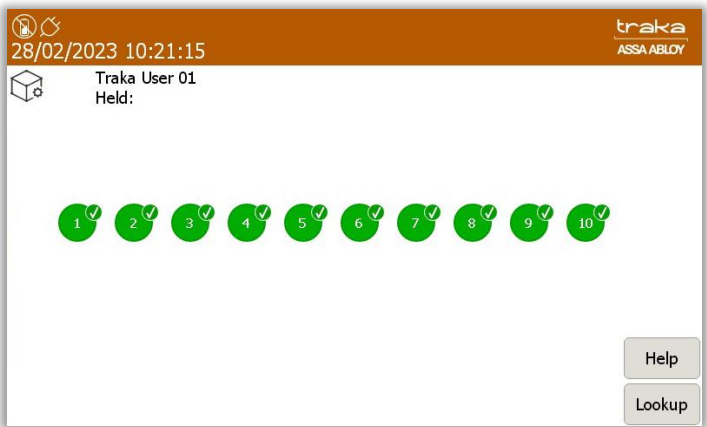


Selecting this option will allow the user to view & run reports at the Traka Touch system.



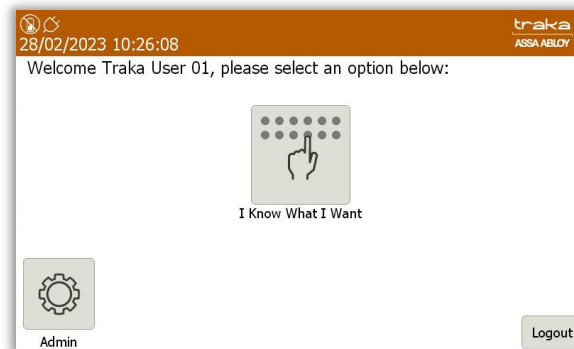
Users with Item Only Permissions

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.



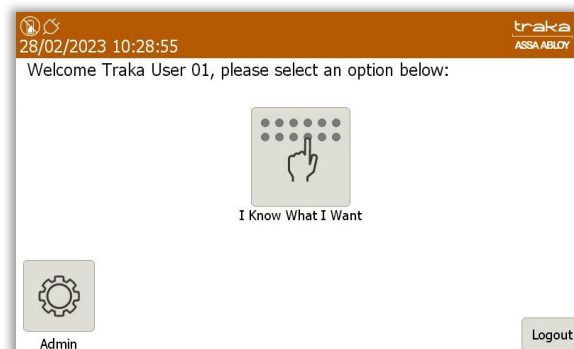
Users with System Admin & Items

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.



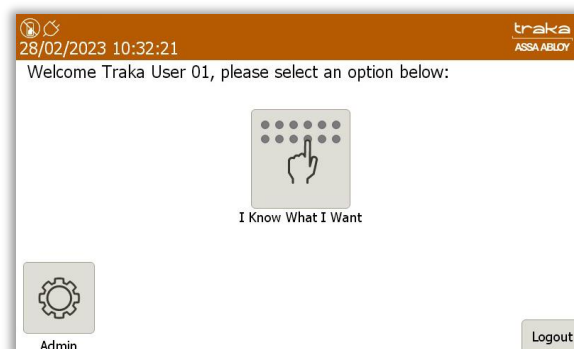
Users with User Admin & Items

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.



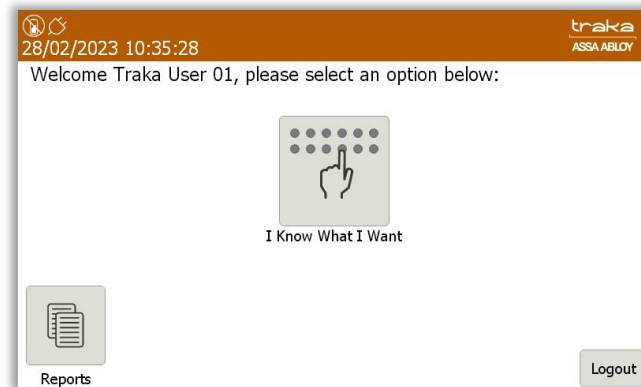
Users with Item Admin & Items

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.



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.

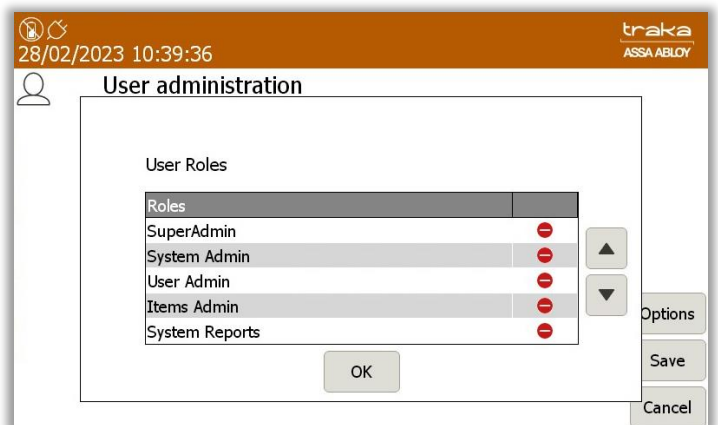


From the User Roles screen, it is also possible to create different combinations of roles that can be assigned to specific users. These can be applied to users with access to both admin roles and items or admin roles only.

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

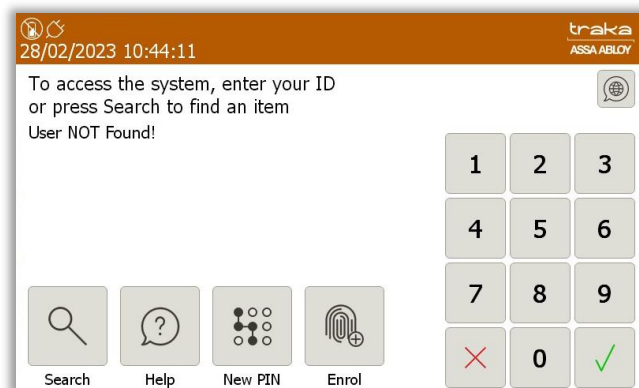


7.3 MULTIPLE ID & PIN ATTEMPTS

Multiple ID Attempts

A user that has been assigned with ID access maybe 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:

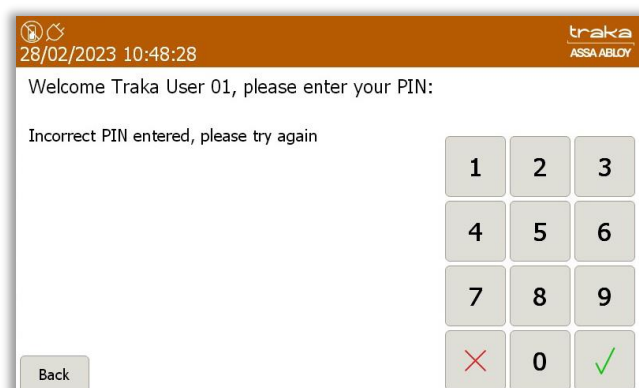


The number of attempts can be set via a configuration through Traka and also through [General Options](#) in Traka Touch. The value can be set between 0-10. However, setting the value to zero will still display the **User NOT Found!** Message after an unsuccessful ID entry but no report will be generated.

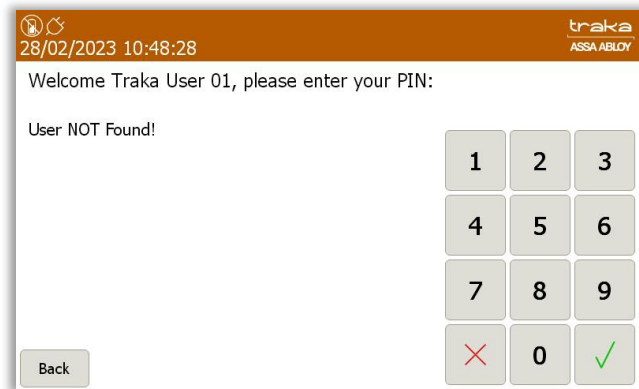
Multiple PIN Attempts

A user that has been assigned with a PIN maybe granted a number of 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:



If by the third attempt, the user still enters an incorrect PIN, they will see the following message on the screen:



The screenshot shows a mobile application interface for Traka. At the top, there is a status bar with the date and time '28/02/2023 10:48:28' and the Traka logo with 'ASSA ABLLOY' underneath. Below the status bar, the text 'Welcome Traka User 01, please enter your PIN:' is displayed. Underneath this, the message 'User NOT Found!' is shown. To the right of the message is a numeric keypad with buttons for digits 1 through 9, 0, a red 'X' for backspace, and a green checkmark for confirmation. At the bottom left of the screen is a 'Back' button.

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.

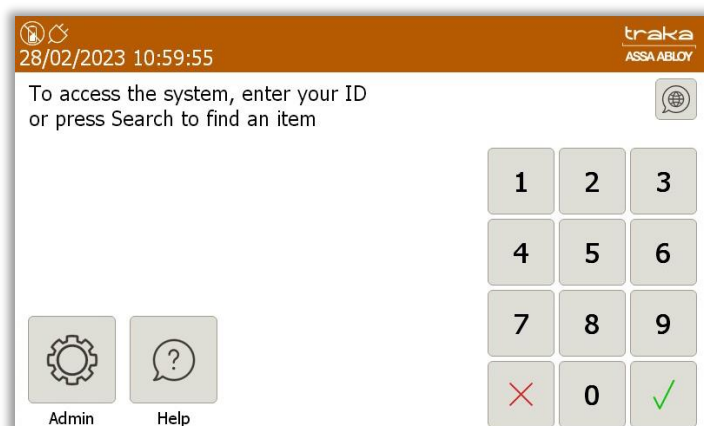
The number of attempts can be set via a configuration through Traka and also through [General Options](#) in Traka Touch. The value can be set between 0-10. However, setting the value to zero will only display the **User NOT Found!** Message after an unsuccessful PIN entry. The user will not be logged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

8. USERS

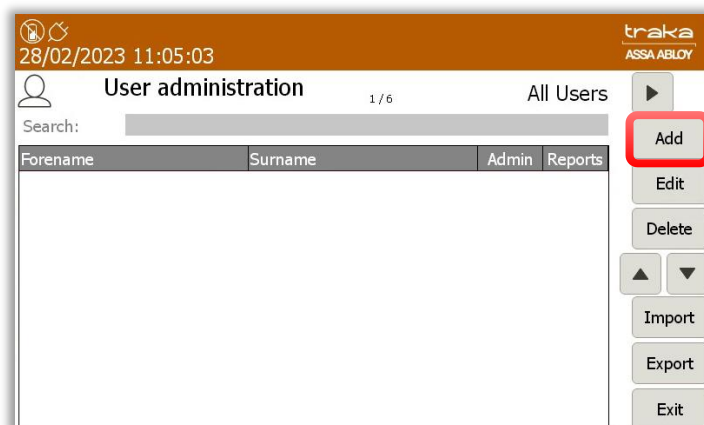
8.1 CREATING THE FIRST ADMIN USER

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 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 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 system will automatically fill in the field for you.

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

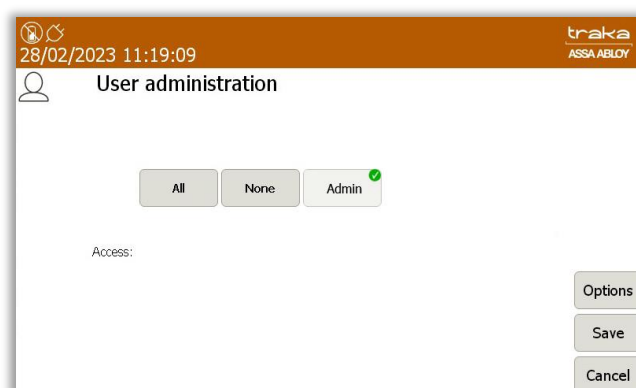
8. From the Access screen select which items you wish to have access to and whether or not you wish to view and export key reports. Each of the access buttons on screen corresponds with an item in the system. E.g., The '1' button will only grant or remove access to the item in position 1. The tick and 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.



The screenshot shows the 'User administration' screen with a header bar containing the date '28/02/2023 11:19:09' and the 'traka ASSA ABLLOY' logo. Below the header, there is a 'User administration' title and a profile icon. Underneath, there are three buttons: 'All', 'None', and 'Roles'. Below these, there is a row of 10 buttons numbered 1 to 10, each with a green checkmark icon. To the right of these buttons are three more buttons: 'Options', 'Save', and 'Cancel'.

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:



The screenshot shows the 'User administration' screen with a header bar containing the date '28/02/2023 11:19:09' and the 'traka ASSA ABLLOY' logo. Below the header, there is a 'User administration' title and a profile icon. Underneath, there are three buttons: 'All', 'None', and 'Admin'. The 'Admin' button has a green checkmark icon. Below these buttons, there is a label 'Access:'. To the right of the buttons are three more buttons: 'Options', 'Save', and 'Cancel'.

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.



The screenshot shows the 'User administration' screen with a header bar containing the date '28/02/2023 12:23:23' and the 'traka ASSA ABLLOY' logo. Below the header, there is a 'User administration' title and a profile icon. Underneath, there are four labels: 'Start Date: 27/02/2023 08:43', 'Expiry Date: 27/02/2023 08:43', 'PIN Expiry Date: 29/03/2023 08:43', and 'Force user to change PIN on next login:'. To the right of these labels are three buttons: 'Next', 'Save', and 'Cancel'.

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:

The screenshot shows the 'User administration' screen with a date picker for 'Start Date'. The date picker is set to February 27, 2023, at 08:43. The background shows fields for Start Date, Expiry Date, PIN Expiry Date, and Force use. The date picker has 'Set' and 'Cancel' buttons.

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:

The screenshot shows the 'User administration' screen with a date picker for 'Expiry Date'. The date picker is set to December 31, 2050, at 08:43. The background shows fields for Start Date, Expiry Date, PIN Expiry Date, and Force use. The date picker has 'Set' and 'Cancel' buttons.

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:

The screenshot shows the 'User administration' screen with a date picker for 'PIN Expiry Date'. The date picker is set to February 28, 2023, at 08:43. The background shows fields for Start Date, Expiry Date, PIN Expiry Date, and Force use. The date picker has 'Set' and 'Cancel' buttons.

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.

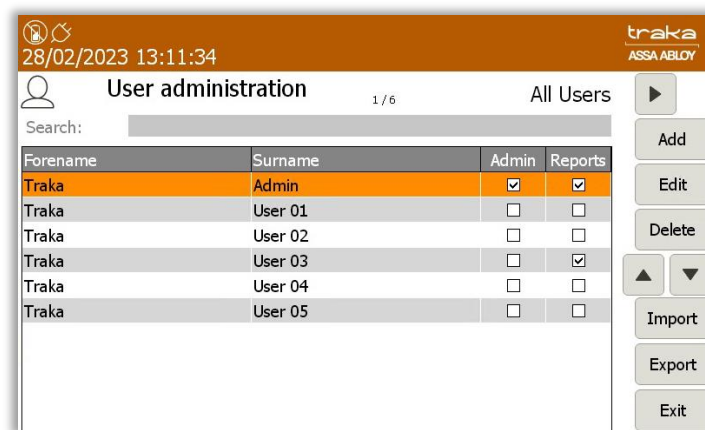
User Curfew Type

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.

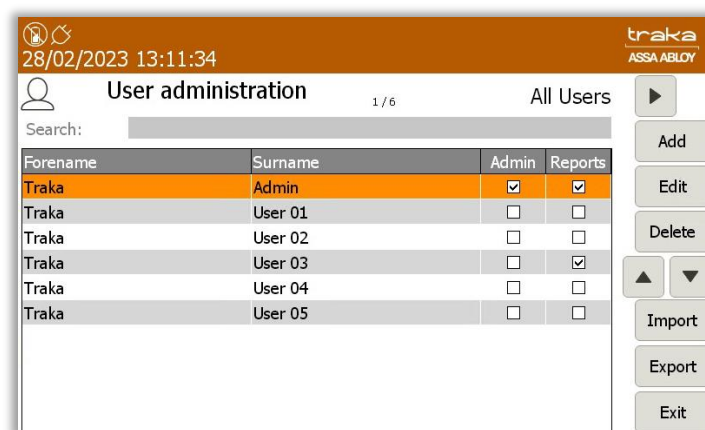
After adding the user, you will be taken back to the User Admin page.



The screenshot shows the 'User administration' page with a search bar and a table of users. The table has columns for Forename, Surname, Admin, and Reports. The 'Admin' column has checkboxes, and the 'Reports' column has checkboxes. The 'Add' button is highlighted.

Forename	Surname	Admin	Reports
Traka	Admin	☒	☒
Traka	User 01	☐	☐
Traka	User 02	☐	☐
Traka	User 03	☐	☒
Traka	User 04	☐	☐
Traka	User 05	☐	☐

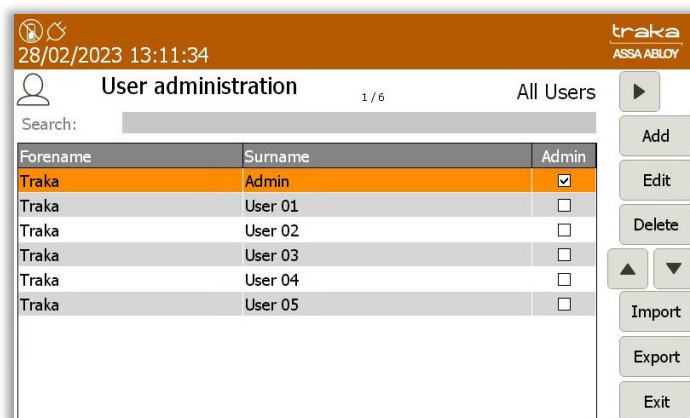
To add more users simply click the **Add** button and repeat this process. After adding the user, you will be taken back to the User Admin page.



The screenshot shows the 'User administration' page with a search bar and a table of users. The table has columns for Forename, Surname, Admin, and Reports. The 'Admin' column has checkboxes, and the 'Reports' column has checkboxes. The 'Add' button is highlighted.

Forename	Surname	Admin	Reports
Traka	Admin	☒	☒
Traka	User 01	☐	☐
Traka	User 02	☐	☐
Traka	User 03	☐	☒
Traka	User 04	☐	☐
Traka	User 05	☐	☐

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.

16/10/2024 10:35:21

traka ASSA ABLOY

User administration

Forename: Traka

Surname: User 1

Display Name: Traka User 1

Keypad ID: 1111

Credential ID:

Enrolment ID:

PIN:

Language: (English (UK))

12? 1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

[A] a s d f g h j k l .

z x c v Space b n m ,

Access

Save

Cancel

08/10/2024 10:55:12

traka ASSA ABLOY

User administration

Forename: Traka

Surname: User 1

Display Name: Traka User 1

Keypad ID: 1111

Credential ID: Available in TrakaWeb

Enrolment ID:

PIN:

Language: (English (UK))

12? 1 2 3 4 5 6 7 8 9 0

Q W E R T Y U I O P

[A] A S D F G H J K L .

Z X C V Space B N M ,

Access

Save

Cancel

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.

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.

NOTE: If your Traka Touch has RRMS enabled, you will not have the option to select which iFobs the user has access to.

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

The screenshot shows the 'User administration' screen in the Traka system. At the top, there is a header bar with the date and time '28/02/2023 14:52:28' and the Traka logo. Below the header, there is a user icon and the text 'User administration'. Underneath, there is an 'Access:' label followed by three buttons: 'All', 'None', and 'Roles'. Below these buttons, there is a row of 10 numbered buttons (1 to 10). Buttons 1, 2, 5, 6, and 10 have a green checkmark, while buttons 3, 4, 7, 8, and 9 have a red minus sign. To the right of the numbered buttons, there are three buttons: 'Options', 'Save', and 'Cancel'.

NOTE: If you have RRMS enabled, the option to allocate iFobs to users is not available as shown in the example below:

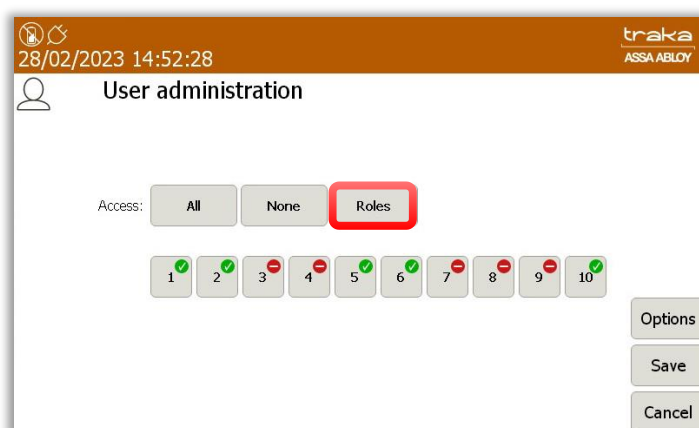
The screenshot shows the 'User administration' screen in the Traka system, similar to the previous one. However, in this version, the row of 10 numbered buttons (1 to 10) is missing. The 'Access:' label and the 'All', 'None', and 'Roles' buttons are still present. The 'Options', 'Save', and 'Cancel' buttons are also present on the right side.

9. From the Access screen, select which items you wish to have access to and whether or not you wish to view and export key 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.

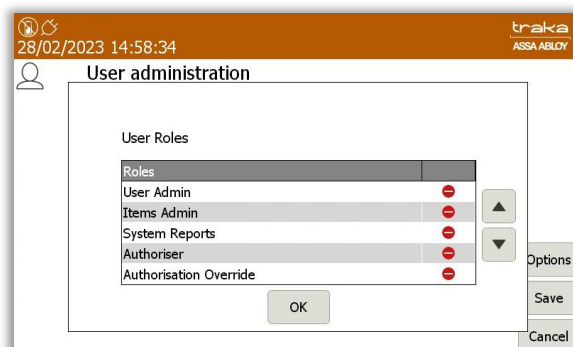
NOTE: Item Access Groups is a TrakaWEB feature. It does not apply to stand-alone systems. For more information on Item Access Groups, refer to the TrakaWEB User Guide - UD0018 or UD0260 - TrakaWEB Version 4 User Guide.

Roles

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. 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.



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.

traka
ASSA ABLOY

28/02/2023 15:01:07

User administration

Start Date: 27/02/2023 14:57

Expiry Date: 27/02/2023 14:57

PIN Expiry Date: 30/03/2023 11:27

Force user to change PIN on next login:

Next
Save
Cancel

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 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:

traka
ASSA ABLOY

28/02/2023 13:03:42

User administration

Start Date: 27/

Expiry Date: 27/

PIN Expiry Date: 29/

Force use

Start Date:

Day	Month	Year	Hour	Minute
25		2021	06	41
26	January	2022	07	42
27	February	2023	08	43
28	March	2024	09	44
	April	2025	10	45

Set Cancel

Next
Save
Cancel

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:

traka
ASSA ABLOY

28/02/2023 13:06:49

User administration

Start Date: 27/

Expiry Date: 27/

PIN Expiry Date: 29/

Force use

Expiry Date:

Day	Month	Year	Hour	Minute
29	October	2048	06	41
30	November	2049	07	42
31	December	2050	08	43
			09	44
			10	45

Set Cancel

Next
Save
Cancel

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:

The screenshot shows a 'User administration' interface. A pop-up window titled 'PIN Expiry Date:' is displayed, allowing selection of a date and time. The date is set to 28 February 2023, and the time is 08:43. The background interface includes fields for 'Start Date: 27/...', 'Expiry Date: 27/...', 'PIN Expiry Date: 29/...', and 'Force use'. There are also 'Set' and 'Cancel' buttons for the pop-up, and 'Next', 'Save', and 'Cancel' buttons for the main interface. The top status bar shows the date '28/02/2023 13:08:55' and the 'traka ASSA ABLLOY' logo.

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 iFob 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.

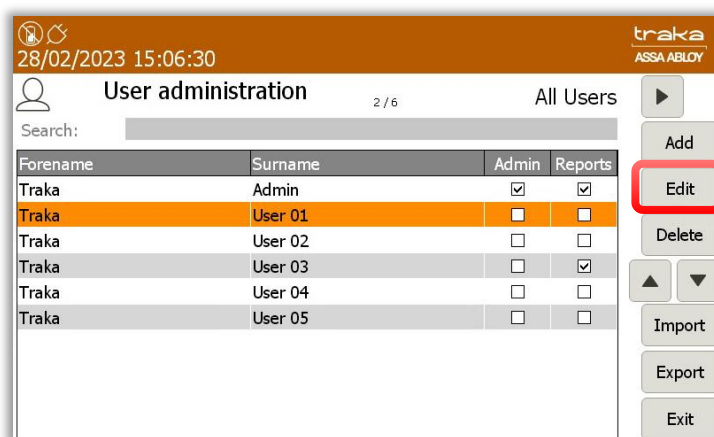
Please refer to the [Sagem MorphoSmart Reader Section](#) for details on how to enrol the user.

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

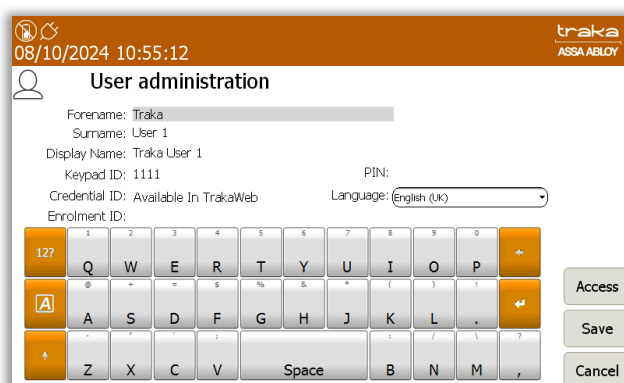
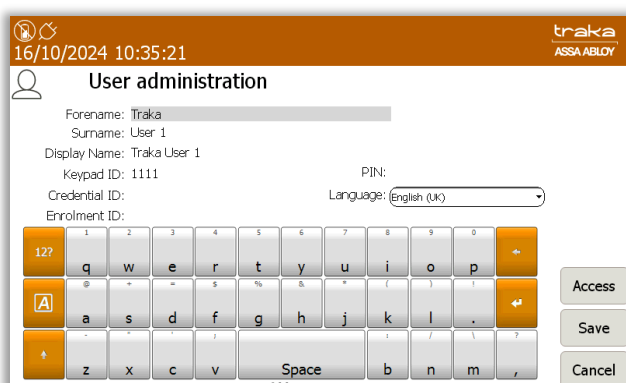
NOTE: This action can only be performed by an Admin user.

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.

4. Simply scroll through the user details and change the desired settings.



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. 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:

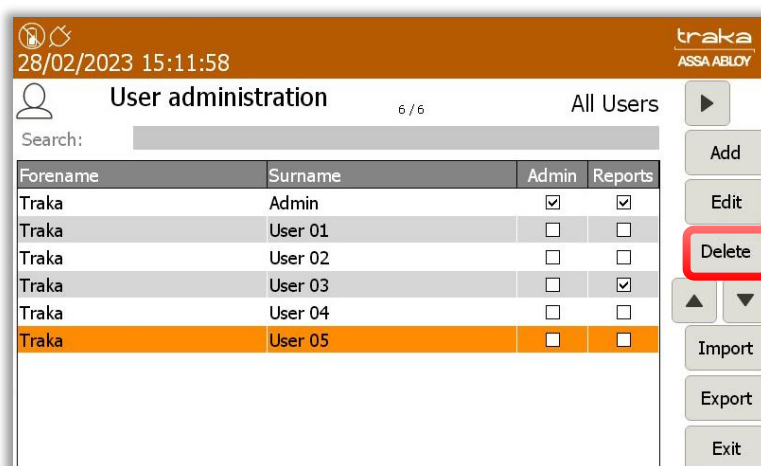
- Define the user as inactive so that the user cannot use the Traka system(s) any more
- Replace the User 'Forename' & 'Surname' with non-specific details such as 'Former employee#1'

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).

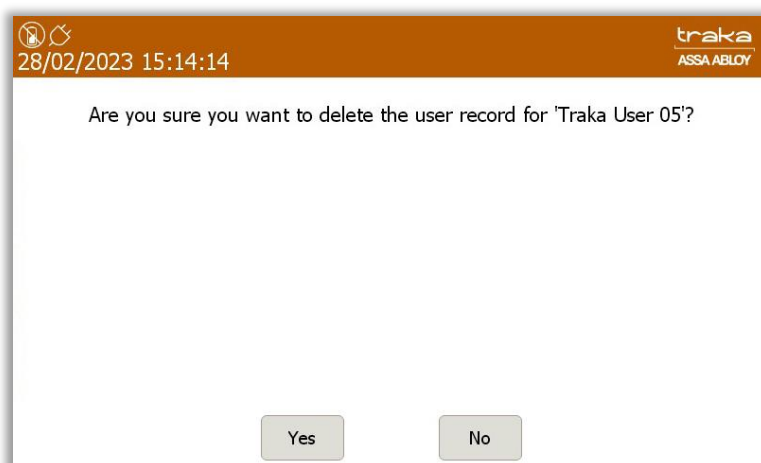
NOTE: This action can only be performed by an Admin user.

1. Access the system and click **Admin, Users**, then highlight the desired user and select **Delete**.



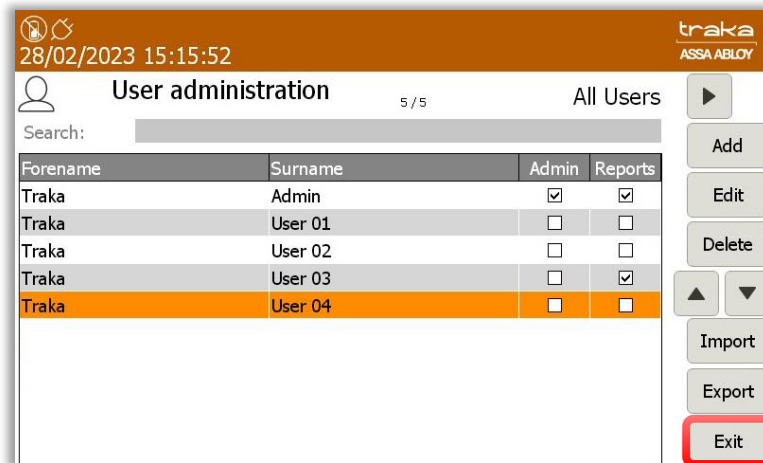
NOTE: If Multiple Credentials has been enabled, the Import and Export buttons will not be listed. For further information, please refer to UD0260 – TrakaWEB Version 4 User Guide.

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.

- You will then notice the user has been removed from the user list.

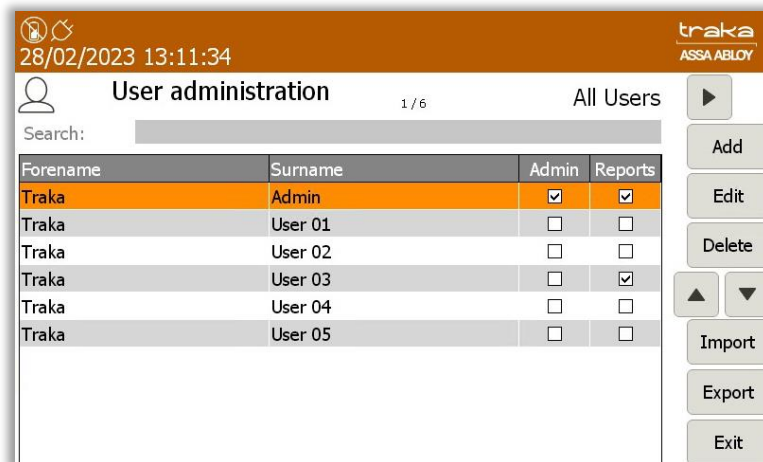


- Click **Exit** to be taken back to the administration menu. From there, click **Exit** again to return to the login screen.

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.

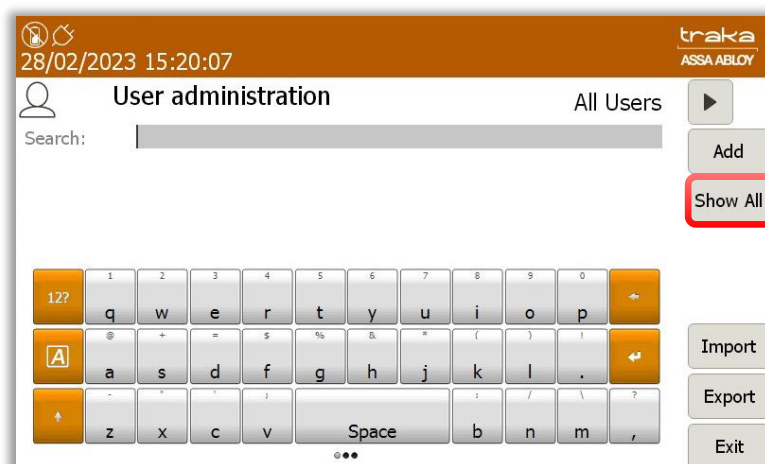
- Click on the search bar.



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.

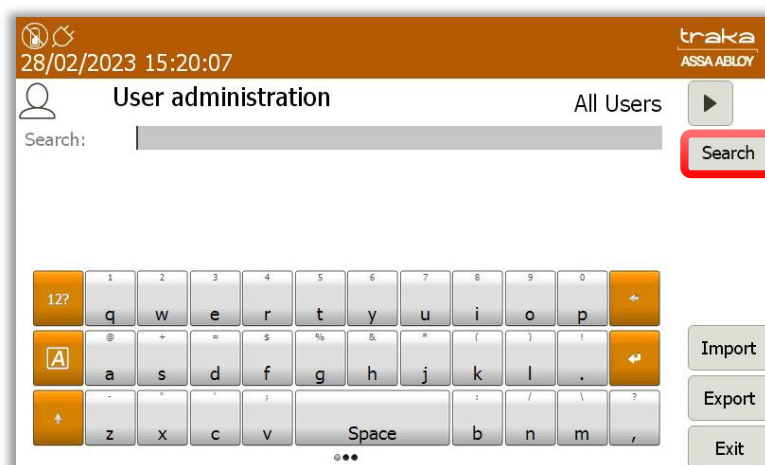


Selecting **Show All** will display all the users within the grid.

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.



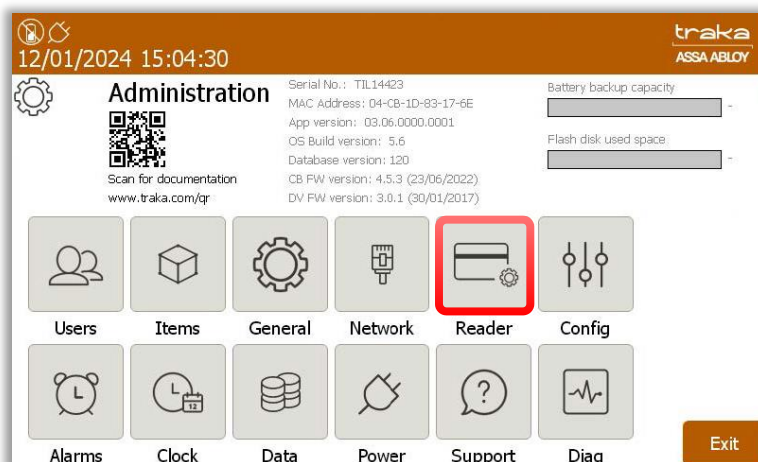
A username can be entered in the search bar. However, a minimum of 2 characters may be entered. Clicking on **Search** will display all matching results.

8.6 USER ENROLMENT ID

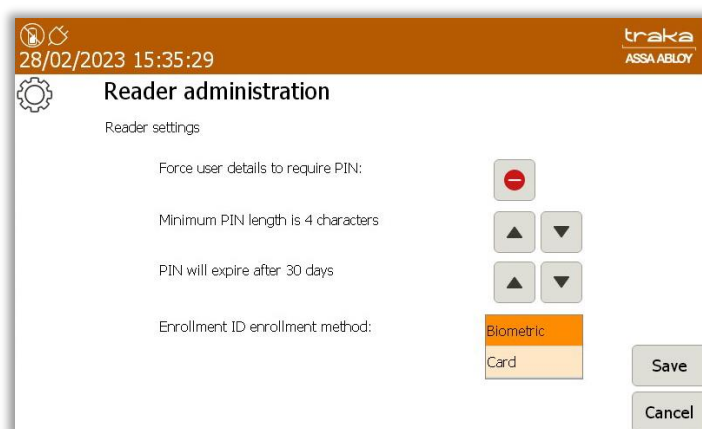
An Enrolment ID is a number assigned to a user to enable them to enrol directly at the Traka system without the need for an admin user to be present. This feature can be used only with Card or Biometric readers.

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**.

28/02/2023 15:39:00

traka
ASSA ABLOY

User administration

Forename: Traka
Surname: Admin
Display Name: Traka Admin
Keypad ID: 1234
Card ID:
PIN:
Language: English (UK)

Enrolment ID:

12? 1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

@ + = % & * () _ !

a s d f g h j k l .

~ " ' , ; ' / \ ?

z x c v Space b n m ,

Access
Save
Cancel

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

28/02/2023 15:42:24

traka
ASSA ABLOY

To access the system, enter your ID
or press Search to find an item

Search Help New PIN Enrol

1 2 3
4 5 6
7 8 9
X 0 ✓

- The user will be prompted to enter their Enrolment ID. Enter the ID and click  (enter).

28/02/2023 15:51:36

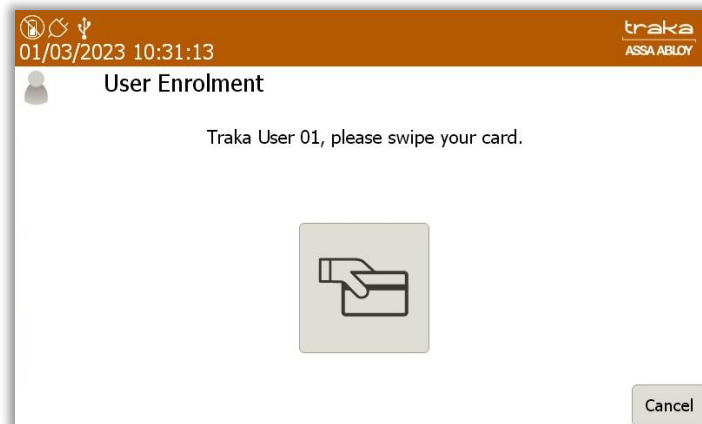
traka
ASSA ABLOY

Please enter your Enrolment ID using the Keypad

Back

1 2 3
4 5 6
7 8 9
X 0 ✓

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 section 'Sagem MorphoSmart Reader'. If you are using a card reader, you will be prompted to swipe your card.



6. Swipe your card to complete the enrolment.



9. ITEM ADMINISTRATION

9.1 INITIAL SETUP

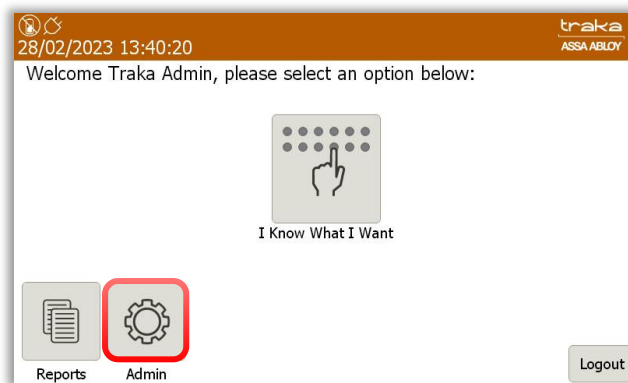
NOTE: If your Traka Touch has RRMS enabled, you will not be able to configure iFobs.

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.

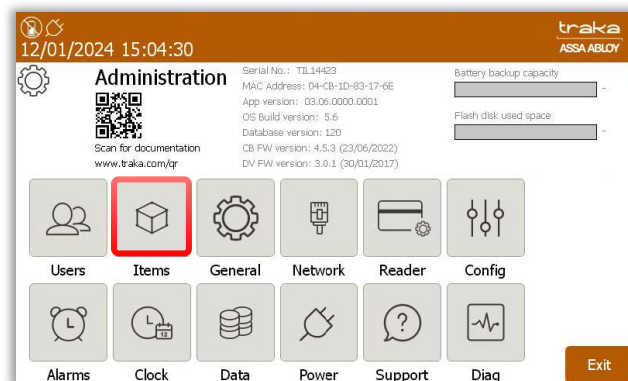
NOTE: This procedure must be carried out by an Admin user.

During the initial iFob setup, the Traka Touch system will scan for all the existing iFobs in the system and assign them to a detail field in the Item record.

1. As an Admin user, log in to the Traka Touch system and select the **Admin** button.

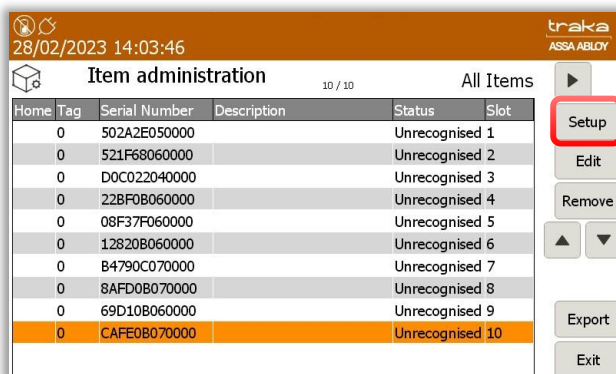


2. From the admin menu, select the **Items** button.

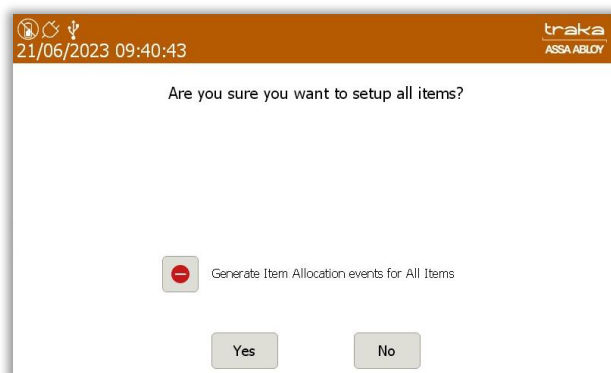


The Item administration menu will show all the available slots and items in the system. As the items are only known to be in the system, they will have no item record.

3. Select the **Setup** button.

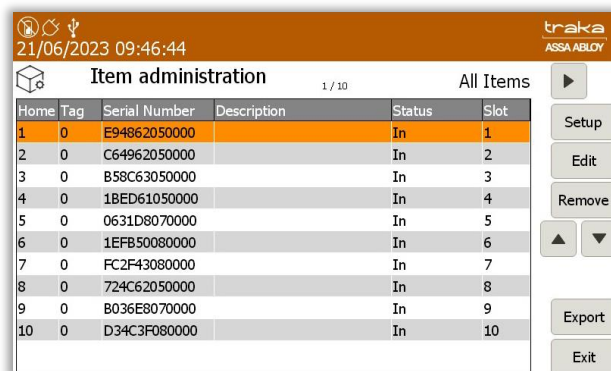


A message will appear on the screen asking if you want to setup all items. Should a situation occur where TrakaWEB does not reflect the allocation events in Traka Touch, the Generate Item Allocation Events for All Items button will enable you to force a sync to rectify the issue. By default, this is set as inactive.



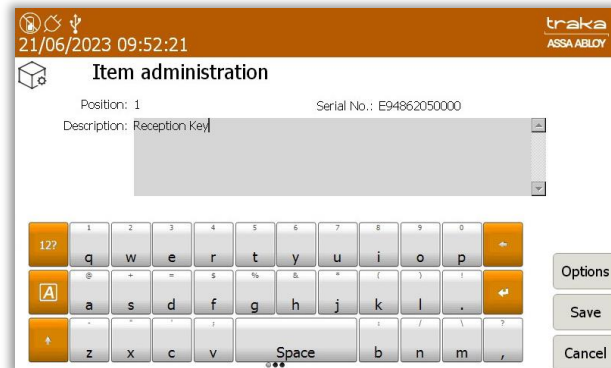
Once the process has completed, the status column will show all the items as **In**.

4. Select the **Exit** button to continue.



At this stage, new items may be created and attached to iFobs within TrakaWEB. For more information, refer to **UD0018 – TrakaWEB User Guide** or **UD0260 – TrakaWEB Version 4 User Guide**.

5. 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.
6. Enter a description into the provided field using the alphanumeric keypad.

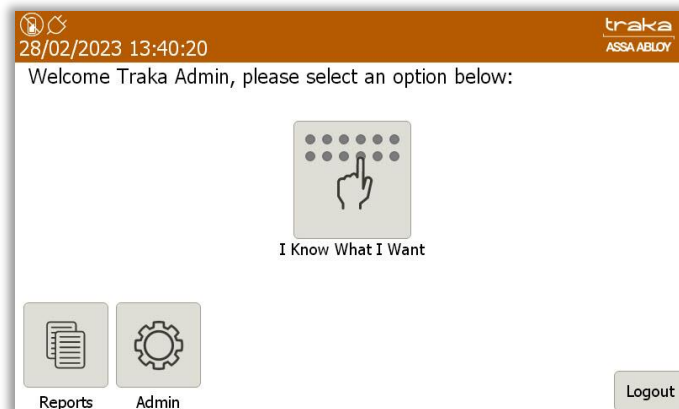


7. Click **Save** and you will be taken back to the Item Administration page. To edit more items simply highlight the item and click the **Edit** button.
8. When you have finished editing items, click **Exit** and you will be taken back to the Admin menu. You may now logout.

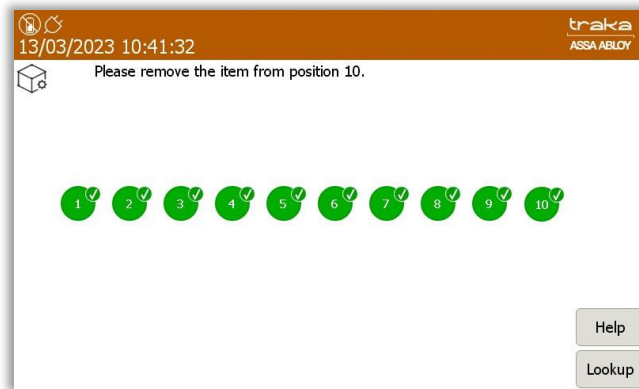
9.2 DEALLOCATING AN IFOB

Under certain conditions, you may wish to deallocate an iFob from the system. The iFob may later be reallocated if required thus maintaining a history within TrakaWEB.

1. As an Admin user, log into the Traka Touch system and select **I Know What I Want**.

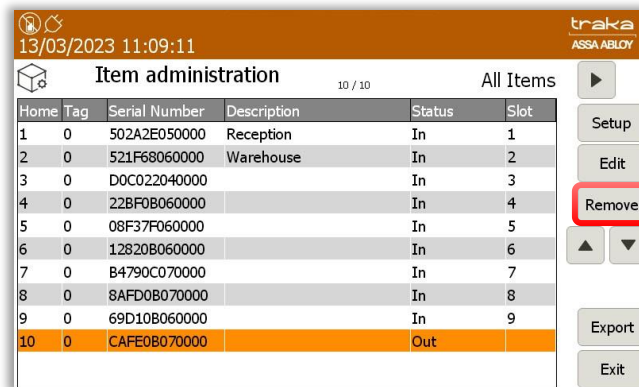


2. The door will open, and you may select and take the iFob from the system.



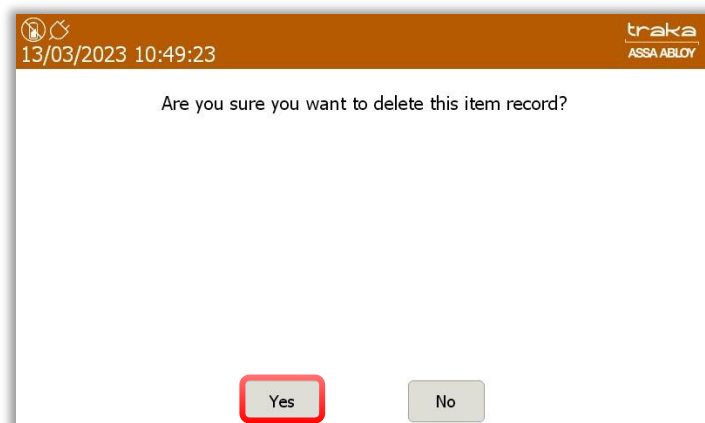
With the iFob physically taken from the system, its Item Record can now be removed from the Touch system.

3. As an Admin user, log in to the Traka Touch system and navigate to the **Item administration** screen.
4. Select the iFob you wish to remove from the system followed by selecting the **Remove** button.



You will now be asked to confirm that you wish to delete the record for the selected item.

5. Select **Yes** to continue.



The Item record will now be removed from the system.

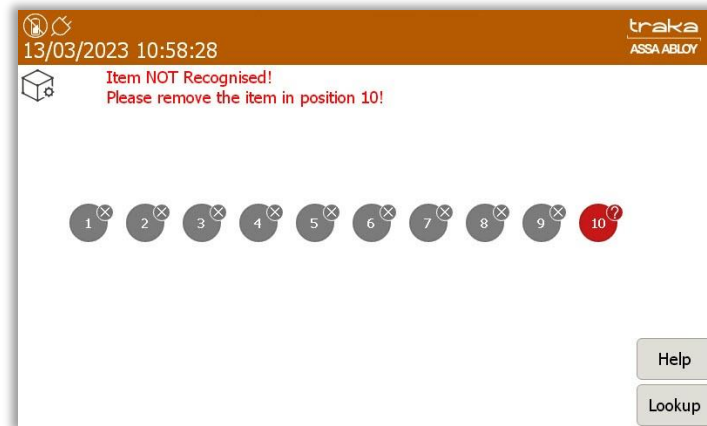
NOTE: Although the iFob and its record have been removed, its event history will be retained.

9.3 ALLOCATING AN IFOB

Other than replacing an existing iFob, this section may be also used as a guide for replacing a removed iFob as a result of being damaged, unreadable, or the iFob has been lost.

1. To allocate a new iFob, log into the system as an Admin user and select **I Know What I Want**.
2. Once the door opens, insert the new iFob into the available position.

A message will appear on the screen informing you that the iFob has not been recognised.



3. Next, close the door to exit from the screen.
4. Log into the Traka Touch system as an Admin user and navigate to the **Item Administration** screen.

From the example below, the item is in the system but not recognised.

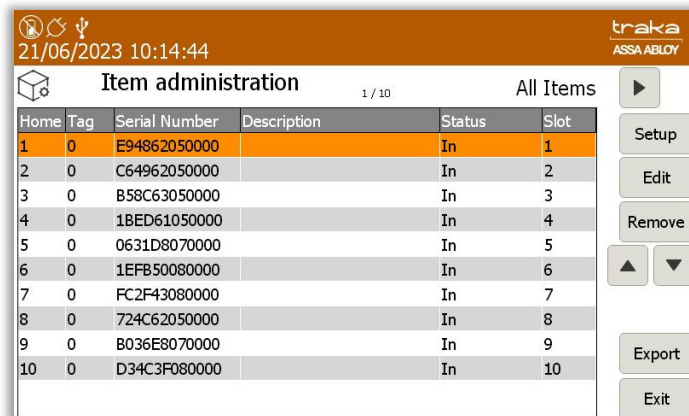
5. Complete the setup process as explained in the previous section.

The system will detect that a new Item has been added.

6. Select **Setup** to allocate the item or items.



The new item record will be added to the system.



traka
ASSA ABLOY

21/06/2023 10:14:44

Item administration 1 / 10 All Items

Home	Tag	Serial Number	Description	Status	Slot
1	0	E94862050000		In	1
2	0	C64962050000		In	2
3	0	B58C63050000		In	3
4	0	18ED61050000		In	4
5	0	0631D8070000		In	5
6	0	1EFB50080000		In	6
7	0	FC2F43080000		In	7
8	0	724C62050000		In	8
9	0	B036E8070000		In	9
10	0	D34C3F080000		In	10

Setup
Edit
Remove
Export
Exit

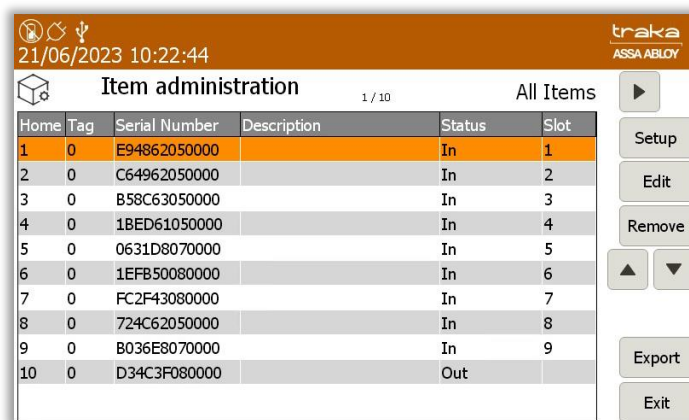
7. Once completed, select **Exit**.

To reallocate a previously removed iFob, follow the steps in the previous section to deallocate the iFob and then reallocate with the original.

9.4 REPLACING AN IFOB

A situation may arise where an iFob needs to be replaced. An example being an iFob that is damaged or lost. The event history of the iFob will be maintained after it has been deallocated.

1. Log into the system as an Admin user and navigate to the **Item Administration** screen.



traka
ASSA ABLOY

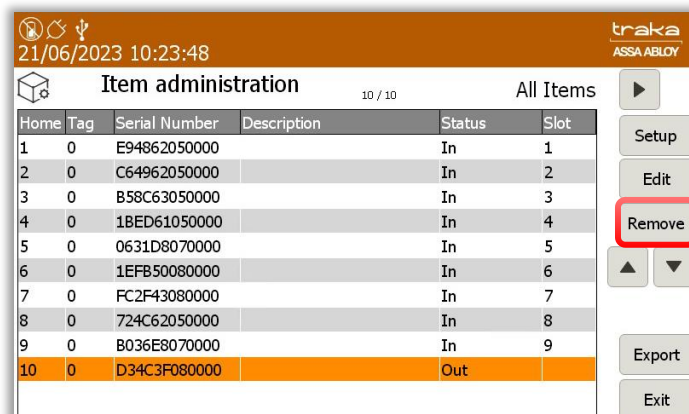
21/06/2023 10:22:44

Item administration 1 / 10 All Items

Home	Tag	Serial Number	Description	Status	Slot
1	0	E94862050000		In	1
2	0	C64962050000		In	2
3	0	B58C63050000		In	3
4	0	18ED61050000		In	4
5	0	0631D8070000		In	5
6	0	1EFB50080000		In	6
7	0	FC2F43080000		In	7
8	0	724C62050000		In	8
9	0	B036E8070000		In	9
10	0	D34C3F080000		Out	

Setup
Edit
Remove
Export
Exit

2. Select the position of the iFob that will be removed and select the **Remove** button.



traka
ASSA ABLOY

21/06/2023 10:23:48

Item administration 10 / 10 All Items

Home	Tag	Serial Number	Description	Status	Slot
1	0	E94862050000		In	1
2	0	C64962050000		In	2
3	0	B58C63050000		In	3
4	0	18ED61050000		In	4
5	0	0631D8070000		In	5
6	0	1EFB50080000		In	6
7	0	FC2F43080000		In	7
8	0	724C62050000		In	8
9	0	B036E8070000		In	9
10	0	D34C3F080000		Out	

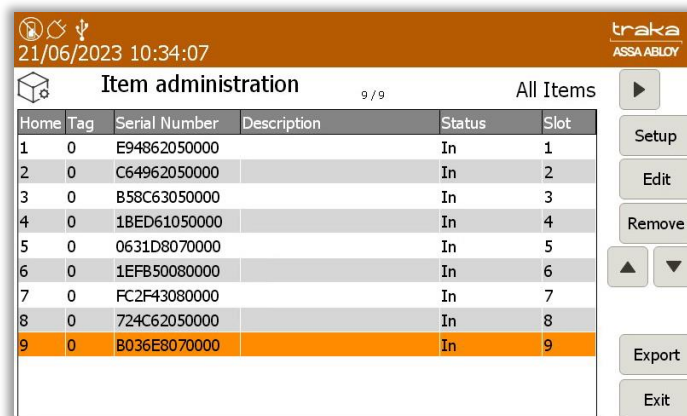
Setup
Edit
Remove
Export
Exit

You will now be asked to confirm that you wish to delete the record for the selected item.

3. Select the **Yes** button to continue.

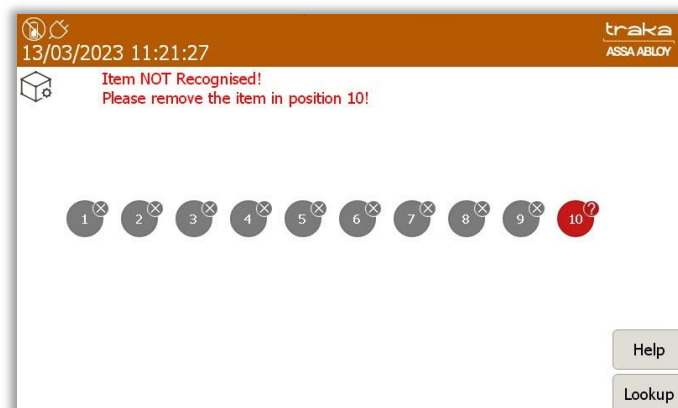


The item record will now be removed from the system.



4. Log back into the system and choose **I Know What I Want.**

You will be presented with the following screen.

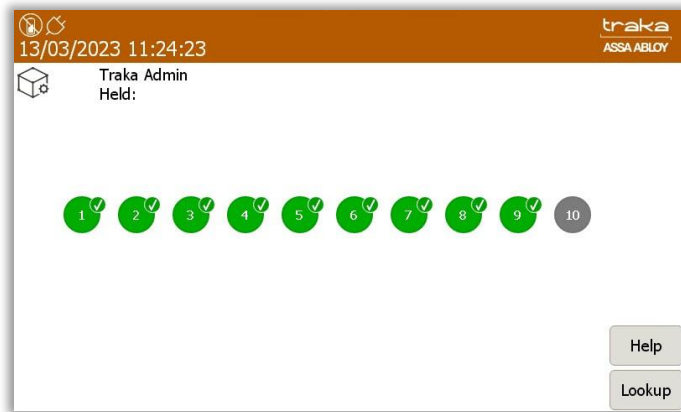


5. Remove the deallocated item from the system and close the door.

The replacement iFob is now ready to be added to the system.

6. Log into the system and select **I Know What I Want.**

The door will now open, and you will see the available slot for the new iFob.

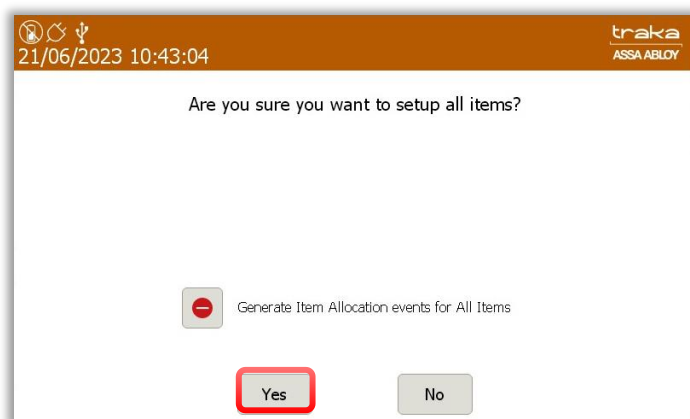


7. Insert the new iFob and then close the door.
8. Next, log back into the system and navigate to the **Item Administration** screen.

The **Item Administration** screen will show all the items currently in the system. In the example below, there is one unrecognised item in the system.

Home	Tag	Serial Number	Description	Status	Slot
	0	D34C3F080000		Unrecognised	10
1	0	E94862050000		In	1
2	0	C64962050000		In	2
3	0	B58C63050000		In	3
4	0	18ED61050000		In	4
5	0	0631D8070000		In	5
6	0	1EFB50080000		In	6
7	0	FC2F43080000		In	7
8	0	724C62050000		In	8
9	0	B036E8070000		In	9

9. Select the **Setup** button to continue allocating the new item to the system.
10. A screen will appear asking if you wish to add the iFob, select **Yes** to continue.

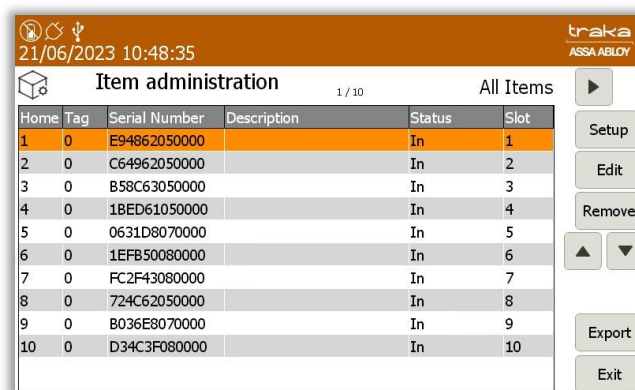


The new item will be detected by the system, select the **Setup** button to continue.



NOTE: Selecting 'Skip' will return you to the Item Administration screen.

Once the setup process has completed, the item will be shown in the list on the Item administration screen.

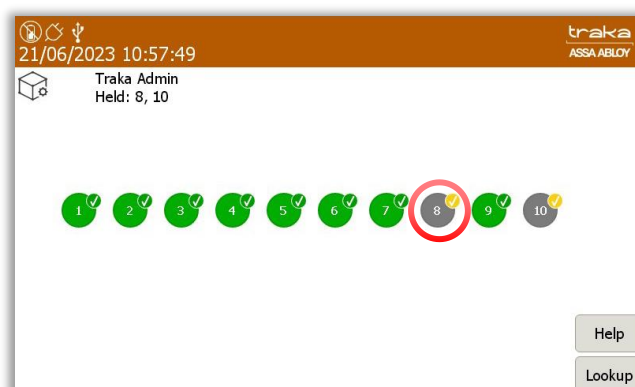


NOTE: Users of Traka integrations must refer to the appropriate integration user guides, for any further steps that may be required.

9.5 RELOCATING AN IFOB WITHIN THE SAME SYSTEM

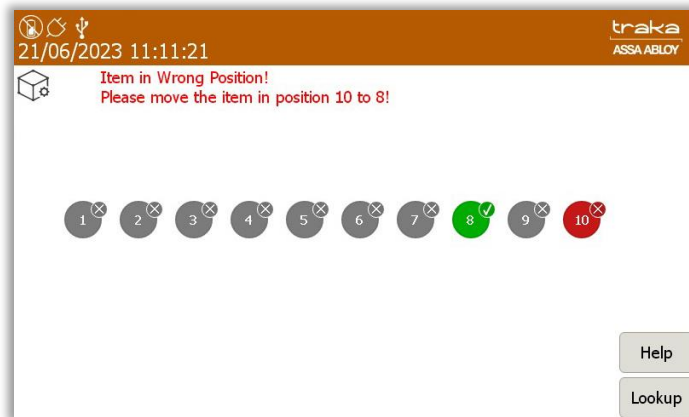
If required, it is possible to assign a new home position for an iFob within the same system even if the designated position currently has an iFob associated with it. In this example, the item from position 10 is currently out of the system and the item from position 8 will be relocated to that position.

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.

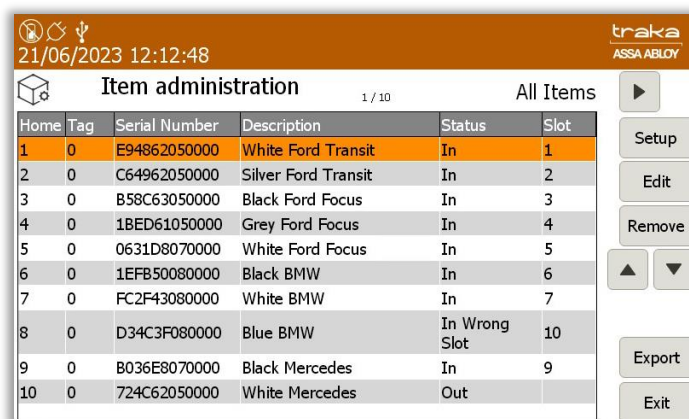


2. Log back into the system and select **I Know What I Want**. Once the door has opened, insert the iFob into a vacant position.

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



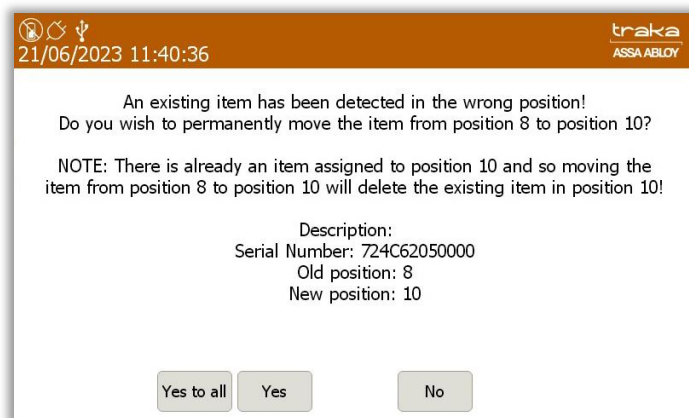
3. Now close the door.
4. Log into the system and navigate to the **Item Administration** screen. You will see that the relocated item status is shown as **In Wrong Slot**.



5. Next, run the setup process.
6. At the next screen, select **Yes** to continue.

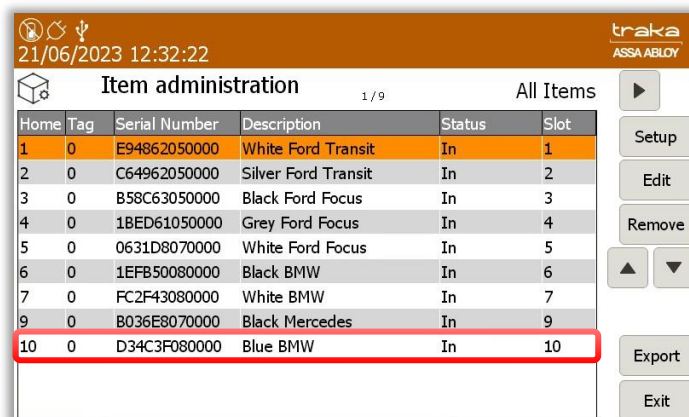


The next screen will inform you that there is already an item assigned to that position and if you choose to move another item into that position, the existing item will be deleted.

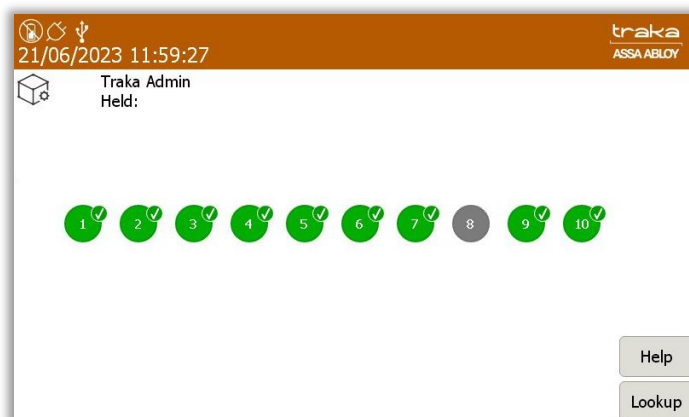


7. As it is the intention to relocate the item, select **Yes** to continue.

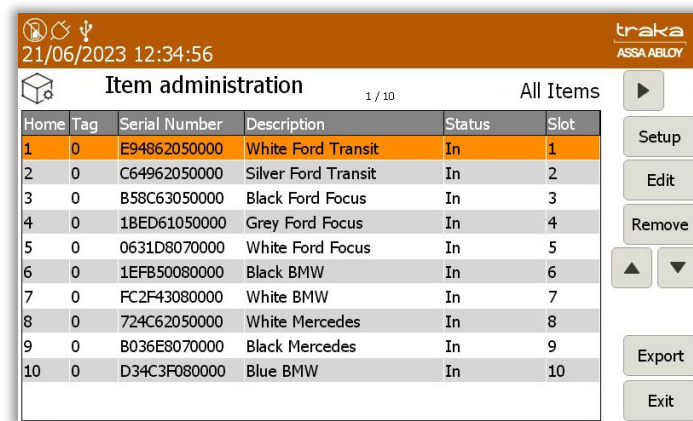
You will then be returned to the **Item Administration** screen. You will see that position 10 now holds the iFob record for the item that was previously in position 8.



The previous position 10 iFob record has now been deleted leaving position 8 deallocated.



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



21/06/2023 12:34:56 traka ASSA ABLOY

Item administration 1 / 10 All Items

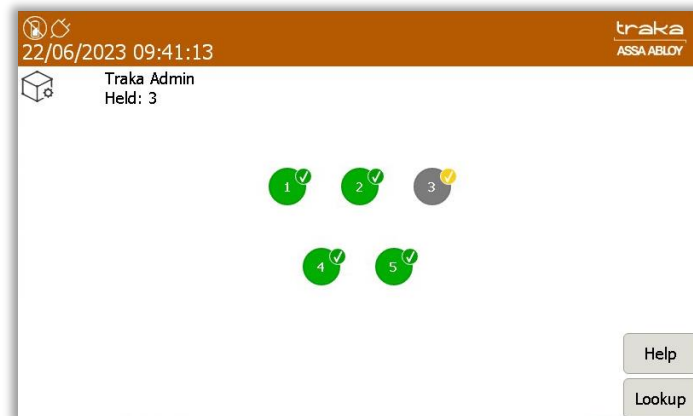
Home	Tag	Serial Number	Description	Status	Slot
1	0	E94862050000	White Ford Transit	In	1
2	0	C64962050000	Silver Ford Transit	In	2
3	0	B58C63050000	Black Ford Focus	In	3
4	0	18ED61050000	Grey Ford Focus	In	4
5	0	0631D8070000	White Ford Focus	In	5
6	0	1EFB50080000	Black BMW	In	6
7	0	FC2F43080000	White BMW	In	7
8	0	724C62050000	White Mercedes	In	8
9	0	B036E8070000	Black Mercedes	In	9
10	0	D34C3F080000	Blue BMW	In	10

Buttons: Setup, Edit, Remove, Export, Exit

9.6 RELOCATING AN IFOB FROM ONE SYSTEM TO ANOTHER

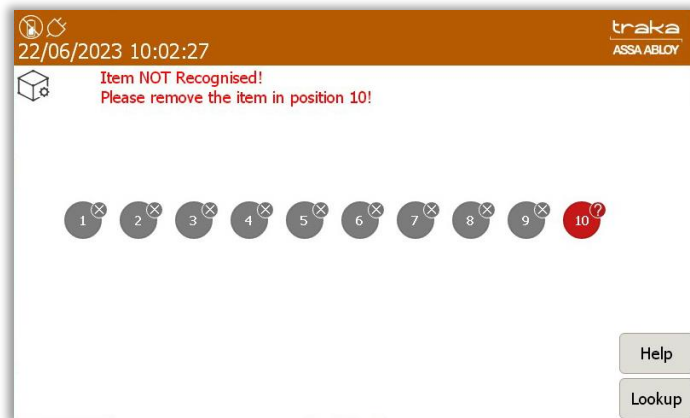
If required, it is possible to assign a new home position for an iFob from a different system even if the designated position currently has an iFob associated with it. In this example, the item from position 10 of the designated system is currently out of the system and an iFob in position 3 from another 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.

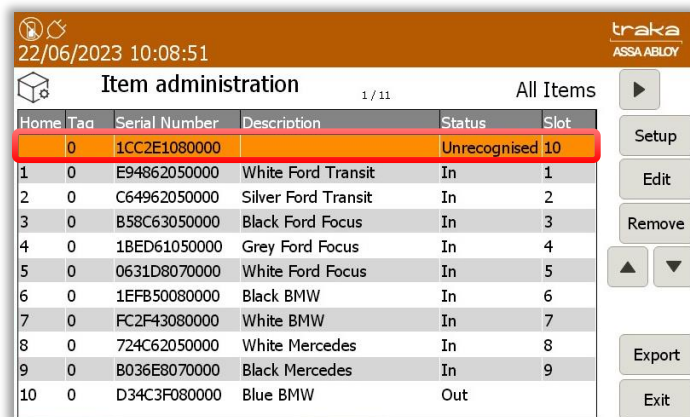


2. Log into the system that you wish to relocate the iFob and select **I Know What I Want**. Once the door has opened insert the iFob into the vacant position.

You will be presented with a message indicating that the item is not recognised.



- Now close the door.
- Log into the system and navigate to the **Item Administration** screen. You will see that the relocated item status for position 10 is shown as **Unrecognised**.



- Next, run the setup process.
- 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.

22/06/2023 10:33:40 traka ASSA ABLOY

A new item has been detected in position 10
however position 10 already has an item assigned to it.
Do you wish to setup a new item or replace the current item?

Description: Blue BMW
New Serial Number: 1CC2E1080000
Old Serial Number: D34C3F080000

Setup: A completely new item to be setup.
Replace: New serial number(tag) for existing item.

Setup Replace Skip Cancel

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.

22/06/2023 10:38:15 traka ASSA ABLOY

Item administration 1 / 10 All Items

Home	Tag	Serial Number	Description	Status	Slot
1	0	E94862050000	White Ford Transit	In	1
2	0	C64962050000	Silver Ford Transit	In	2
3	0	B58C63050000	Black Ford Focus	In	3
4	0	18ED61050000	Grey Ford Focus	In	4
5	0	0631D8070000	White Ford Focus	In	5
6	0	1EFB50080000	Black BMW	In	6
7	0	FC2F43080000	White BMW	In	7
8	0	724C62050000	White Mercedes	In	8
9	0	B036E8070000	Black Mercedes	In	9
10	0	35AB61050000		In	10

Setup Edit Remove Export Exit

If you choose the **Replace** option. The iFob will replace the existing iFob but use the existing iFob record.

22/06/2023 10:51:23 traka ASSA ABLOY

Item administration 10 / 10 All Items

Home	Tag	Serial Number	Description	Status	Slot
1	0	E94862050000	White Ford Transit	In	1
2	0	C64962050000	Silver Ford Transit	In	2
3	0	B58C63050000	Black Ford Focus	In	3
4	0	18ED61050000	Grey Ford Focus	In	4
5	0	0631D8070000	White Ford Focus	In	5
6	0	1EFB50080000	Black BMW	In	6
7	0	FC2F43080000	White BMW	In	7
8	0	724C62050000	White Mercedes	In	8
9	0	B036E8070000	Black Mercedes	In	9
10	0	D34C3F080000	Blue BMW	In	10

Setup Edit Remove Export Exit

9.6.1 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 iFob in an Advanced First in/First Out group is relocated, the item will be deallocated and removed from the group. For an iFob 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 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**.

9.6.2 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 iFob 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 iFob 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**.

9.6.3 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**.

9.6.4 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**.

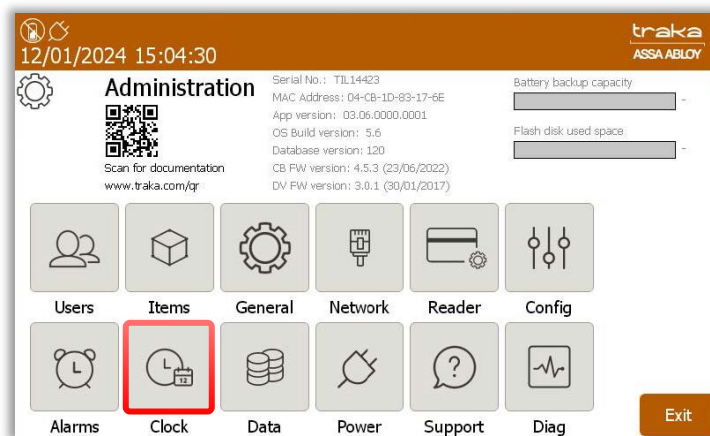
9.6.5 RELOCATING ITEMS WITH AN ASSOCIATED ACCESS SCHEDULE

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**.

10. CHANGING THE CLOCK SETTINGS

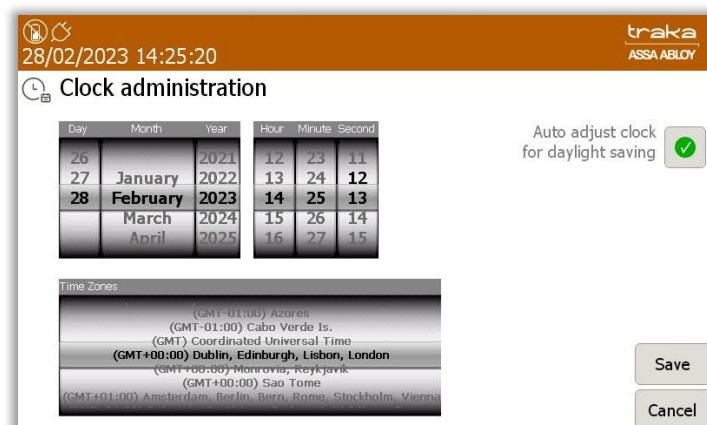
If necessary, the system clock setting maybe changed from within the Administration menu.

1. From the Administration Menu, select the **Clock** icon.



At the next screen, you will be able to edit the Day, Month, Year, Hour, Minutes, Seconds, and the Time Zone.

2. By tapping above or below the current settings you can scroll up or down as required to change the clock settings as shown in this example:



3. Once you have completed making your changes, click on **Save** to be taken back to the Administration Menu.

11. SYSTEM OPERATION

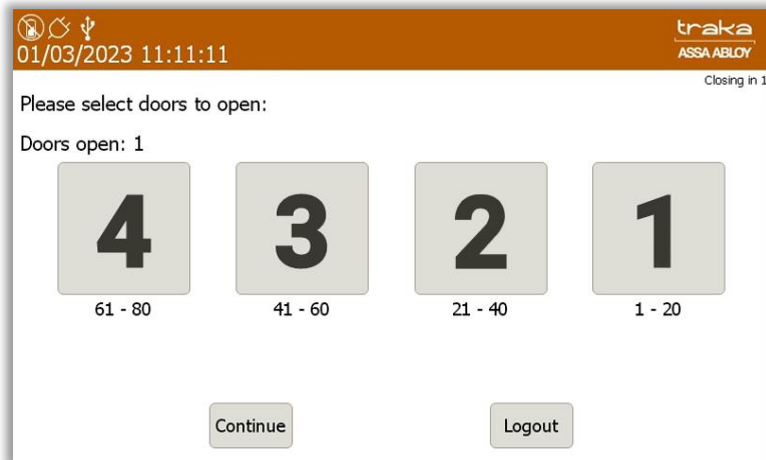
11.1 REMOVING AN ITEM

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 the item to be released from the system in one of two methods, **I Need To Search** or **I Know What I Want**.

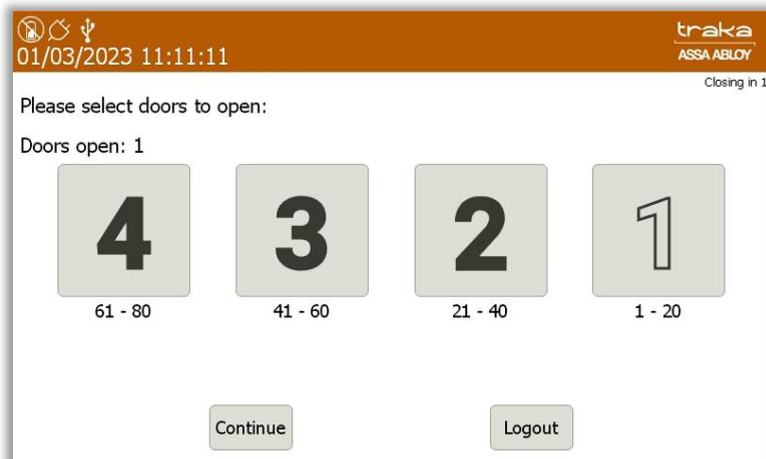
By default, each Traka Touch system is configured with the **I Know What I Want** mode. For more information on the item release screen, please review the [Item Release Screen](#) section. To change the item release preferences, please refer to the [General Options](#) section.

NOTE: This method of release does not apply if you have RRMS enabled

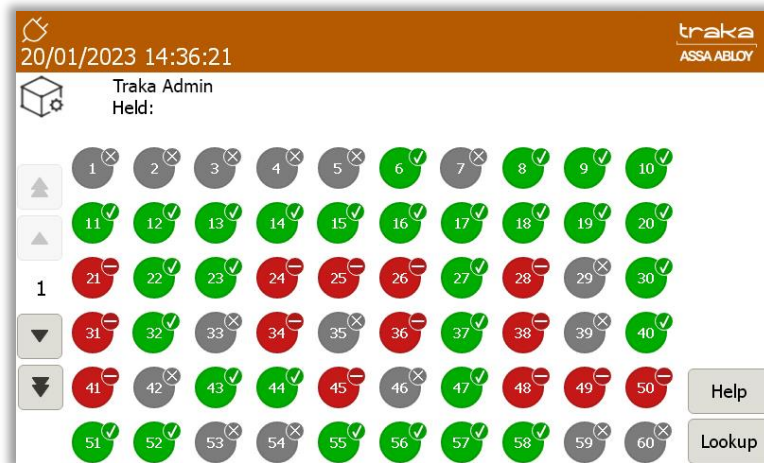
1. Access the system and select **I Know What I Want** (if applicable). If your system has extension-cabinets, you will be prompted to select which door(s) you want to open. If your system does not have extension-cabinets, proceed to step 3.



2. You can select any number of doors to open providing you have access to 1 or more items within that cabinet. Each door you select will open automatically. Once you have selected the door(s) you wish to open, click **Continue**.



3. The system door will open, and you will be presented with a screen similar to the following:



- 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.



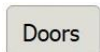
- Grey symbols mean no item is assigned to the slot.



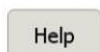
- Single arrow – scroll through pages of position numbers using this button. The display will show a maximum of 60 positions on each page.



- 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.

4. **Press** the  button on the touch screen of the item you wish to remove.
5. You will hear a beep.
6. **Wait** for the “click” (unlocking item).
7. **Remove** the iFob.

11.2 OVERRIDE OF AN EMPTY SLOT

Should an iFob develop a fault and become unrecognisable by the system, the slot will be shown as empty on the Touch screen. A standard user will be unable to remove any iFobs in this situation. An admin user will be able to release any faulty iFobs by selecting them from the Touch screen by selecting the empty slot. An event will be recorded which can be viewed in Reports. It will be shown as 'Admin Override of Empty Slot'.

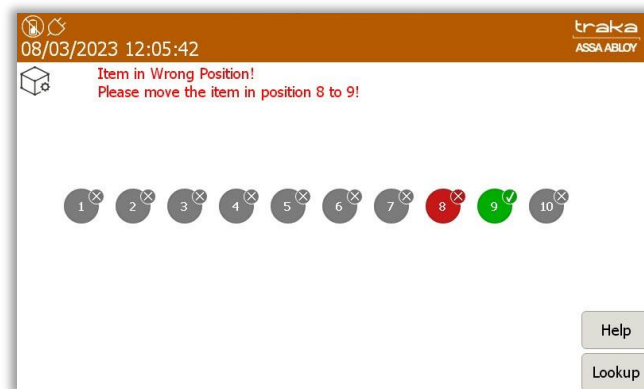
11.3 RETURNING AN ITEM

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

1. **Access** the system.
2. **Check** the Tag number on the key bunch.
3. **Insert** the iFob into the matching position number.

11.4 ITEM IN WRONG SLOT

When an item is returned to the incorrect position, the system will prompt you to remove the item 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.

11.5 NO DOOR SYSTEMS

If your system is a no door system, the method for removing iFobs is the same as the method used for a system with a door. However, by default once an iFob has been removed, the user will automatically be logged out of the system.

NOTE: An option is available to override this, which will leave the user logged in until they press the logout button or their session times out. This option must be enabled in the configuration file.

When returning iFobs, the user can either log into the system first, or simply place the iFob back into its position without logging in. If the user returns the iFob without logging in, then any features such as Reason Logging or Notes Logging etc. (used in conjunction with TrakaWEB) will not be requested. If the user does log into the system to return an iFob, then any Reason Logging or Notes Logging etc. will be requested.

NOTE: If the user returns an iFob without logging in it is not possible for the system to know who returned the iFob. Therefore, no username will be logged against the iFob returned event.

On a system with a door, once the door is closed the user is automatically logged out. On a no-door system, there is a logout button available for the user to logout at any time.

11.6 NON-LOCKING RECEPTOR STRIPS

Non-Locking Receptor Strips are not fitted with solenoids to lock the iFobs in their positions. Therefore, the iFobs can physically be removed without the need to be electronically released. They can also be used alongside locking strips in the same system.

The process used for removing and returning iFobs for a locking strip can also be used for a non-locking strip. Once an iFob has been selected for removal, the LED of that position will flash. However, there will be no 'click' from the release of the solenoid. Alternatively, iFobs can simply be removed once the door has opened without being selected on the item selection screen, and the system will recognise which iFobs have been taken.

If non-locking strips are used in conjunction with TrakaWEB and features such as Reason Logging or Notes Logging, the feature will be requested once the iFob has been removed or returned.

11.7 AUTO OPEN ALL DOORS ON LOGIN

The Auto Open All Doors on Login functionality requires a configuration setup for it to be enabled on the Traka Touch System. The option only applies to multi-door key cabinet systems. Once enabled, the behaviour of the **I Know What I want** screen will be altered so that all the doors to cabinets corresponding to a users' item access or items that the user is holding will open. This option will not function if a user logs in using **I Need To Search**. The option to select **Doors** will be made available in the event of a door being closed in error.

11.8 ATTACHING KEYS TO IFOBS

Traka can provide you with standard key rings to allow you to attach your keys to your iFobs. Alternatively, Traka can also provide security seals to securely lock the keys and iFobs together.

11.8.1 KEYRINGS

1. Carefully pry the key ring open
2. Slot your key(s) onto the key ring
3. Slot your iFob on the key ring



11.8.2 SECURITY SEALS

1. Cut the provided nylon tube to a length of **90mm** (3 ⁹/₁₆ inch) and thread over the cable. This is important to ensure a long life from the cable seal and to prevent a long free end of cable showing.
2. Insert the cable through the Traka iFob and your key(s).
3. If you have Traka ID tags, add one of these as well.
4. Once assembled, push the free end of the cable into the hole in the locking body and ensure it is securely fixed. After inserting as far as possible, pull on the cable to ensure that it is permanently secured inside the locking body.



12. REPORTS

To view Reports, a user with report access must log into the system.

12.1 GENERATING AND EXPORTING REPORTS

NOTE: Reports are not available when using RRMS

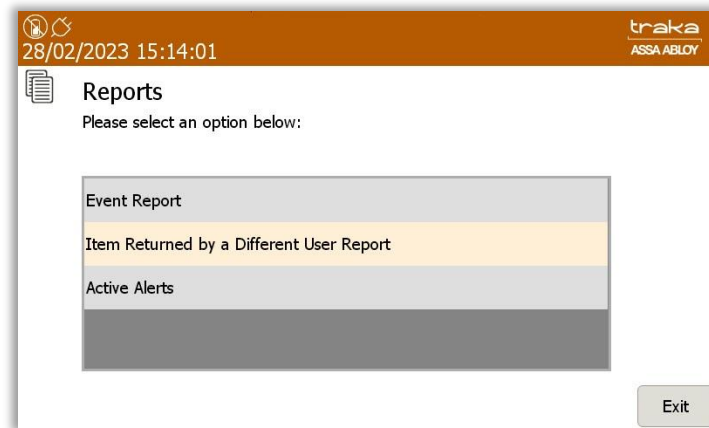
Reports allow you to view all the transactions and events that have occurred in a user definable period of time.

NOTE: This action can only be performed by a user with Reports permissions and must log into the system.

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

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.

2. Select the desired report.

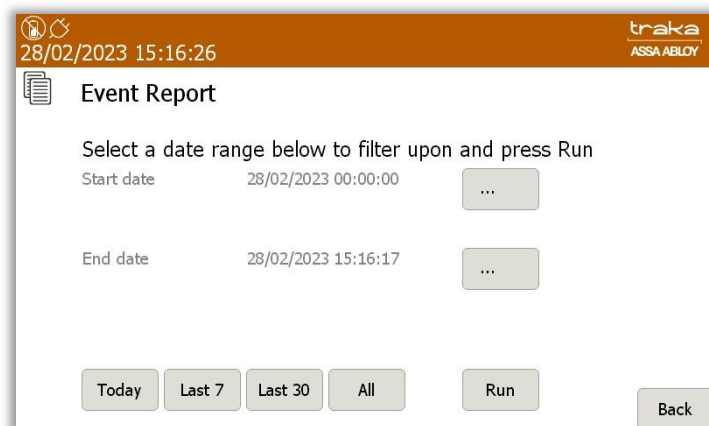


The Reports options will provide you with a number of set ways to filter the report as required. Alternatively, you can choose to set more specific dates.

Event Report

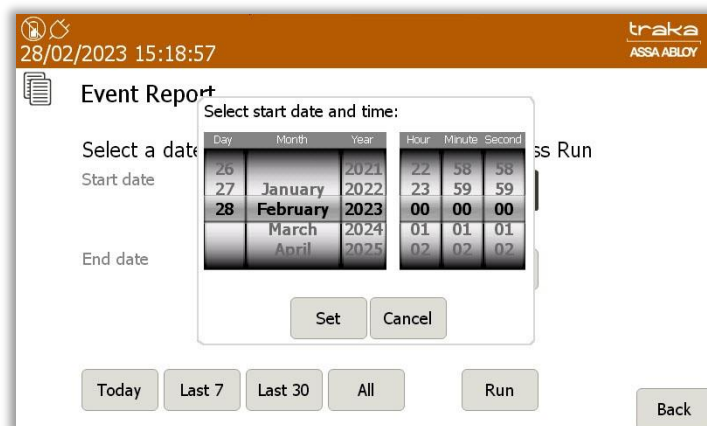
This report shows you all types of event activity.

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



- The  button will provide all the reports for today.
- The  button will provide the events from the last seven days.
- The  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.



Event Report

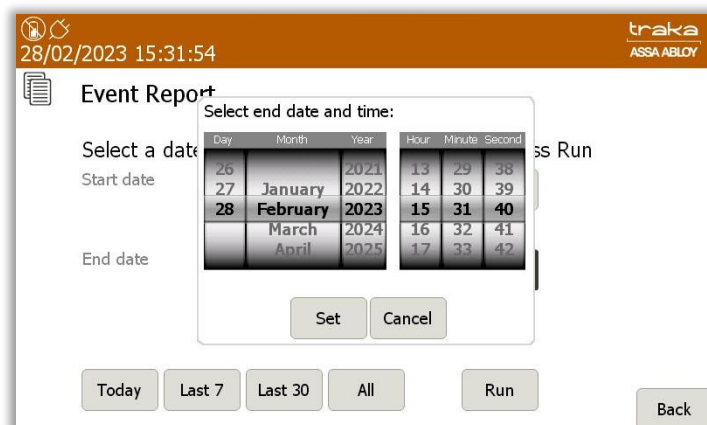
Select start date and time:

Day	Month	Year	Hour	Minute	Second
26	January	2021	22	58	58
27	January	2022	23	59	59
28	February	2023	00	00	00
	March	2024	01	01	01
	April	2025	02	02	02

Set Cancel

Today Last 7 Last 30 All Run Back

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.



Event Report

Select end date and time:

Day	Month	Year	Hour	Minute	Second
26	January	2021	13	29	38
27	January	2022	14	30	39
28	February	2023	15	31	40
	March	2024	16	32	41
	April	2025	17	33	42

Set Cancel

Today Last 7 Last 30 All Run Back

1. Select one of the filtering options above and click the  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:

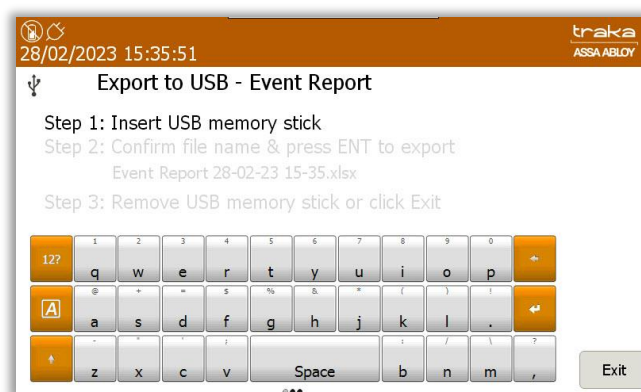
- Item in but not on charge
- Item in with charge fault
- Unidentified item on charge
- Unidentified item charged
- Unidentified charged fault
- USB charger undetectable
- Door left open

12.2 EXPORTING REPORTS

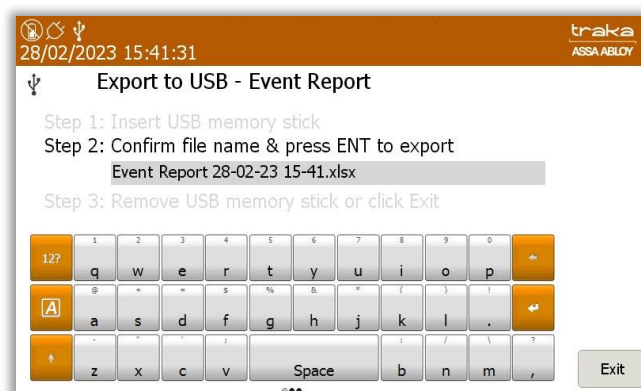
It is possible to export Event Reports and Illegal Handover Reports to a USB Memory Stick.

NOTE: For further information on USB memory stick specification, refer to section [6.2](#).

1. To export the reports to a USB memory stick, click the  button.
2. The door will open (if applicable) and ask that you insert a USB memory stick.



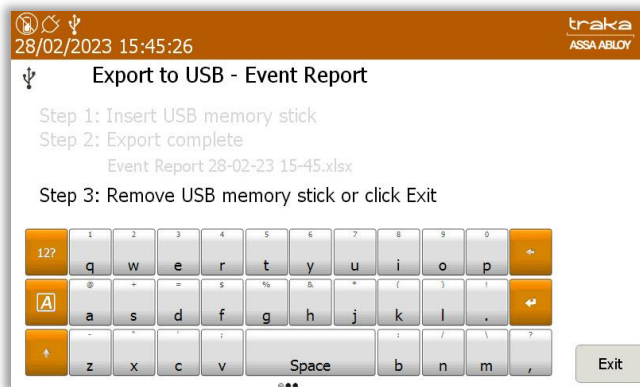
3. Enter the desired file name for the report and press  (enter).



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  button to be taken back to the login screen.

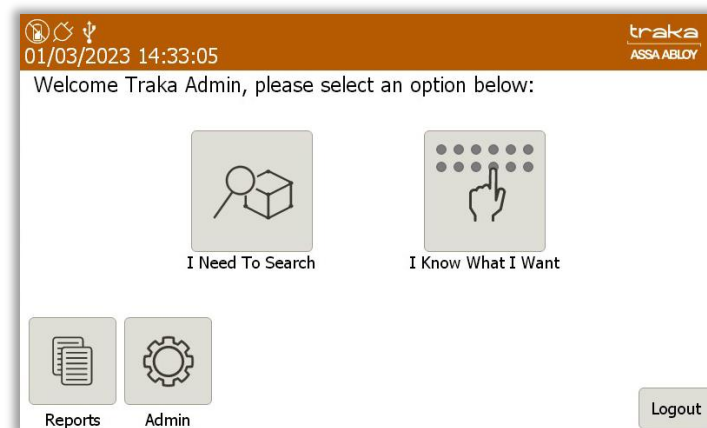
13. ADVANCED USER GUIDE

13.1 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](#).

Depending on which option is selected, when a user identifies themselves to the system, they will be presented with a screen similar to the following...

NOTE: If a user has admin or report permissions, both of these buttons will also appear on the selection screen.



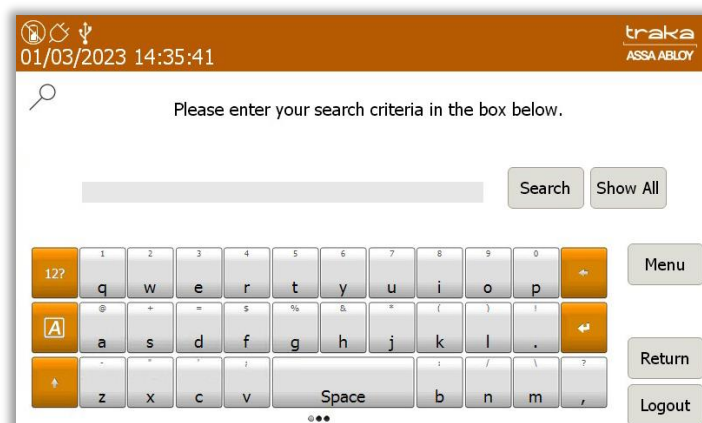
There are two options that allow the user to remove items from the system in different ways...

- **'I Need to Search'** – 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'** – Will allow you to select which items you wish to remove via the on-screen display showing all the items currently in the system.

NOTE: 'I Know What I Want' is the standard release method for Traka Touch systems. To make changes to this please review the [General Options](#) section.

13.1.1 SEARCHING FOR ITEMS

Selecting the 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. Leaving the field blank and clicking the 'Show All' button will list all of the items currently in the system.

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

Re

Search

Show All

E.g., Typing 'Re' into the search field will retrieve any item description with 're' in the title. As shown below...

- Reception Door
- Warehouse Key
- Store Room

01/03/2023 14:42:20

traka
ASSA ABLOY

Please touch search results to select them. Touch selected items to deselect them.

Search Results For: RE

Selected Items

Pos	Tag	Description	Pos	Tag	Description
1	0	Warehouse Key			
2	0	Reception Door			
3	0	Store Room			

Search

Logout

Return

Selecting an item from the left-hand column (results) will automatically move it into the right-hand column (selected items).

01/03/2023 14:44:19

traka
ASSA ABLOY

Please touch search results to select them. Touch selected items to deselect them.

Search Results For: RE

Selected Items

Pos	Tag	Description	Pos	Tag	Description
1	0	Warehouse Key	2	0	Reception Door
3	0	Store Room			

Search

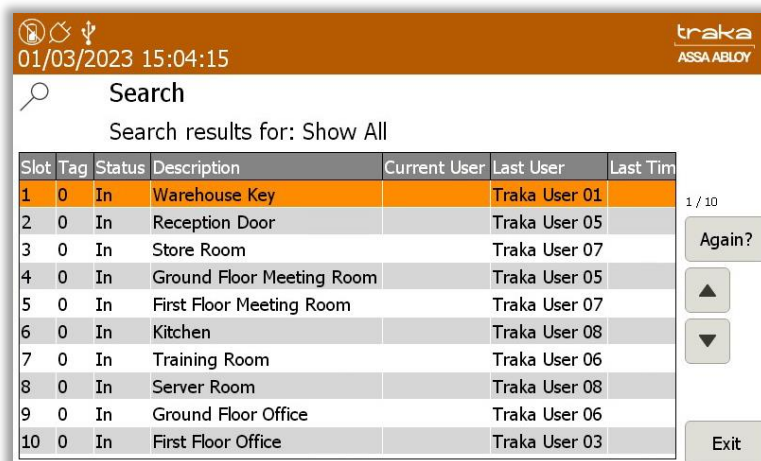
Logout

Return

Release

Once you have selected all the items you wish to remove, click the **Release** button. The system door will then open and begin to release the selected items to you.

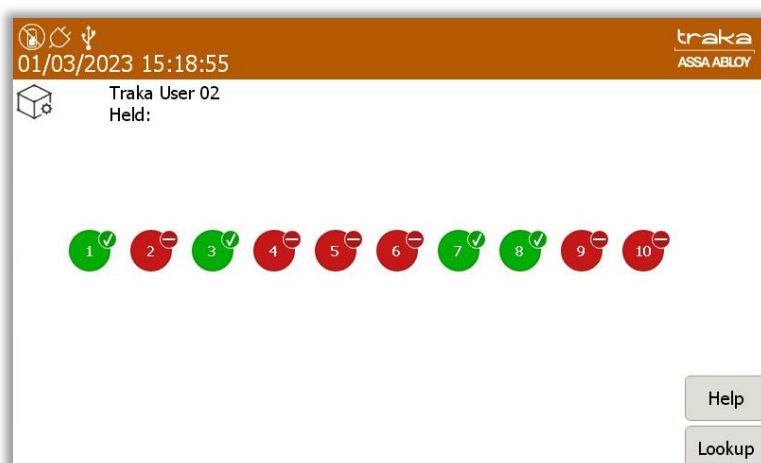
NOTE: With RRMS enabled, the search results will be displayed differently as shown in the example below:



Slot	Tag	Status	Description	Current User	Last User	Last Time
1	0	In	Warehouse Key		Traka User 01	
2	0	In	Reception Door		Traka User 05	
3	0	In	Store Room		Traka User 07	
4	0	In	Ground Floor Meeting Room		Traka User 05	
5	0	In	First Floor Meeting Room		Traka User 07	
6	0	In	Kitchen		Traka User 08	
7	0	In	Training Room		Traka User 06	
8	0	In	Server Room		Traka User 08	
9	0	In	Ground Floor Office		Traka User 06	
10	0	In	First Floor Office		Traka User 03	

13.1.2 I KNOW WHAT I WANT

Selecting 'I Know What I Want' will take you to the following 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 release them to you, providing you have the correct permissions.

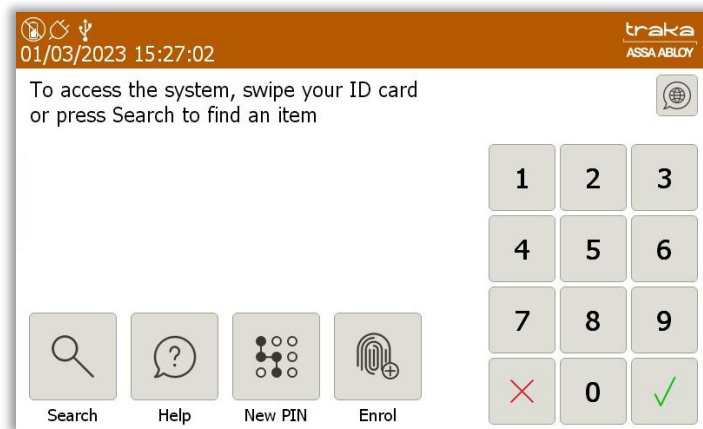
NOTE: This is the standard release method for Traka Touch systems. To make changes to this please review the [General Options](#) section.

13.2 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 does not have a PIN, then this will be enforced 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 entered 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 verification.

NOTE: There is a minimum number of digits the PIN needs to be set at. 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

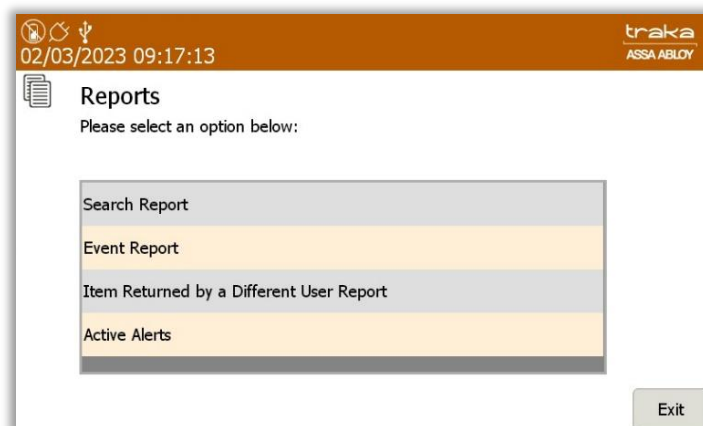
1. From the main login screen select **New PIN**.
2. You will then be asked to identify yourself at the cabinet via Keypad ID, ID card or fingerprint.
3. Once you have identified yourself at the system you will be asked to enter your current PIN.
4. You will then be prompted to enter your new PIN.
5.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

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.

13.3 SEARCH REPORT

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

By default, the **Search Report** option resides in the Reports section.

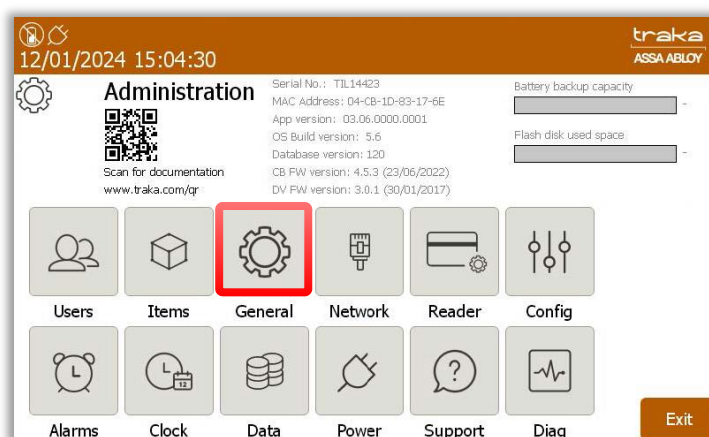


It can however be relocated by a user with Admin access to the Login screen. This section will explain how to accomplish this.

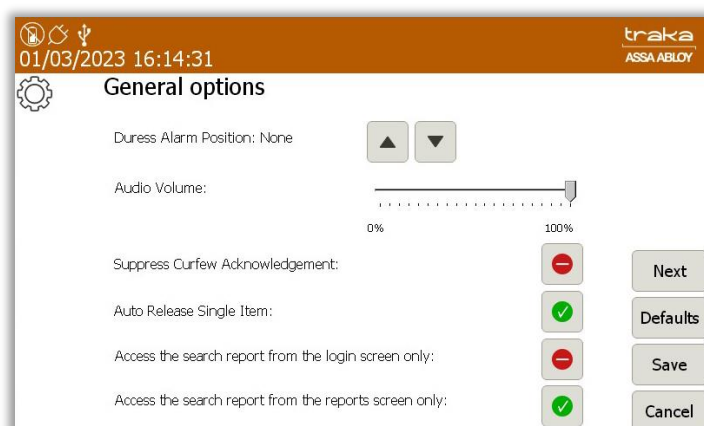
1. Access the system with a User ID, Credential, or fingerprint.



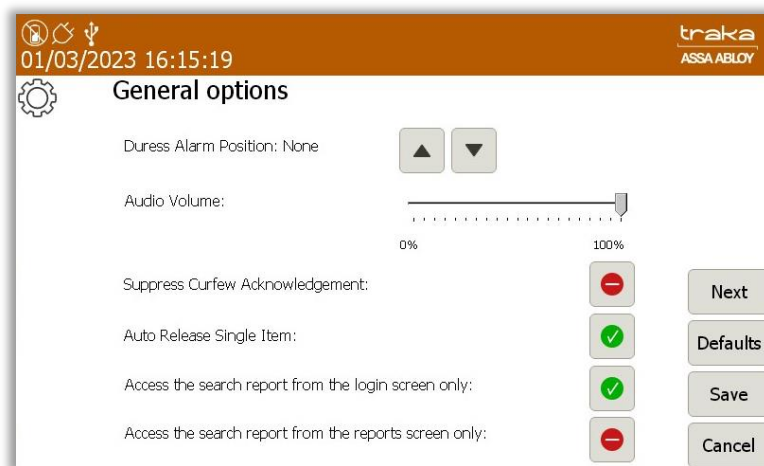
2. Click on **Admin** and then from the Administration screen, click on **General**.



The General Options screen will display the current settings for the **Search Report**. The image below shows the default settings.

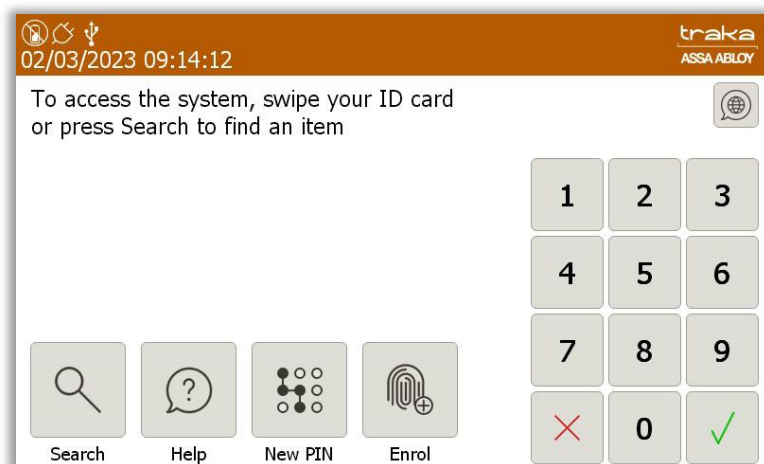


3. Click on the  symbol. It will change to a  symbol as shown below.



4. Click **Save** and then exit back to the Login screen.

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



13.4 ITEM AUTHORISATION

NOTE: The Authorisation option is not available if you are using RRMS

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.

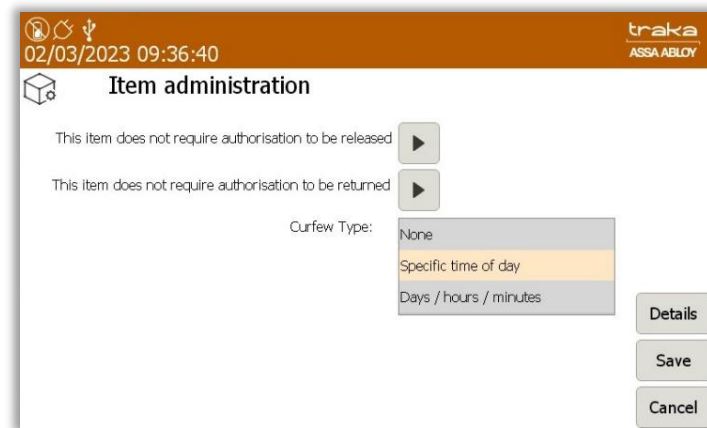
NOTE: A system with non-locking receptor strips will release an item without prompting authorisation.

13.4.1 SETTING UP THE ITEMS

NOTE: This action can only be performed by an Admin user. Please refer to 'Ways to Access the System' 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 from the bottom right-hand corner of the screen.
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.

13.4.2 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.

The screenshot shows the Traka system interface. At the top, the status bar displays the date and time '02/03/2023 10:24:30' and the Traka logo with 'ASSA ABLOY' underneath. The main display area shows 'Pos 1: Warehouse Key' and a welcome message: 'Welcome Traka Admin, authorisation granted.' To the right of the text is a numeric keypad with buttons for digits 1-9, 0, a red 'X' for cancel, and a green checkmark for confirm. A 'Cancel' button is located at the bottom left of the keypad area.

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

The screenshot shows the Traka system interface. At the top, the status bar displays the date and time '02/03/2023 10:46:59' and the Traka logo with 'ASSA ABLOY' underneath. The main display area shows 'Pos 1: Warehouse Key' and a message: 'Item 1 requires authorisation for removal. Please ask authoriser 2 of 2 to swipe their Card or enter their Keypad ID.' To the right of the text is a numeric keypad with buttons for digits 1-9, 0, a red 'X' for cancel, and a green checkmark for confirm. A 'Cancel' button is located at the bottom left of the keypad area.

4. Once all authorisers have been verified, the item will be released from the system.

The screenshot shows the Traka system interface. At the top, the status bar displays the date and time '02/03/2023 10:27:46' and the Traka logo with 'ASSA ABLOY' underneath. The main display area shows 'Pos 1: Warehouse Key' and a welcome message: 'Welcome Traka User 01, authorisation granted.' To the right of the text is a numeric keypad with buttons for digits 1-9, 0, a red 'X' for cancel, and a green checkmark for confirm. A 'Cancel' button is located at the bottom left of the keypad area.

NOTE: If an Authoriser requests to take an item that has been configured with 1 or more authorisers, they will also need to seek authorisation from another authoriser. In other words, the authoriser cannot authorise themselves.

13.4.3 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.

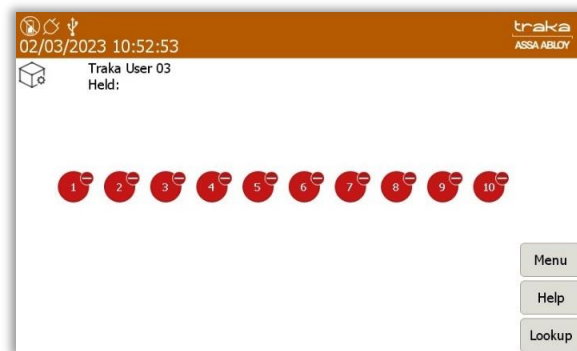
For more information on configuring the Authoriser from a Different Group option, please refer to **UD0018 – TrakaWEB User Guide** and **UD0260 – TrakaWEB Version 4 User Guide**.

13.4.3.1 USER PROCESS - REMOVAL

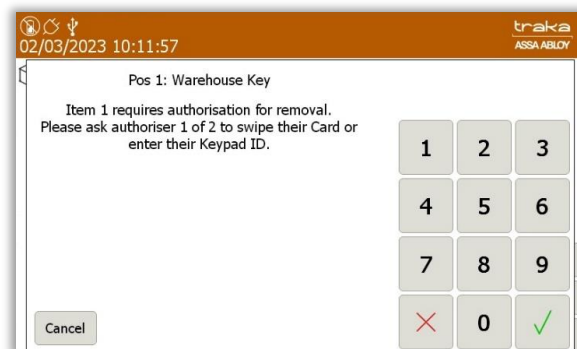
The following example assumes that the User without the authoriser role is in a separate User Group from the Users that do have the authoriser role. The Item that the User is requesting requires two Authorisers. In turn, these must be in separate groups.

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

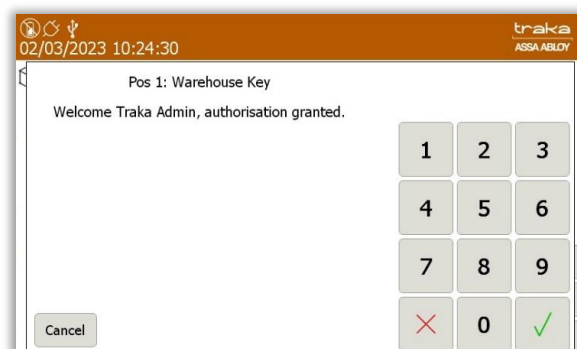
NOTE: If the user is not assigned to a User Group, they will be unable to access any items that require authorisation from authorisers in different groups. They will then see the following screen in Traka Touch:



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.

The screenshot shows a software interface with an orange header bar. On the left of the header are icons for a person, a key, and a USB symbol, followed by the date and time '02/03/2023 10:46:59'. On the right is the 'traka ASSA ABLOY' logo. The main area has the text 'Pos 1: Warehouse Key' and 'Item 1 requires authorisation for removal. Please ask authoriser 2 of 2 to swipe their Card or enter their Keypad ID.' Below this text is a numeric keypad with buttons for digits 1-9, 0, a red 'X' for cancel, and a green checkmark for confirm. A 'Cancel' button is also present in the bottom left corner.

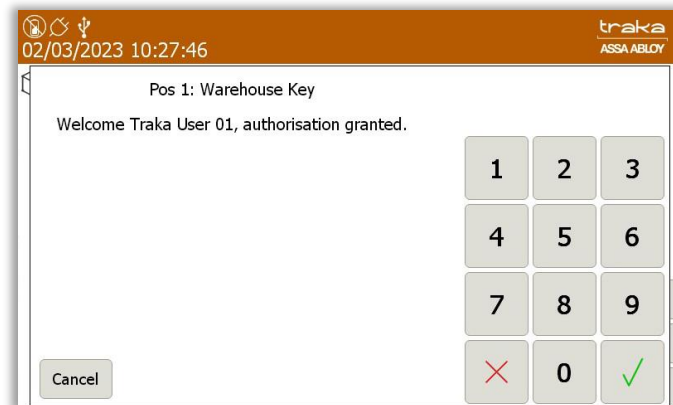
As previously mentioned, authorisers must belong to different User Groups. If an authoriser from the same group attempts to access the system, the following message will appear:

The screenshot shows the same software interface as before, but with a different message: 'Pos 1: Warehouse Key' and 'Each authoriser must belong to a different authoriser group!'. The numeric keypad and 'Cancel' button remain in the same positions.

It is also important that each authoriser is different. The person attempting to remove the Item/iFob cannot authorise them self.

The screenshot shows the same software interface, but with the message: 'Pos 1: Warehouse Key' and 'Each authoriser must be different!'. The numeric keypad and 'Cancel' button remain in the same positions.

Once an authoriser from a different User Group accesses the system, the following message will appear:

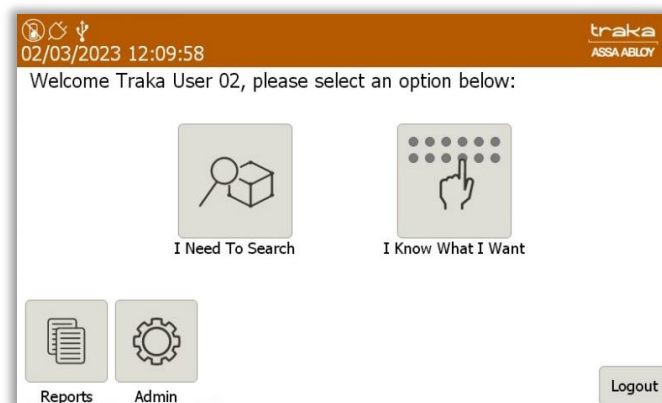


The Item/iFob will then be released to the User.

13.4.3.2 USER PROCESS – RETURN

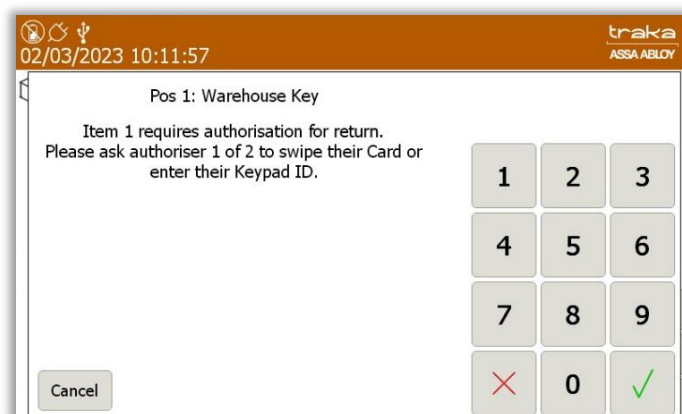
This example assumes that the User without the authoriser role is in a separate User Group from the Users that do have the authoriser role. The Item that the User is returning requires two Authorisers. In turn, these must be in separate groups.

1. The user without authorisation logs into the system to return an Item/iFob and is presented with the following screen.

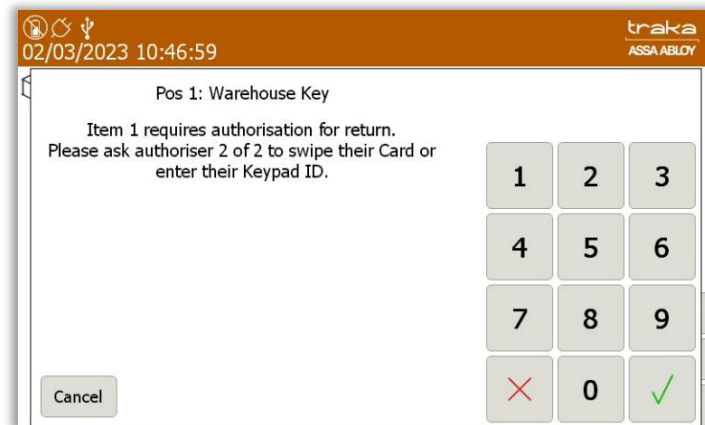


2. After selecting **I Know What I Want**, the door will open, and the user may return the item/iFob.

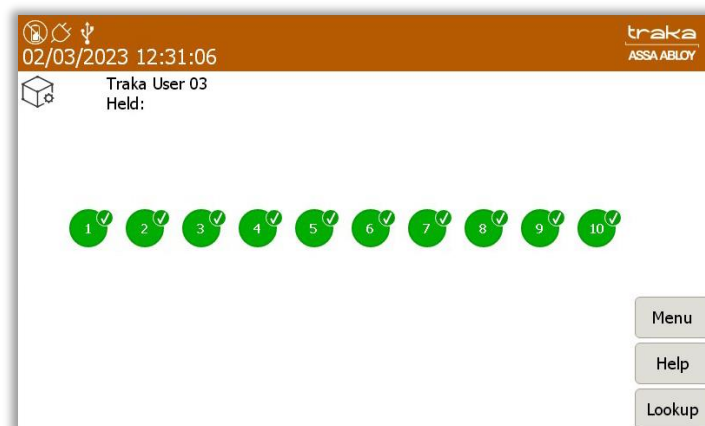
At this stage, a message will be displayed requesting that an authoriser must enter their ID at the touch screen.



In this example, 2 authorisers are required.



Upon successful completion, the door maybe closed.



13.5 EXPORTING & IMPORTING

NOTE: This section does not apply to systems with RRMS enabled.

It is possible to export and import information such as users, items and permissions 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. Please view the relevant sections below.

To use the import feature, you would first need to enter all 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: For further information on USB memory stick specification, refer to section [6.2](#).

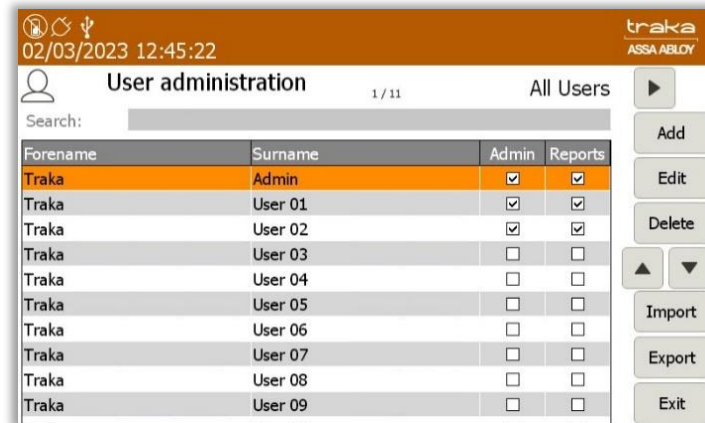
NOTE: If your current user list is empty, the spreadsheet will still be exported to your USB memory stick.

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.

13.5.1 EXPORTING USERS

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

1. Identify yourself to the system and select **Admin**.
2. Select **Users**.

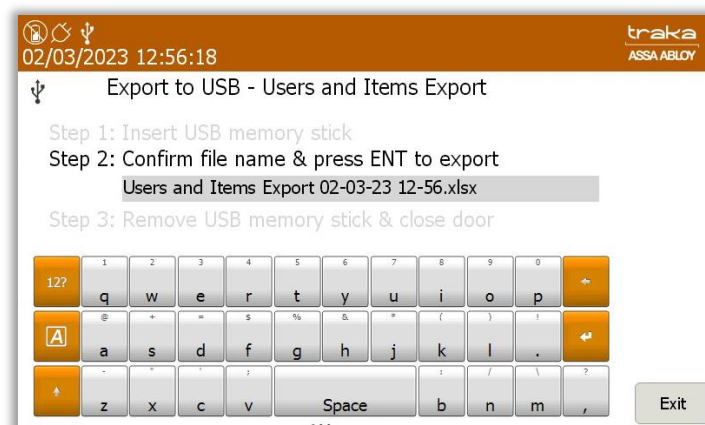


3. Select the **Export** button.
4. The system door will open and prompt you to insert a USB stick into the vacant socket.

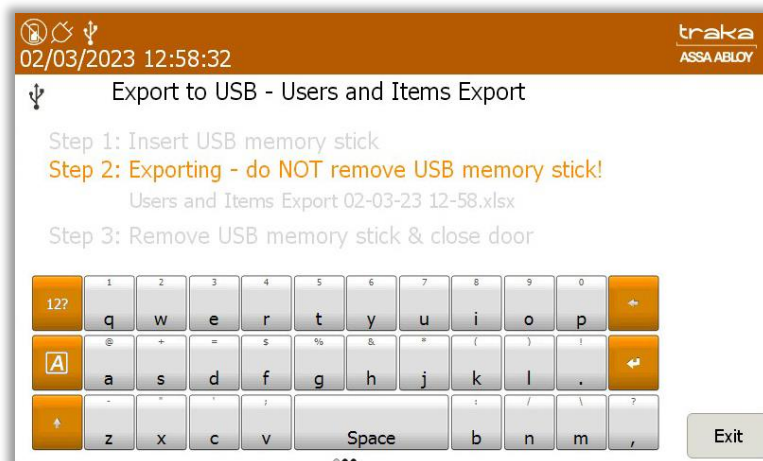


NOTE: The USB location will be different depending on which Traka Touch system you have. Please consult your separate installation document or the system drawings you have been provided with. If in doubt, please contact Traka using the [Technical Support](#) page at the end of this document.

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.

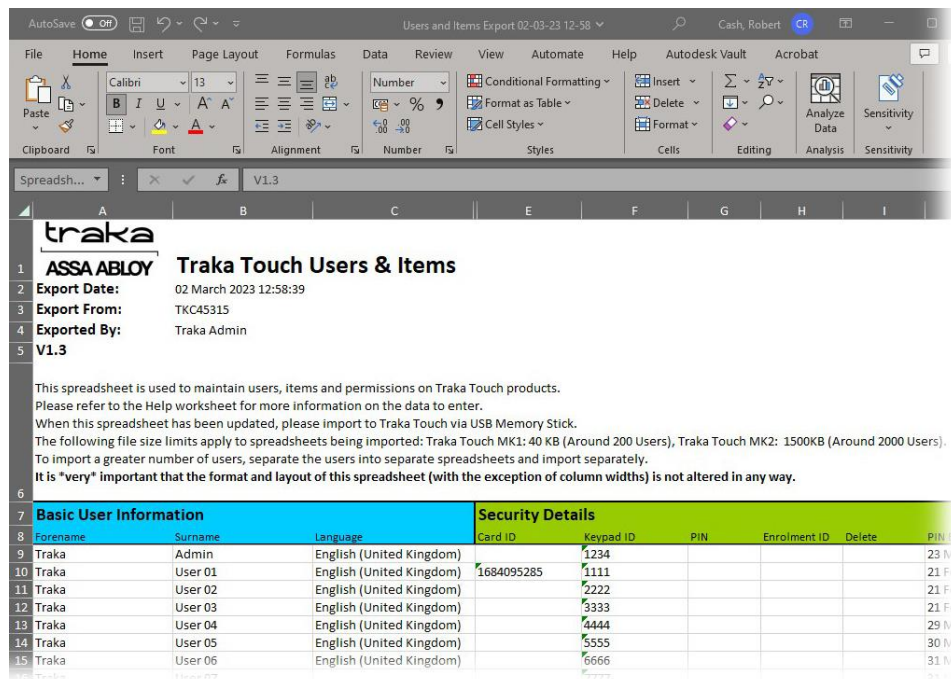
13.5.2 IMPORTING USERS

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 do not need to fill in all the information; it is there to be completed if required.

1. Export the Spreadsheet as explained in the 'Exporting Users' section.
2. Open the Spreadsheet on a PC.



- 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	Authoriser
21 February 2023 08:53:23	21 February 2073 08:53:23		Y	Y	Y
21 February 2023 00:00:00	21 February 2053 00:00:00		0 Y	Y	Y
21 February 2023 00:00:00	21 February 2053 00:00:00		Y	Y	Y
21 February 2023 00:00:00	21 February 2053 00:00:00				
27 February 2023 15:00:24	27 February 2073 15:00:24				
28 February 2023 15:17:52	28 February 2073 15:17:52		0		
01 March 2023 14:49:11	01 March 2073 14:49:11				
01 March 2023 14:50:00	01 March 2073 14:50:00				
01 March 2023 14:50:41	01 March 2073 14:50:41				
01 March 2023 14:51:09	01 March 2073 14:51:09				
01 March 2023 14:51:41	01 March 2073 14:51:41				

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.

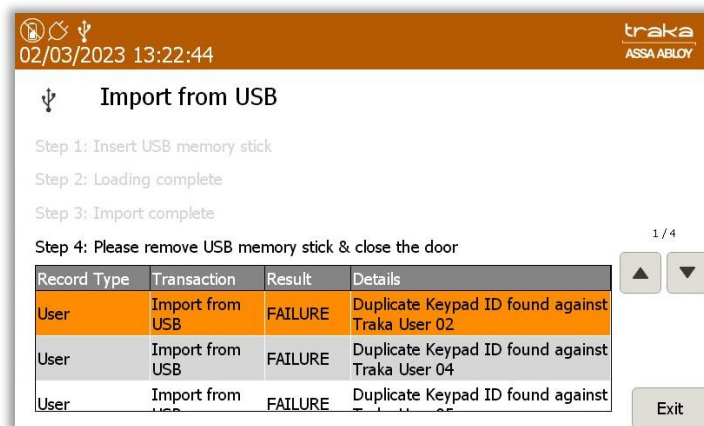
Item Descriptions	1	2	3	4	5	6	7	8	9	10	11	12
Warehouse Key	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Reception Door	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Store Room	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Ground Floor Meeting Room	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
First Floor Meeting Room	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Kitchen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Training Room	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Server Room	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
Ground Floor Office	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
First Floor Office	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		

- When finished save the Spreadsheet onto a 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.

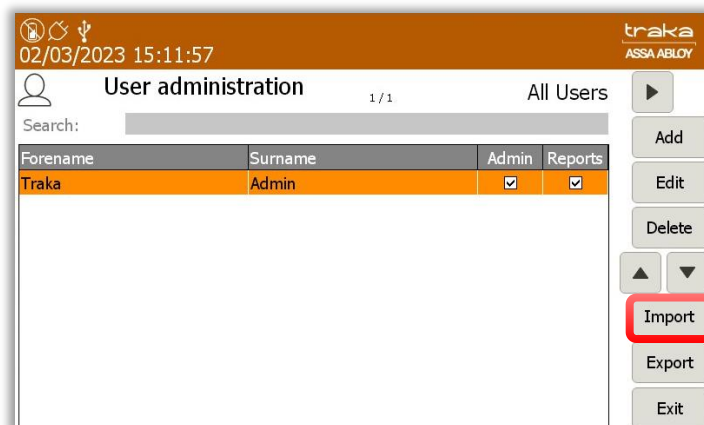


13.5.2.3 IMPORTING THE INFORMATION INTO THE SYSTEM

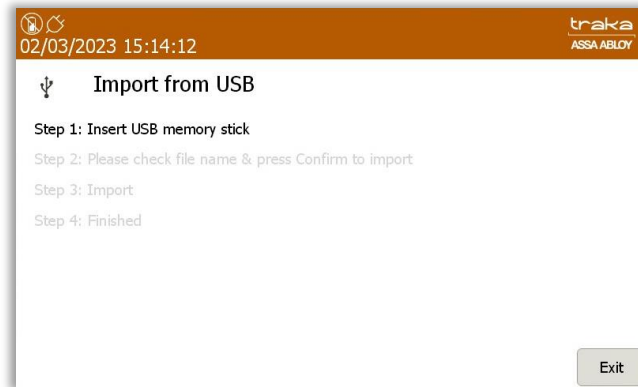
NOTE: This action can only be performed by an Admin user.

NOTE: For further information on USB memory stick specification, refer to section [6.2](#).

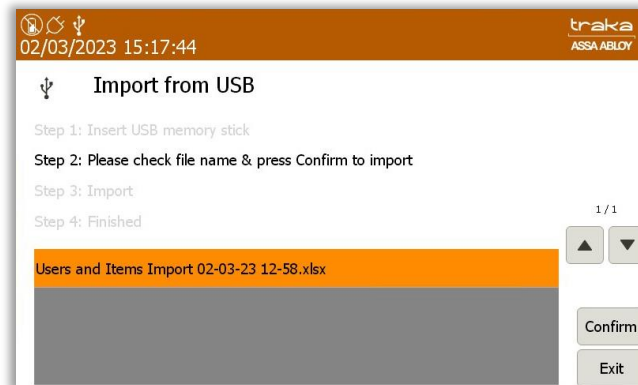
1. Access the system and click **Admin**.
2. Click **Users**.
3. Select the **Import** Button.



4. The system door will open and prompt you to insert a USB stick into the USB socket.



5. Select the correct file from the USB.



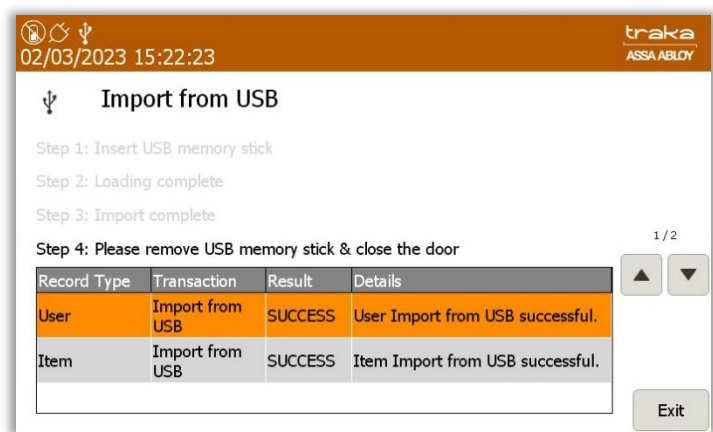
6. You will then be asked if you would like to import the user list. Click **Yes**.



7. The system will then begin to load and import the list.



- Once complete the table will display that the import was a success. You can now remove the USB memory stick.

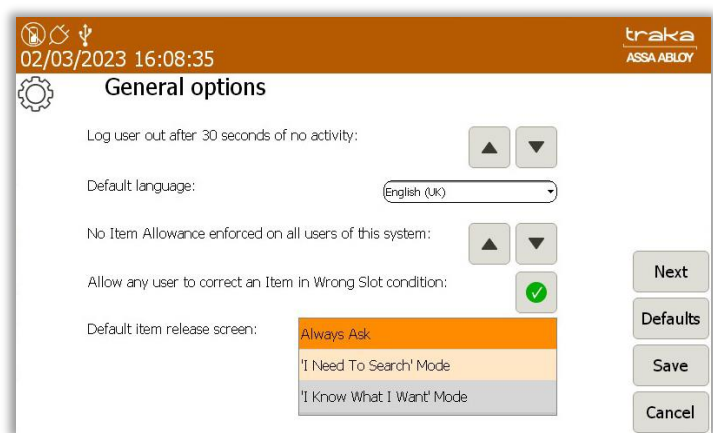


NOTE: If there is an error while importing, please contact Traka Support using the technical support page at the back of this document.

13.6 GENERAL OPTIONS

NOTE: Accessing the General Options must be carried out by an administrator.

- Access the system and click the **Admin** button.
- 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 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 recommend 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 dropdown menu to select the desired language to enable a new system default language. When a user logs out of the system, the system will revert 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.

Item Allowance

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

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

Allow Any User to Correct an iFob in Wrong Slot condition

When a user returns an item to an incorrect position in the system, Traka Touch will inform that user that the item belongs in another position. The system will release the item and allow them to remove the item then insert it into the correct position.

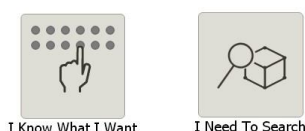
If the 'Allow Any User to Correct an iFob in Wrong Slot Condition' is ticked, any user can select the item in the wrong compartment and the system will release the door regardless of that user's access and permissions. Both doors will open allowing the user to return the item to the correct compartment.

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 any user to be allowed to move incorrectly positioned items from the wrong location to the right location, leave this option ticked, otherwise un-tick the option to turn this feature off.

Default Item Release Screen

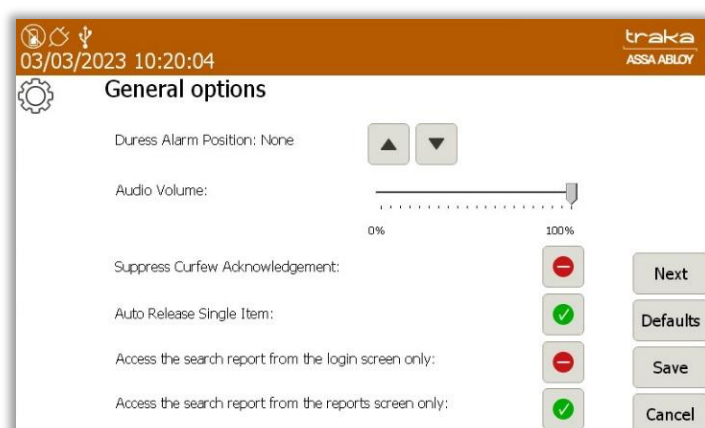
The latest Traka Touch application can display a selection screen that appears when a valid user logs into the system, depending on what option is enabled in the general options. This selection screen can have one or both of the following buttons depending on what is selected in the General options.



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 of the 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.

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.

Auto Release Single Item

The option for 'Auto Release Single Item' is located on the second page of 'General Options' under the 'Admin' option. If a user has entitlement to only one item and no access to admin or report functions, it will be released to them automatically once they have entered their ID number. This function also eliminates any on-screen navigational requirements by the user and will also allow them to return the item once it has been released. By default, this option is set as active but can be deactivated if required. To achieve this, click on the icon next to 'Auto Release Single Item', to toggle between the two states.

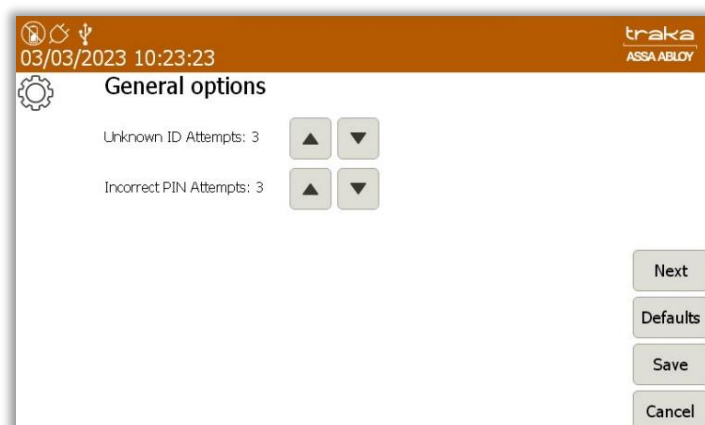
Access the Search Report from the Login Screen only

Selecting 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

Selecting 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.

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**.

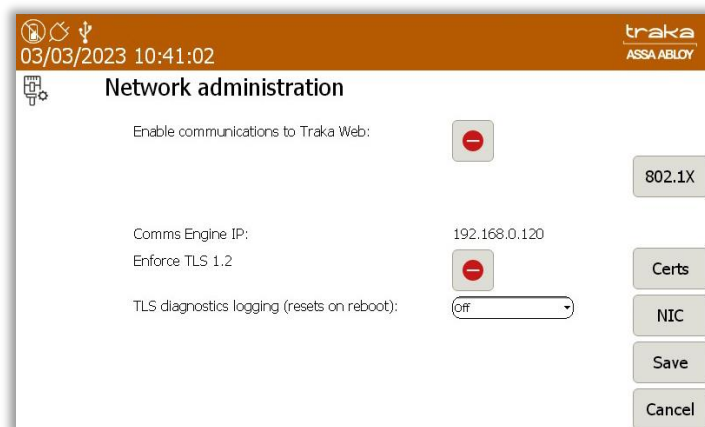
13.7 NETWORK ADMINISTRATION

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

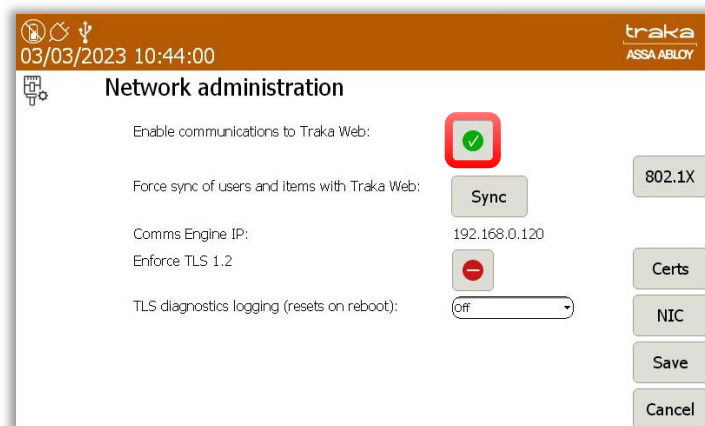
Please ensure TrakaWEB has been installed and configured before continuing. Please read the latest revision of **TD0013 – Traka Web Installation Guide** and **TD0216 – TrakaWEB Version 4 Installation & Configuration Guide** for more information.

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.



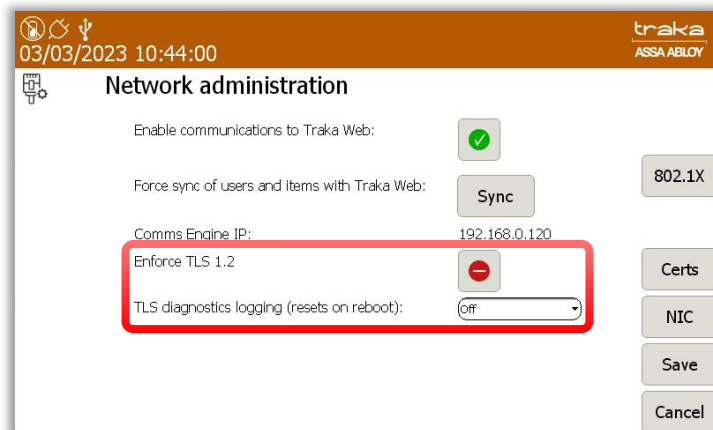
3. To enable communications with TrakaWEB simply select the red line button and ensure the symbol changes to a green tick. The Comms Engine and the Security Mode will remain unknown until you are connected to Traka Web. Once connected the comms engine will display the IP address and the security mode will show the security type used e.g., Comms Engine – 192.168.0.120. Security Mode – SSL.



4. Force sync of users and items with Traka Web?
5. To save changes click **Save**. To view/change other settings please click the **NIC** button.

13.7.1 ENFORCE TLS 1.2

Within Traka Touch Network Administration, there is an Administration Option called **Enforce TLS 1.2**



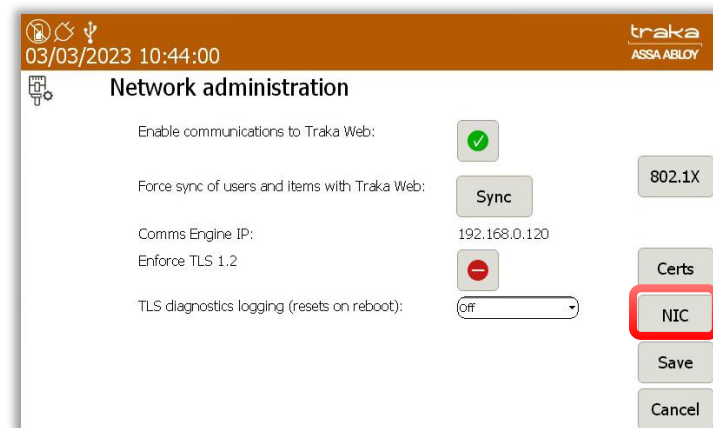
This option is turned off by default. In this state, Traka Touch will communicate with the Comms Engine using TLS 1.0.

With the option enabled, Traka Touch will ONLY communicate with the Comms Engine using TLS 1.2

NOTE: A diagnostics option is available within Network Administration. With the Enforce TLS 1.2 enabled you can configure TLS 1.2 logging levels. This should only be used under the guidance of Traka Support.

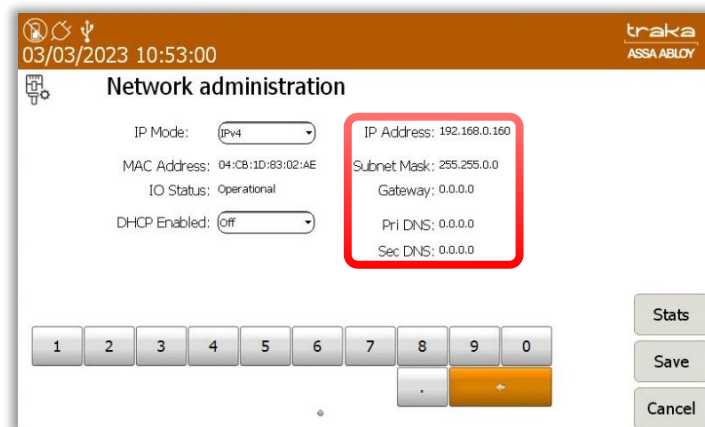
13.7.2 NIC (NETWORK INTERFACE CONTROLLER) SETTINGS

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



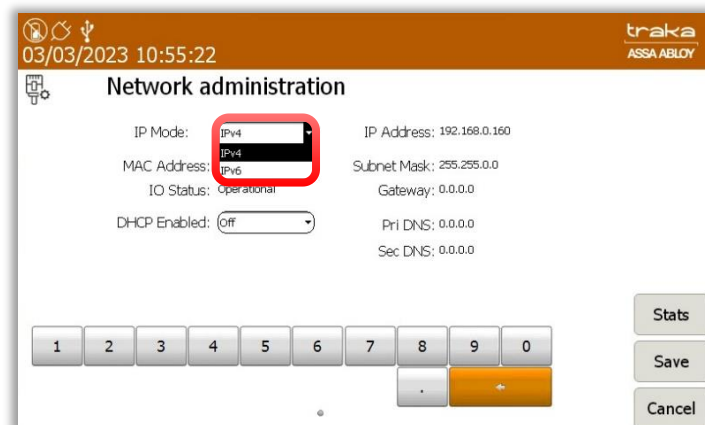
From here, you can view and change your IP address, IPv4 or IPv6, subnet mask, gateway, DNS etc.

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.



The screenshot shows the 'Network administration' screen of the Traka system. The top bar displays the date and time '03/03/2023 10:53:00' and the Traka logo. The interface includes a status bar with icons for signal, battery, and USB. The main content area shows the following settings: IP Mode (IPv4), MAC Address (04:CB:1D:83:02:AE), IO Status (Operational), and DHCP Enabled (Off). A red box highlights the IP Address (192.168.0.160), Subnet Mask (255.255.0.0), Gateway (0.0.0.0), Pri DNS (0.0.0.0), and Sec DNS (0.0.0.0) fields. At the bottom, there is a numeric keypad with buttons for digits 1-9, 0, a decimal point, and a plus sign. On the right side, there are buttons for 'Stats', 'Save', and 'Cancel'.

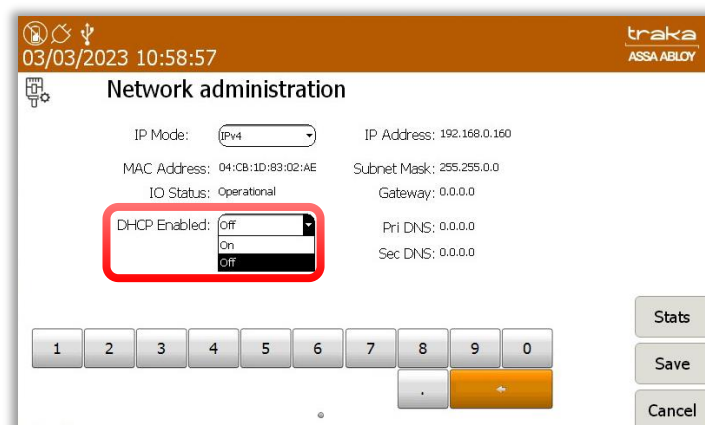
To change the IP Mode, select IP Mode, followed by the Internet Protocol version that you want, IPv4 or IPv6.



This screenshot shows the 'Network administration' screen with the IP Mode dropdown menu open. The dropdown menu lists 'IPv4' and 'IPv6'. A red box highlights the dropdown menu. The other settings remain the same as in the previous screenshot. The bottom keypad and right-side buttons are also visible.

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.



This screenshot shows the 'Network administration' screen with the DHCP Enabled dropdown menu open. The dropdown menu lists 'Off', 'On', and 'Off'. A red box highlights the dropdown menu. The other settings remain the same as in the previous screenshots. The bottom keypad and right-side buttons are also visible.

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.

03/03/2023 11:02:21

traka
ASSA ABLOY

Network administration

Announce listening:

Announce connected:

TCP Statistics:

Connections Accepted: 12

Current Connections: 3

Connections Initiated: 67

Cumulative Connections: 7

Failed Connect Attempts: 0

Errors Received: 0

Reset Connections: 4

TCP Connections:

Announce health:

IP Statistics: Passive Opens: 212553

Packets Received: 212553

Received Header Errors: 0

Received Address Errors: 425

Received Packets Delivered: 212151

Received Packets Discarded: 11

Adapter State:

Status: Operational

IP Address: 192.168.0.160

Refresh

Save

Cancel

Protocol	LocalAd	LocalPor	Remote	Remote	State
TCP	0.0.0.0	5655	0.0.0.0	0	Listen
TCP	0.0.0.0	5800	0.0.0.0	0	Listen
TCP	0.0.0.0	5900	0.0.0.0	0	Listen
TCP	192.168.1	5900	192.168.1	52953	Establishe
TCP	192.168.1	9998	192.168.1	52952	Establishe

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

Announce listening:

Announce connected:

Announce health:

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

Announce listening:

Announce connected:

Announce health:

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.

Announce listening:

Announce connected:

Announce health:

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.

13.7.3 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.

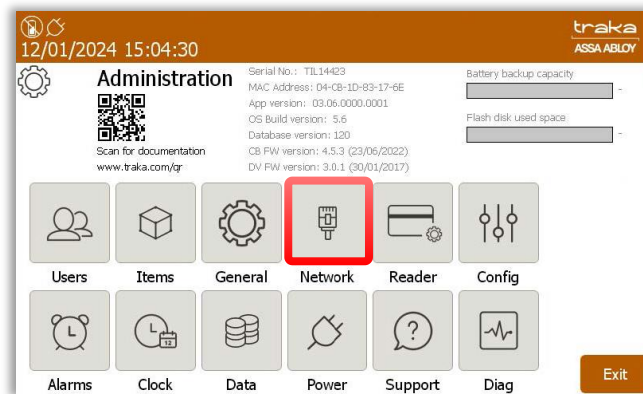
NOTE: Access to the SNMP options can only be performed by an Admin user.

To support the functionality of SNMP, OS v4.4 must be installed for the iMX28 control board and OS v5.4 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

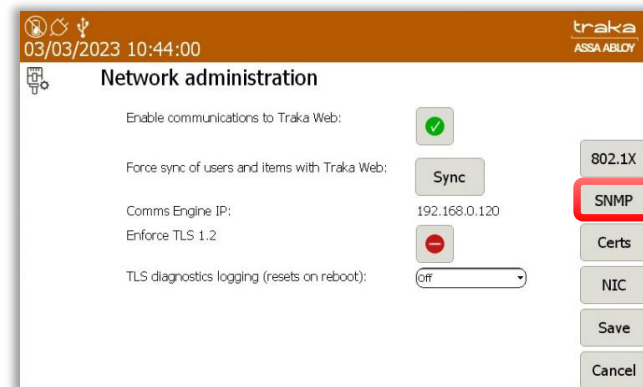
1. Access the system and select the **Admin** button.

2. Select the **Network** button.

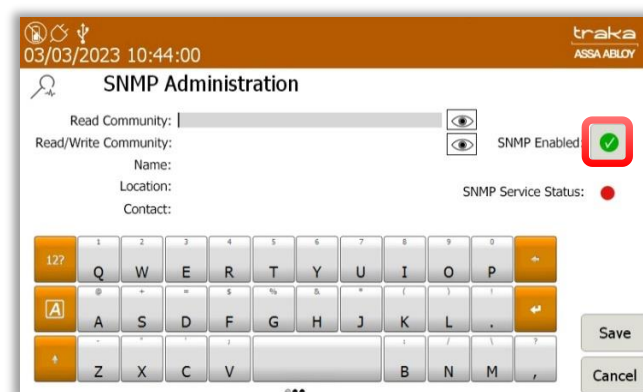


3. Select the **SNMP** button to the right of the screen.

You will now be taken to the SNMP Administration screen.



4. To enable SNMP, select the **SNMP Enabled** button. 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.

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.



13.7.4 802.1X SUPPORT

802.1X is an IEEE standard for Port-Based Network Access Control (PNAC) and provides an authentication mechanism to devices wishing to attach to a Local Area Network.

Please note that when setting up the support for 802.1X, you will require or need to obtain certain information such as Certificates and Certificate Keys utilised by the RADIUS server which will verify the credentials of any network device trying to access the 802.1X network.

NOTE: The Client Certificates will have to be in PEM format and include the full chain which should also incorporate the Root certificate plus the Private key.

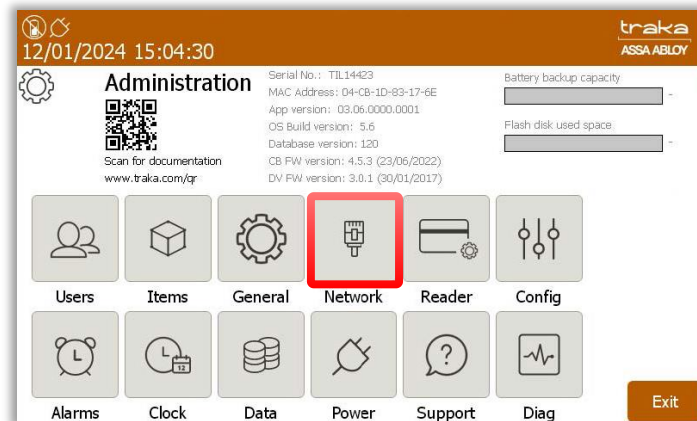
NOTE: Access to the 802.1X options can only be performed by an Admin user.

NOTE: 802.1X is only supported by the MK3 Control Board (iMX6) with a minimum OS of v5.0.

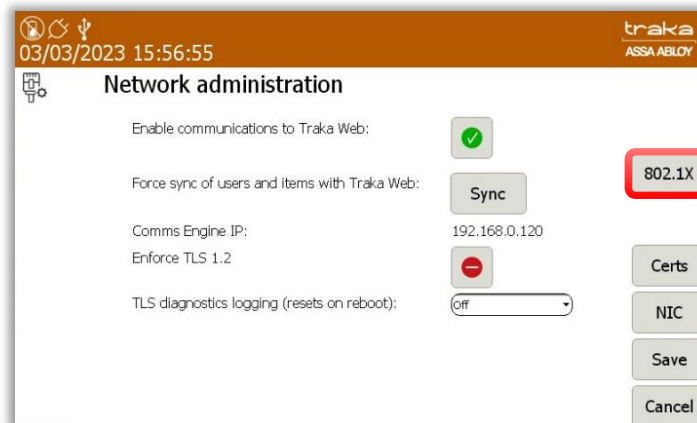
NOTE: For more technical information concerning 802.1X please refer to TD0214 - 802.1x Configuration Guide for Traka Touch.

To support the functionality of 802.1X, Traka Touch App version 3.1.0 or higher is required.

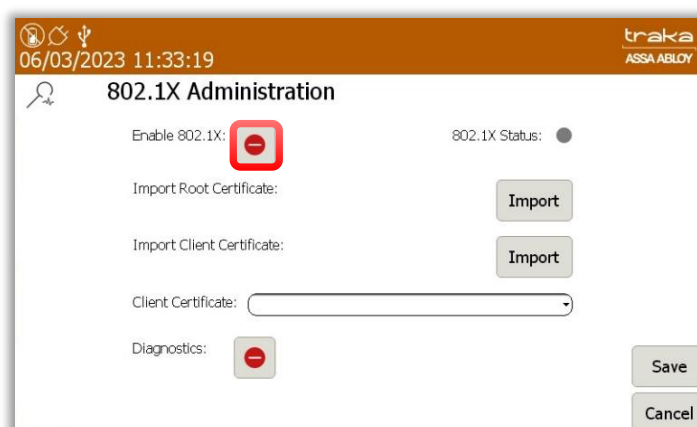
1. Access the system and select the **Admin** button.
2. Select the **Network** button.



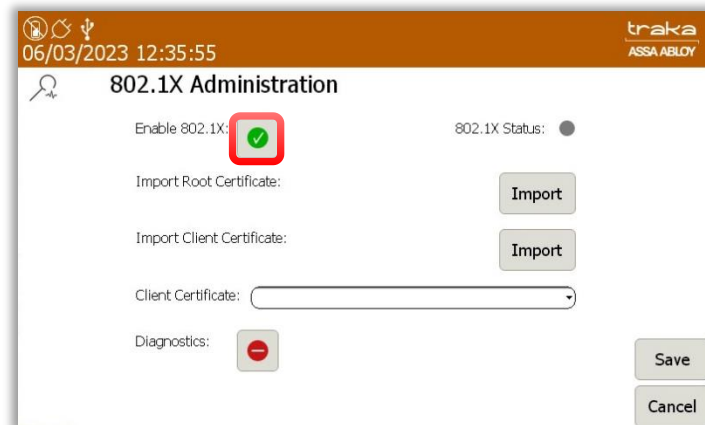
3. Select the **802.1X** button to the right of the screen.



You will now be taken to the 802.1X Administration screen.



4. To Enable 802.1X simply select the red line button and ensure the symbol changes to a green tick.

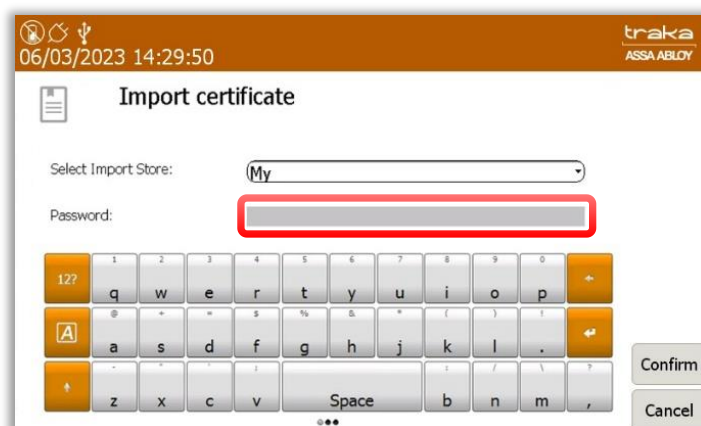


5. You will now be required to complete the fields shown on the screen using the keypad.

When you want to import a Root or Client certificate from a USB memory stick to utilise with 802.1X, please select the appropriate button. This will take you to the following screen:



6. When you import the client certificate you will be required to enter the Private key password.



7. Once the certificate import has been completed, the following screen will be displayed. Select the **OK** button.

8. Now select the Client Certificate from the pull-down menu button and select the **Save** button once you have finished to take you back to the 'Network administration' screen.

The following options and status indicators are available:

Import Root Certificate:

Select the Import button to go to the certificate import page, allowing you to import the 'Root Certificate'.

Import Client Certificate:

Select the Import button to go to the certificate import page, allowing you to import the 'Client Certificate'.

Client Certificate:

This dropdown button will display and allow the selection of all certificates loaded through the client certificate import process, that have not expired or been deleted.

Status:

The following status is displayed when the 802.1X service is unavailable:

802.1X Status: 

The following status is displayed when the 802.1X service is authenticating:

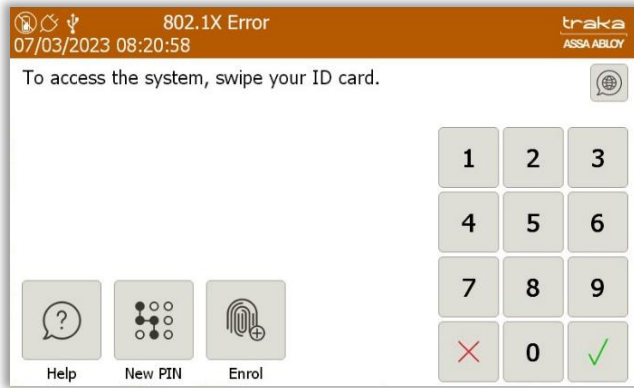
802.1X Status: 

The following status is displayed when the 802.1X service has authenticated:

802.1X Status: 

If the Traka Touch detects an error or problem with the functionality of 802.1X, then one of the following error messages will be displayed:

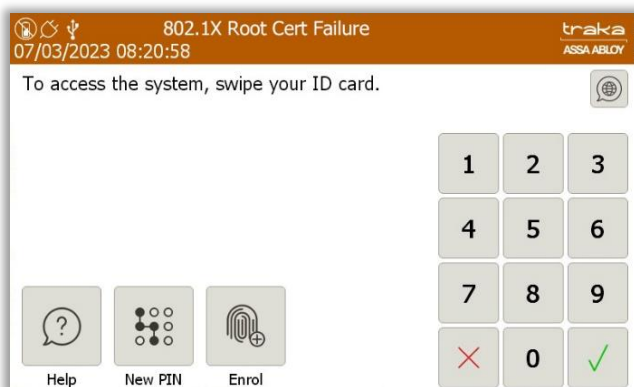
General 802.1X Error



Client Certificate Missing



Root Certificate Failure

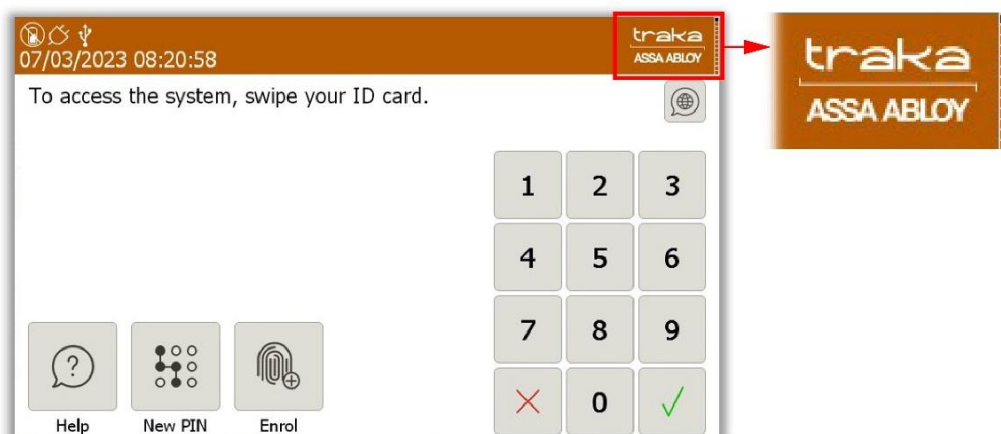


Private Key Missing



13.7.5 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.

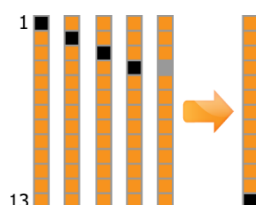


Each block represents a different stage of communication with TrakaWEB. See below for a description of each stage.

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.

13.7.6 ADD THE NEW CA CERTIFICATE INTO THE TRAKA TOUCH 'ROOT STORE' (V2.3.0 & LATER)

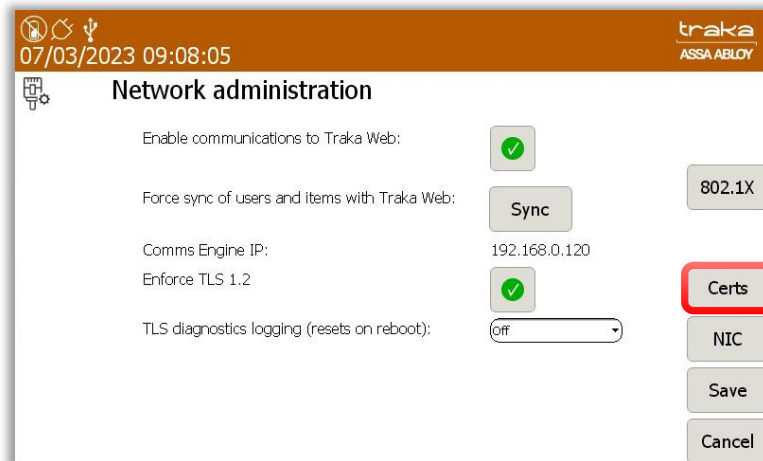
A Public Key Certificate is an electronic document used to prove ownership of a Public Key. The certificate will include information about the key, the identity of its owner and the digital signature of an entity that has verified the certificates contents. If the signature is valid and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificates subject.

A Private Key is used in combination with a Public Key in SSL/TLS protocol to authenticate, secure and manage secure connections during the SSL/TLS handshake process to set up a secure session.

For more information, refer to **TD0179 – Changing Certificates in TrakaWEB & Traka Touch**

In v2.3.0 or later of the Application software a new screen for certification management is added.

Select the **Network** menu from the **Admin** menu followed by the **Certs** button.



07/03/2023 09:08:05

traka
ASSA ABLOY

Network administration

Enable communications to Traka Web: ☒

Force sync of users and items with Traka Web: 802.1X

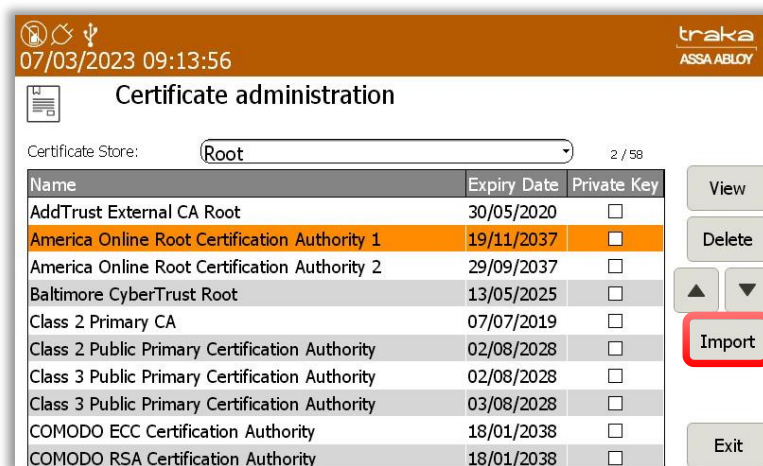
Comms Engine IP: 192.168.0.120

Enforce TLS 1.2: ☒

TLS diagnostics logging (resets on reboot):

Certs
NIC
Save
Cancel

Select **Import**.



07/03/2023 09:13:56

traka
ASSA ABLOY

Certificate administration

Certificate Store: 2 / 58

Name	Expiry Date	Private Key
AddTrust External CA Root	30/05/2020	☐
America Online Root Certification Authority 1	19/11/2037	☐
America Online Root Certification Authority 2	29/09/2037	☐
Baltimore CyberTrust Root	13/05/2025	☐
Class 2 Primary CA	07/07/2019	☐
Class 2 Public Primary Certification Authority	02/08/2028	☐
Class 3 Public Primary Certification Authority	02/08/2028	☐
Class 3 Public Primary Certification Authority	03/08/2028	☐
COMODO ECC Certification Authority	18/01/2038	☐
COMODO RSA Certification Authority	18/01/2038	☐

View
Delete
▲ ▼
Import
Exit

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



07/03/2023 09:30:21

traka
ASSA ABLOY

Import from USB

Step 1: Insert USB memory stick

Step 2: Please check file name & press Confirm to import

Step 3: Import

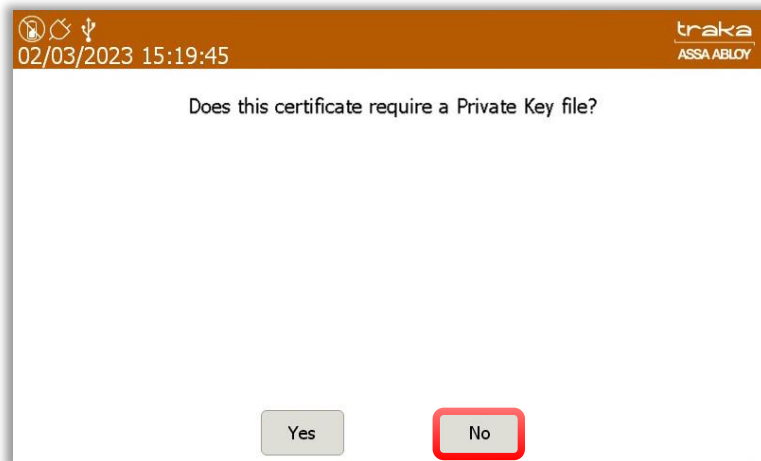
Step 4: Finished

0 / 0

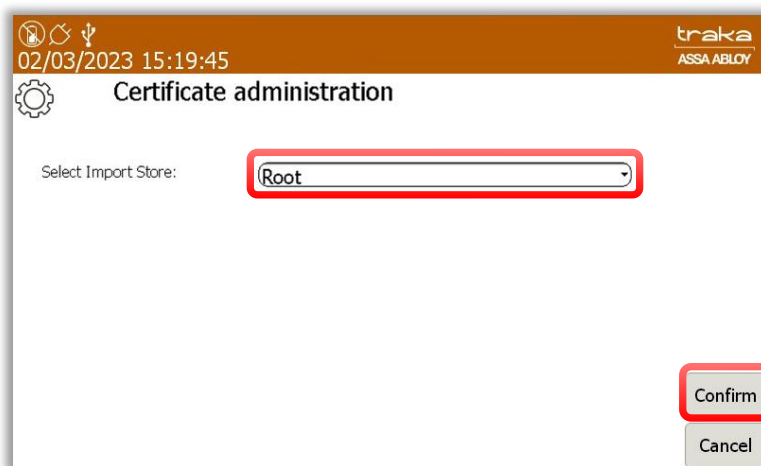
Alliance_Issuing_CA.cer

Confirm
Cancel

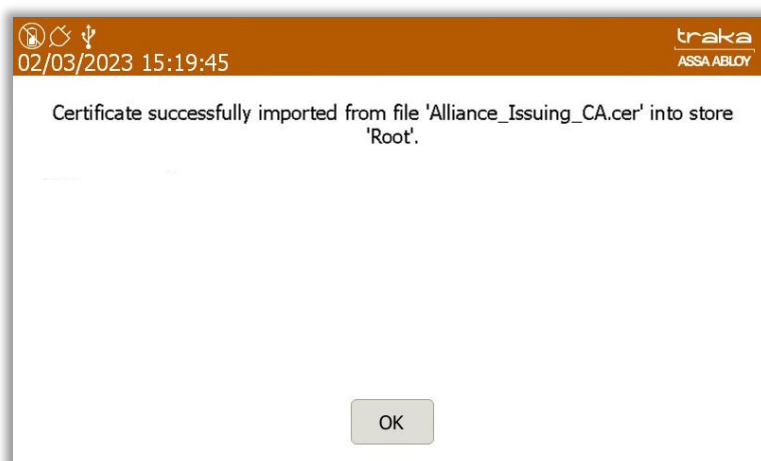
When prompted if the certificate requires a private key, select **No**.



Ensure that the selected import store is **Root** and select **Confirm**.



Once completed you will receive a message confirming that the certificate is imported.



13.7.7 ADD THE NEW CA CERTIFICATE INTO THE TRAKA TOUCH 'ROOT STORE' (PRE V2.3.0)

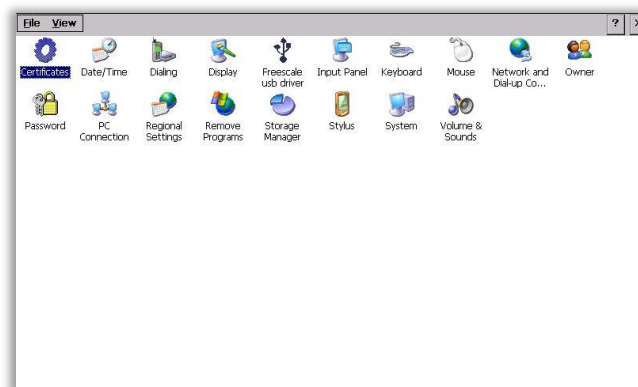
Enter the Traka Touch OS by selecting the **Cog** icon from the **Admin** menu, followed by **Yes** to exit Windows CE.



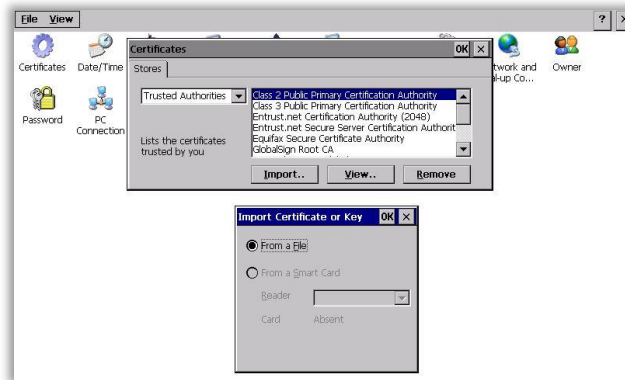
From the **Start** menu of the Touch OS, select **Settings** and **Control Panel**.



Double click on the **Certificates** icon followed by the **Import** button.



Import the CA Certificate with the .crt extension into the Traka Touch Root Store.

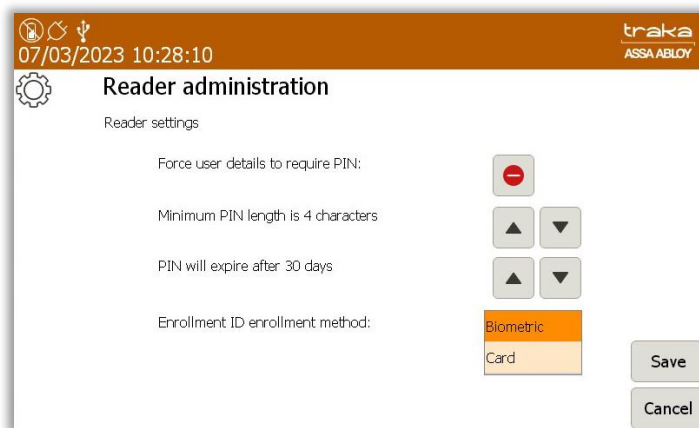


13.8 READER ADMINISTRATION

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

NOTE: Accessing the General Options must be carried out by an administrator.

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 100.

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 number of days being 365 days. You can also select the option 'PIN will Never Expire'.

Enrolment ID enrolment method

This option will enable you to choose between enrolling with biometric or card reader.

3. Once you have selected the desired options, click the **Save** button.

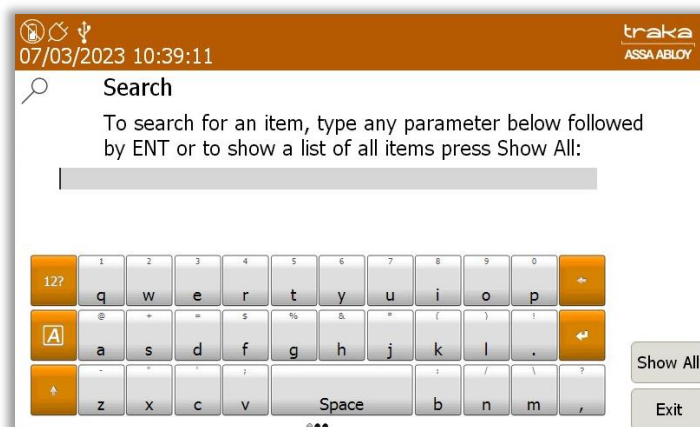
13.9 SEARCH FACILITY

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

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

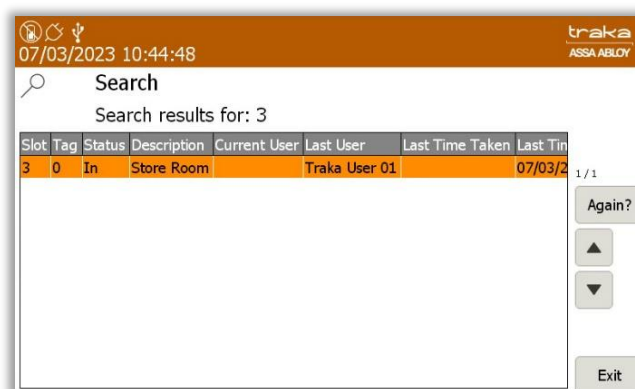
The search facility does not require a user to access the system; it can be used straight from the login screen.

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 position numbers.



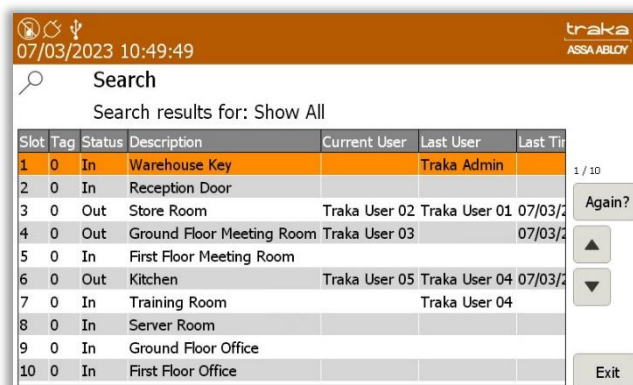
NOTE: Partial searches can be made, e.g., if you wanted to find a key that matched the description 'Front Car Park' instead of typing the whole description you could enter 'front' and the system will search for any description with that word. In addition, the searches are not case sensitive.

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.



Slot	Tag	Status	Description	Current User	Last User	Last Time
1	0	In	Warehouse Key		Traka Admin	
2	0	In	Reception Door			
3	0	Out	Store Room	Traka User 02	Traka User 01	07/03/2023
4	0	Out	Ground Floor Meeting Room	Traka User 03		07/03/2023
5	0	In	First Floor Meeting Room			
6	0	Out	Kitchen	Traka User 05	Traka User 04	07/03/2023
7	0	In	Training Room		Traka User 04	
8	0	In	Server Room			
9	0	In	Ground Floor Office			
10	0	In	First Floor Office			

5. To conduct another search, simply click **Again**.

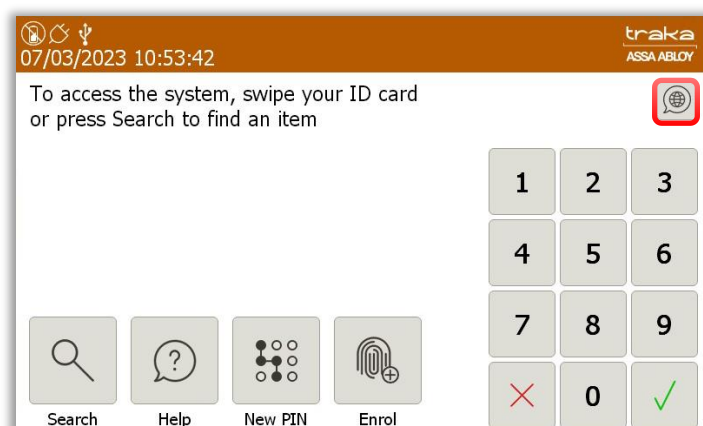
6. Click **Exit** to be return to the login screen.

13.10 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.

13.10.1 CHANGING THE LANGUAGE FOR A SINGLE LOGIN

From the main screen before you login, there are several language options from which to choose. 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.

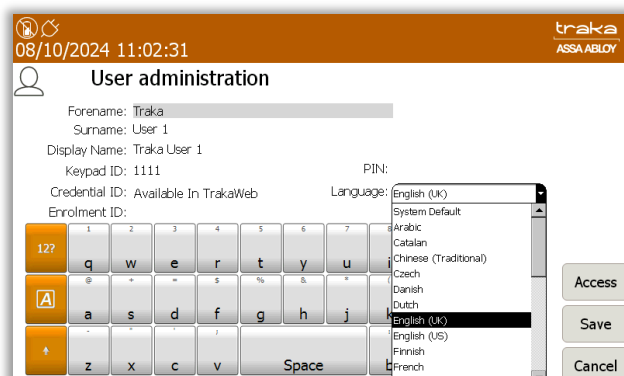
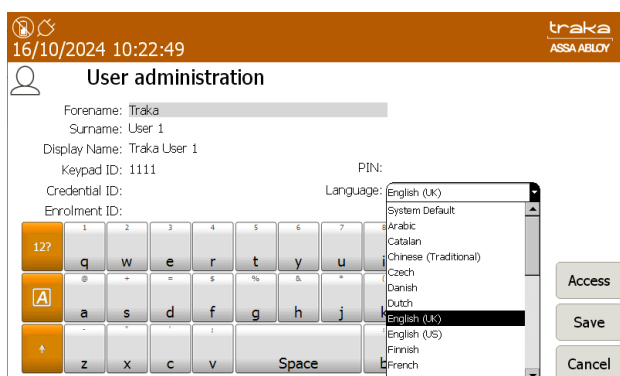




13.10.2 CHANGING LANGUAGES FOR A USER

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

1. Access the system.
2. Click the **Admin** button.
3. Click the **Users** button.
4. Highlight the user and click **Edit**.
5. 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.

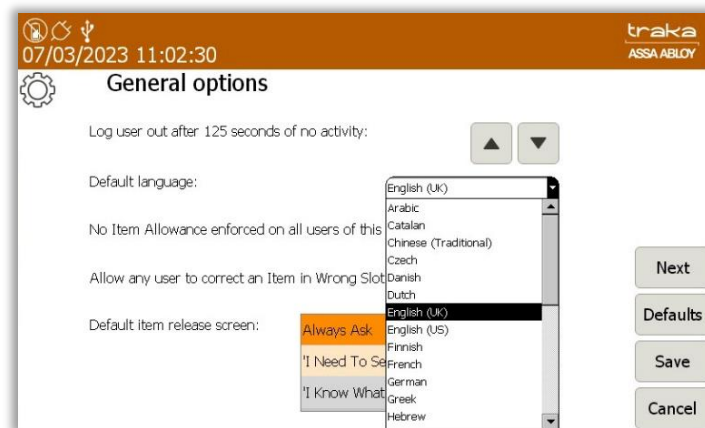


6. Once you have selected the desired language, click **Save**.
7. Click **Exit** and you will be taken back to the Admin screen. From there, click **Exit** again to return to the login screen.

13.10.3 CHANGING THE DEFAULT LANGUAGE OF THE SYSTEM

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

1. Access the system.
2. Click the **Admin** button.
3. Click the **General** button.
4. 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: By default, the Traka Touch system language is set to English.

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.

13.11 ALARMS

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 Event' and 'Off Event' columns detail what conditions must be met before an alarm is switched on or off.

In the example below, an alarm with 'Battery Critical' under 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.



To set an alarm against a relay, simply highlight the desired alarm and then 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.

13.11.1 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 below.

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 iFobs/RFID Tags is undetectable

Cleared under the following conditions:

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

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

13.11.2 TABLE OF ALARM EVENTS

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	<i>Timer</i>
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	<i>Timer</i>
Item Removed	<i>Timer</i>
Item Returned	<i>Timer</i>
Item Returned by a Different User	<i>Timer</i>
Item Returned To Wrong Slot	<i>Timer</i>
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	<i>Timer</i>
Overdue Item Returned	<i>Timer</i>
Override Key Unlocked	Override Key Locked
Panel Opened	Panel Closed
Power Restored	Power Fail
System Lockdown	System Lockdown End

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

13.12 CURFEWS

NOTE: This section is not applicable if you are using RRMS.

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 curfew, 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.

You can set curfews from TrakaWEB also. Please see the latest version of **UD0018 -TrakaWEB User Guide** and **UD0260 – TrakaWEB Version 4 User Guide** for more details.

13.12.1 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 18:30pm each day once it is removed.

NOTE: When in affect, this curfew applies only to the item it is enabled on.

13.12.1.1 HOW TO SET THE CURFEW

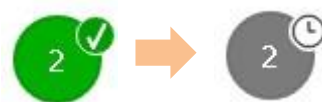
1. An administrator will need to access the system.
2. Click the **Admin** button.
3. Click the **Items** button.
4. Select an item from the list and click the **Edit** button.
5. From the bottom right-hand side of the screen select **Options** to be taken to the curfew page.
6. From here select the **Specific Time of Day** curfew from the drop-down box and set the Hours and Minutes using the directional arrow keys.

- 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

- A user will access the system.
- 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 a user defined period of time, e.g., five o'clock the same day it was removed.

- To remove the iFob the user must click the **Yes** button. Selecting **No** or closing the door will cancel the transaction and will require the user to log in again.
- After selecting **Yes** the iFob will be released allowing the user to remove the iFob. The icon will change from a tick to a grey icon with a curfew symbol displayed as shown here.



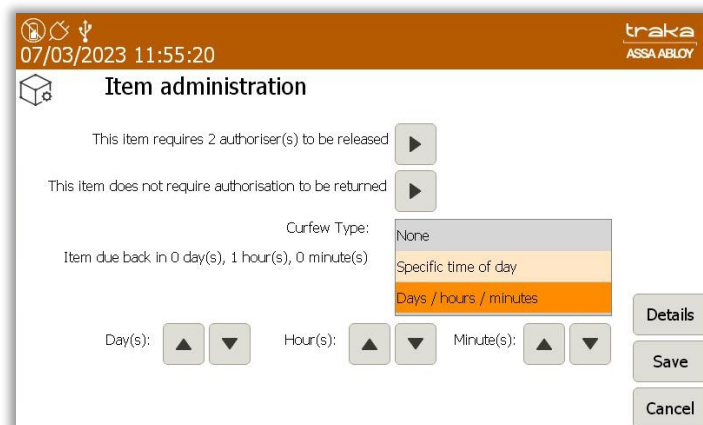
13.12.2 ITEMS WITH A 'NUMBER OF DAYS, HOURS AND MINUTES' CURFEW

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 then be able to set how many Days, Hours and Minutes the item is allowed to be out of the system.

NOTE: When in affect, this curfew applies only to the item it is enabled on.

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 then 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 Days, hours and minutes using the directional arrow keys.

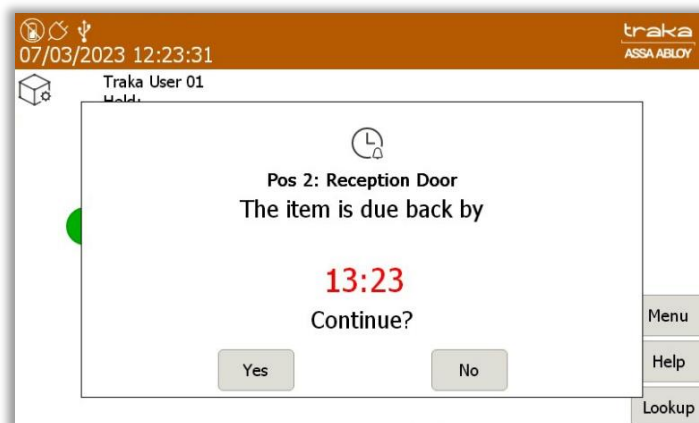


7. Once you have set the curfew click the **Save** button to be taken back to the user list. From there click **Exit** to go back to the admin menu and click **Exit** again to go back to the login screen.

13.12.2.2 USER PROCESS

The following is the process a user must go through to remove an iFob under an absolute curfew.

1. A user will access the system.
2. The user will then attempt to remove the iFob 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 days, 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 iFob the user must click the 'Yes' button. Selecting 'No' or closing the door will cancel the transaction and will require the user to log in again.

4. After selecting 'Yes', the iFob will be released allowing the user to remove the iFob. The on-screen icon will change from the 'green tick' to the following...



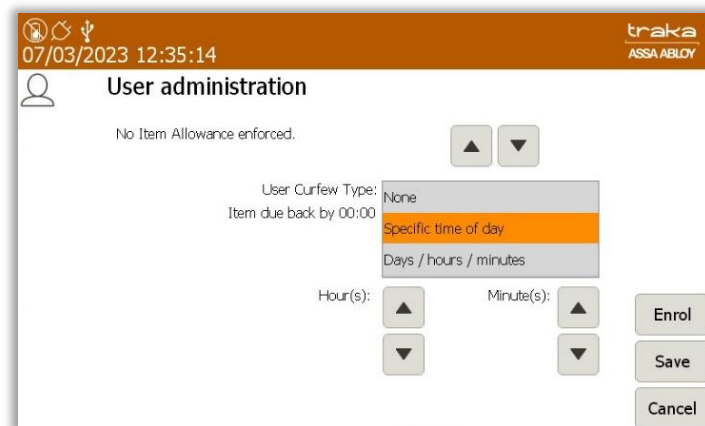
13.12.3 USERS WITH A 'SPECIFIC TIME OF THE DAY' CURFEW

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 item must be back in the system e.g., the item must be returned by 18:30pm each day once it is removed.

NOTE: When in affect 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

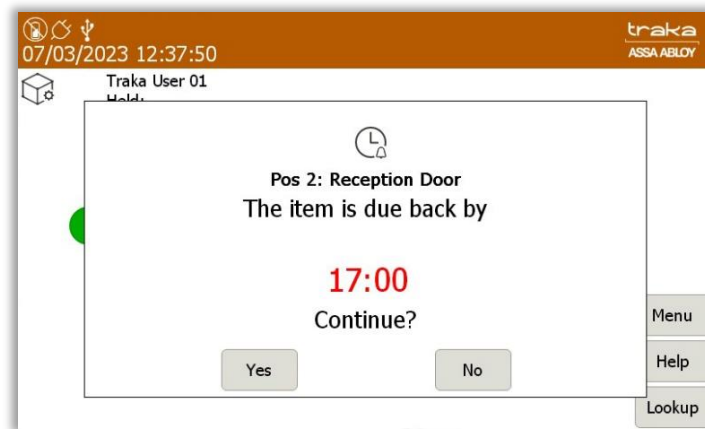
1. An administrator will need to access the system.
2. Click the **Admin** button.
3. Click the **Users** button.
4. Select a user from the list and click the **Edit** button.
5. From the bottom right-hand side of the screen select the **Access**, **Options** and **Next** buttons to be taken to the curfew 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, select the **Save** button to be taken back to the user list. From there, select **Exit** to go back to the admin menu and select **Exit** again to go back to the login screen.

13.12.3.2 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 is now under curfew and is due back by a set time that has been defined in the users' details, e.g., five o'clock.



3. To remove the item the user must click the **Yes** button. Selecting **No** or closing the door 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...



5. The system will now log you out and prompt you to close the door.

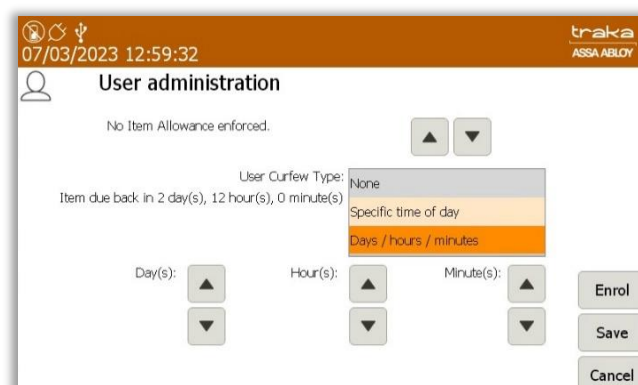
13.12.4 USERS WITH A 'NUMBER OF DAYS, HOURS AND MINUTES' CURFEW

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 then be able to set how many days, hours and minutes the item is allowed to be out of the system.

NOTE: When in affect 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

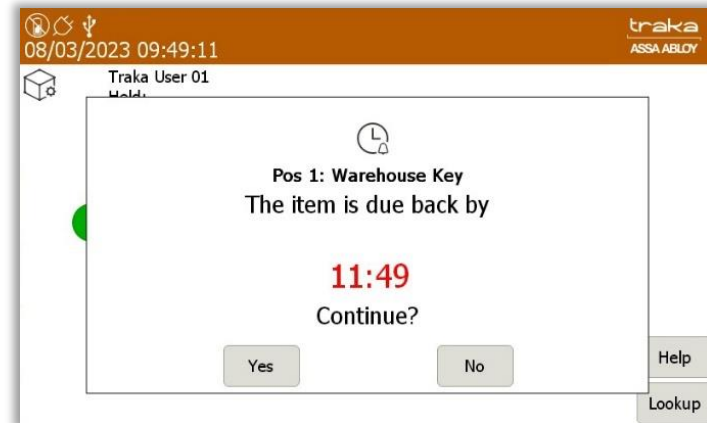
1. An administrator will need to access the system.
2. Select the **Admin** button.
3. Select the **Users** button.
4. Select a user from the list and click the **Edit** button.
5. From the bottom right-hand side of the screen select **Access**, **Options** and **Next** buttons to be taken to the curfew page.
6. From here select the Number of Days, Hours and Minutes curfew from the drop-down box, and set the days, hours and minutes using the directional arrow keys.



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

13.12.4.2 THE USER PROCESS

- The user will access the system.
- The user will then attempt to remove an item. 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 days, hours and minutes specified when setting up the item curfew. In this example, a curfew of 2 hours has been set.



- To remove the item the user must click the **Yes** button. Selecting **No** or closing the door will cancel the transaction and will require the user to log in again.
- After selecting **Yes**, the item will be released from the system. The onscreen icon will change from the 'green tick' to the following...



13.12.5 ALL CURFEWS

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



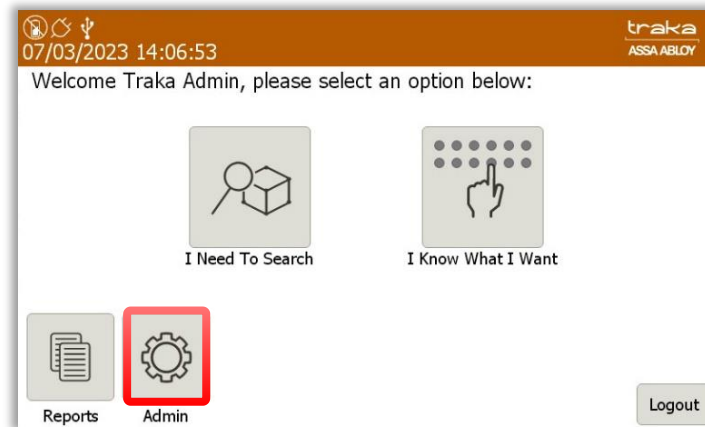
When you access the system and the icon below is shown, this indicates another user has removed the item from the system and that item is currently under a curfew.



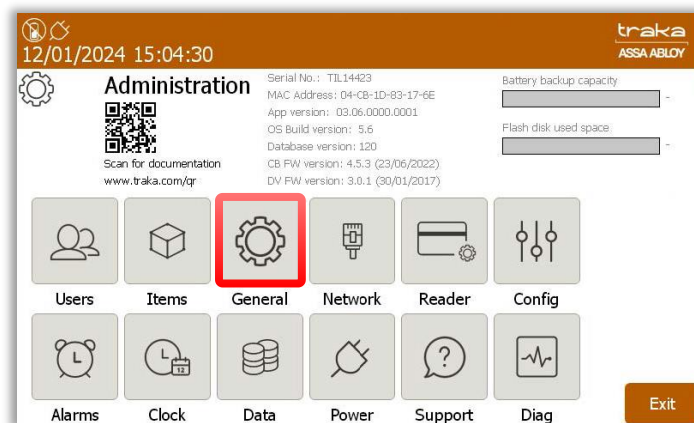
13.12.6 SUPRESS CURFEW ACKNOWLEDGEMENT

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

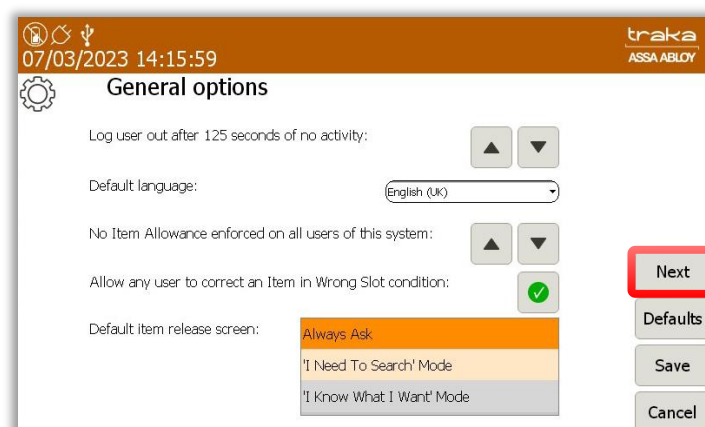
1. After logging on to the Traka Touch system with your ID PIN, swipe card or fingerprint, click on **Admin**.



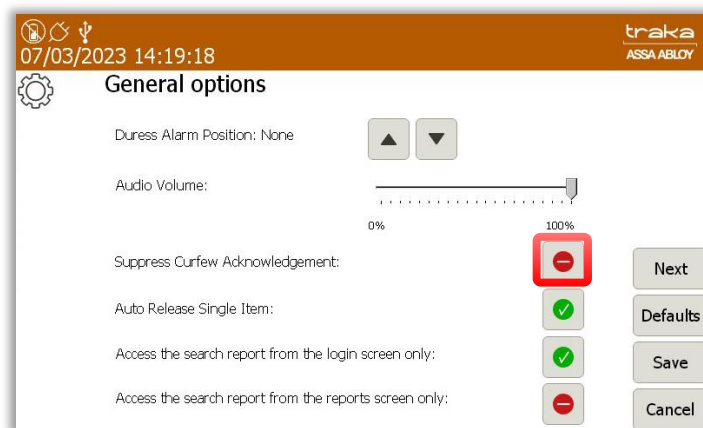
2. Next, click on **General**.



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.

13.13 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.

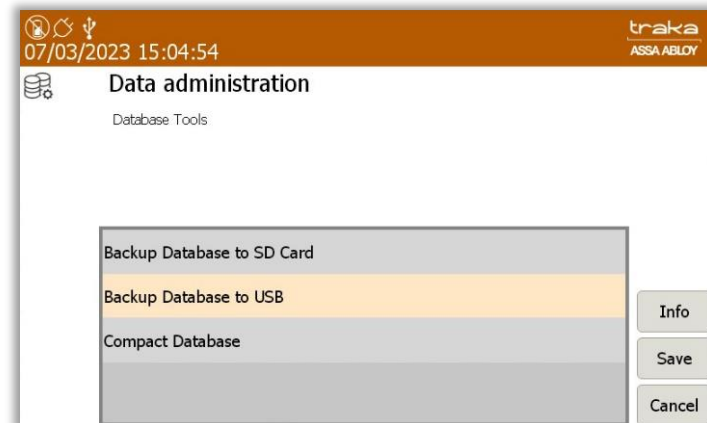
Delete events older than x days - This option can be enabled or disabled by clicking the small tick or cross button. The maximum number of days this can be set to is 1825.

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.



From here, you can do the following...

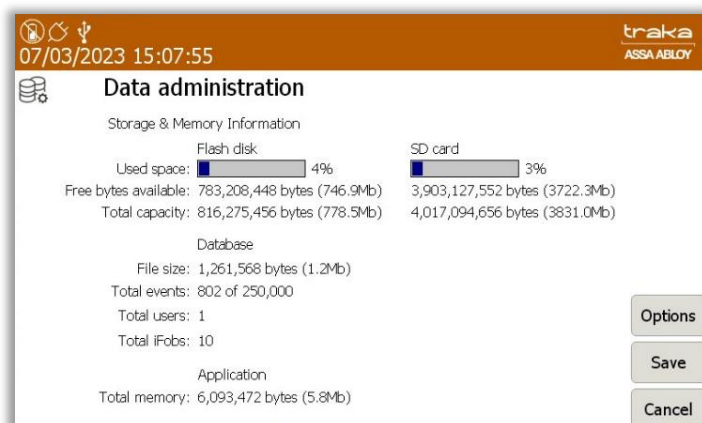
- Backup Database to SD Card
- Backup Database to USB
- Compact Database

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

NOTE: For further information on USB memory stick specification, refer to section [6.2](#).

Information page

The information page displays the memory usage of the flash disk and SD card. It also 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.

To return to the login screen, click **Save** and you will be taken to the admin menu. From there, click **Exit** to be taken back to the login screen.

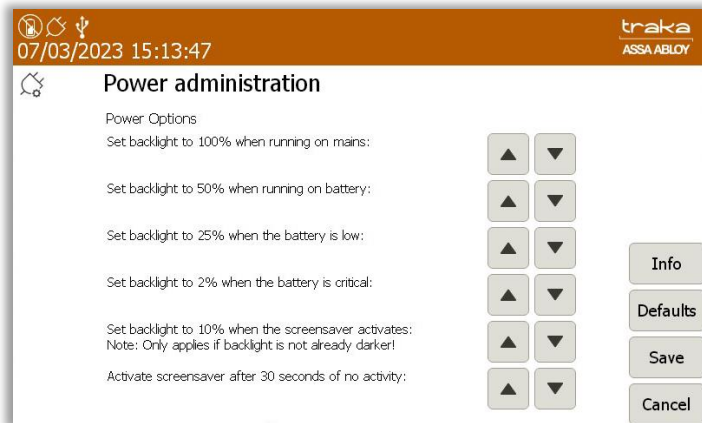
13.14 POWER SETTINGS

The Power Administration section allows you to change the touch screen brightness under certain conditions, such as when the

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.



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...

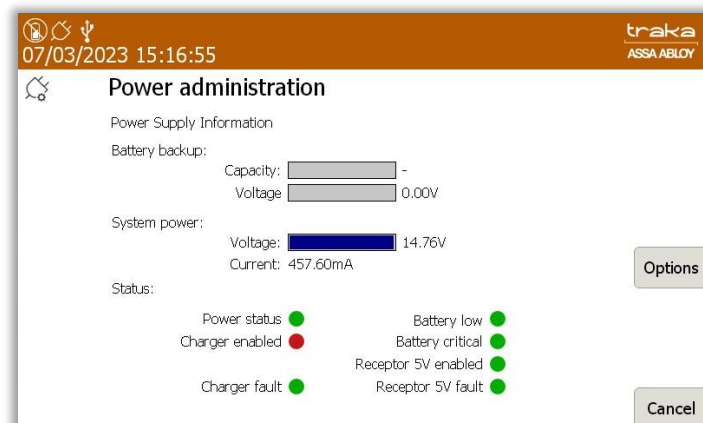
- Set backlight when running on mains
- Set backlight when running on battery
- Set backlight when the battery is low
- Set backlight when the battery is critical
- Set backlight when the screensaver activates

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.



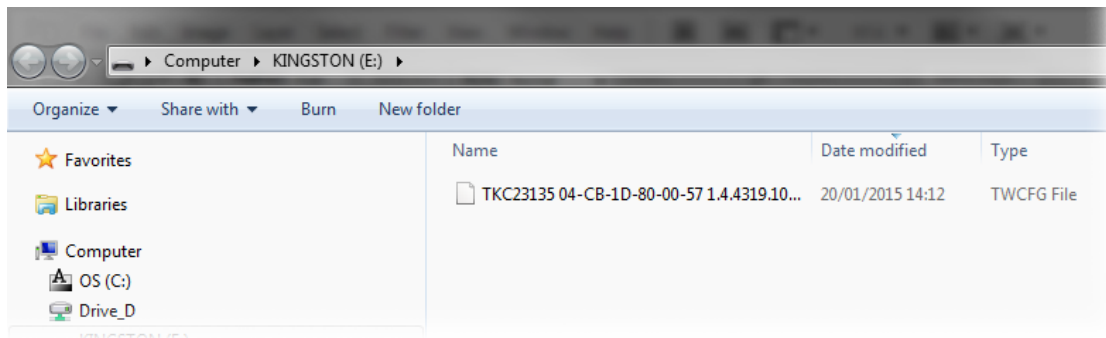
When you have completed your changes click **Exit** and you will be taken back to the admin menu. From there click **Exit** to be taken back to the login screen.

13.15 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 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.

NOTE: For further information on USB memory stick specification, refer to section [6.2](#).

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



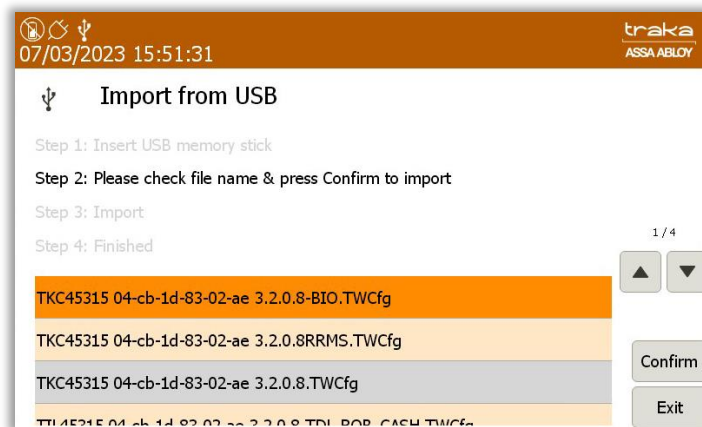
2. Access the system and click the **Admin** button followed by the **Config** button.



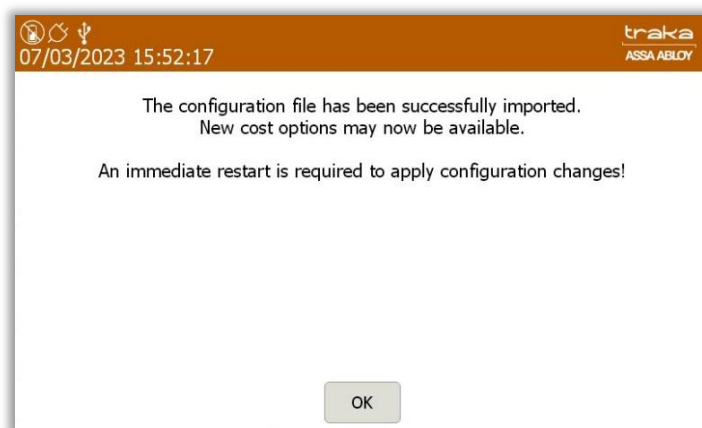
3. Click the **Import** button in the bottom right-hand corner of the Configuration screen.
4. The system will then open the door and prompt you to insert a USB memory stick.



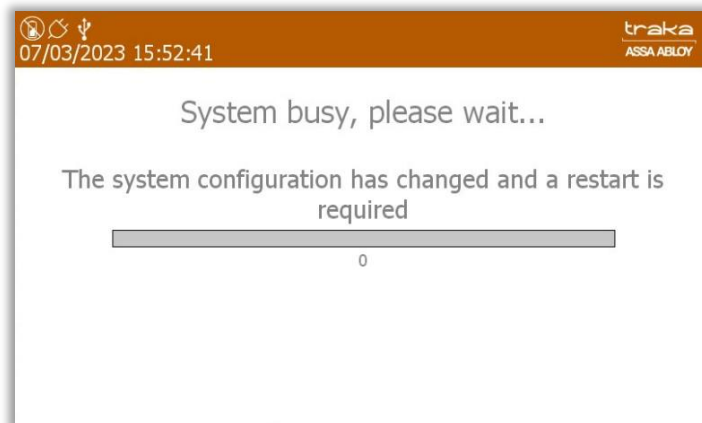
5. Check the file name and click **Confirm** to begin the import process.



6. 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.



7. The system will then restart; this may take a few minutes.



8. Once the system has rebooted you can use it as normal, with all the new features that came with the configuration.

13.16 HELP

13.16.1 VIEWING THE HELP SECTION

The Help section holds all 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.

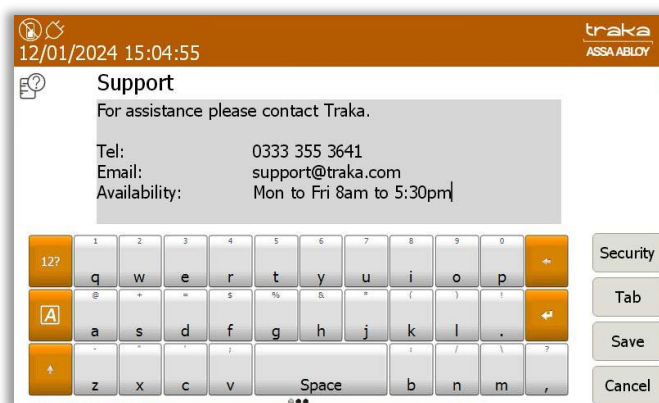


3. Click the **Exit** button to return to the login screen.

13.16.2 CHANGING THE HELP SECTION

To edit the information in the Help 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.



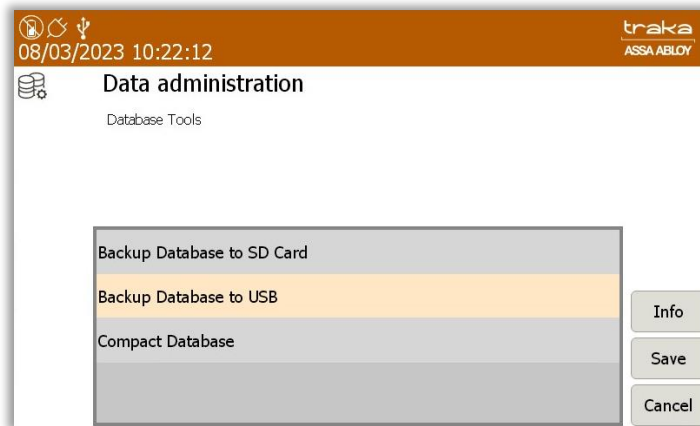
3. To edit the help information simply click on the desired field and use the onscreen keyboard to type the relative information.
4. When you have completed your changes click **Save** and you will be taken back to the admin menu. From there, click **Exit** to be taken back to the login screen.

13.17 BACKING UP THE TRAKA TOUCH DATABASE

The database holds all the information Traka needs to operate including the users, items, keys 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.

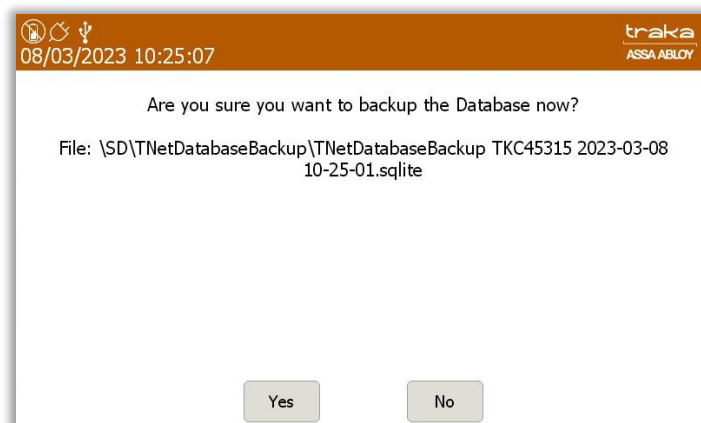
Backup Database to SD Card

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

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

Backup Database to SD Card

2. The system will then ask if you wish to back up the database. Click the **Yes** button.



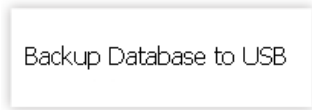
3. When the backup has successfully completed, click the **OK** button.

Backup Database to USB

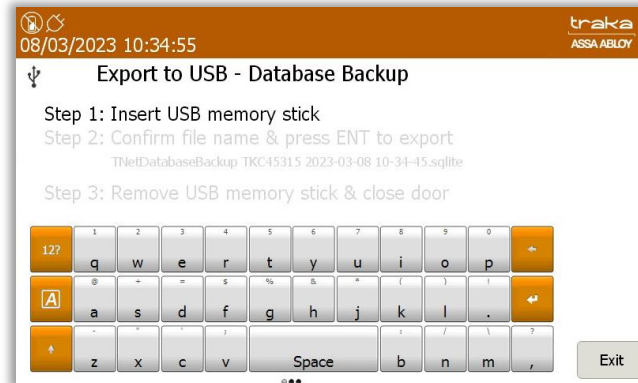
This option will fully backup your database to a USB memory stick.

NOTE: For further information on USB memory stick specification, refer to section [6.2](#).

1. Select the **Backup Database to USB** button.



2. The door will pop open and prompt you to insert a USB memory stick.



3. You can rename the database file if you wish by using the provided keyboard. Once finished, select the  (enter) button.



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



14. SAGEM MORPHOSMART READER

14.1 INTRODUCTION

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

14.2 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.

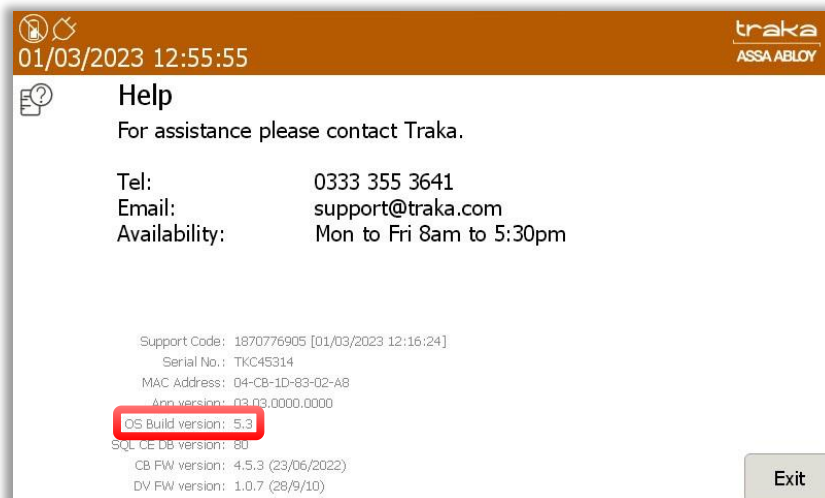
14.2.1 SAGEM READER MODELS

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

14.2.2 TRAKA TOUCH OPERATING SYSTEM

For the Sagem MorphoSmart Fingerprint Reader to work with Traka Touch, the Traka Touch unit must have Windows CE build version 1.9 or later installed. Navigate to the Help section to check the Build Version.



NOTE: If a Traka Touch Base Board or Process Module has to be swapped for any reason, replacements might not have version Windows CE 1.9 installed as default and so 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.

14.2.3 TRAKA TOUCH APPLICATION

For the Sagem MorphoSmart Fingerprint Reader to work with Traka Touch, the Traka Touch unit must have Traka Touch Application version 01.02.4256.41 (07-Sep-12) or later installed.

14.3 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 required for the reader to work – it is simply plug & play.

In addition, it is 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

By using keypad-only mode, any user may choose not to use their biometric (finger) data, 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 functionality is important because under GDPR, users must not be forced to use biometric data. It ensures that users who chose to use their biometric data for this purpose have a genuine alternative and are giving their consent freely.

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

14.4 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 is 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.

14.5 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

14.5.1 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.

The image shows two screenshots of the Traka User administration interface. Both screens display the following information: Forename: Traka, Surname: User 1, Display Name: Traka User 1, Keypad ID: 1111, PIN: (empty), Language: (English (UK)), and Enrolment ID: (empty). The left screenshot shows a keyboard at the bottom. The right screenshot shows the 'Access' button highlighted in a red box.

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

The image shows the Traka User administration interface on the enrol screen. It displays '1 Fingers enrolled' and 'Enrol 1 fingers'. A 'Clear' button is highlighted in a red box. Other buttons visible are 'Enrol', 'Details', 'Save', and 'Cancel'.

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 finger 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**.

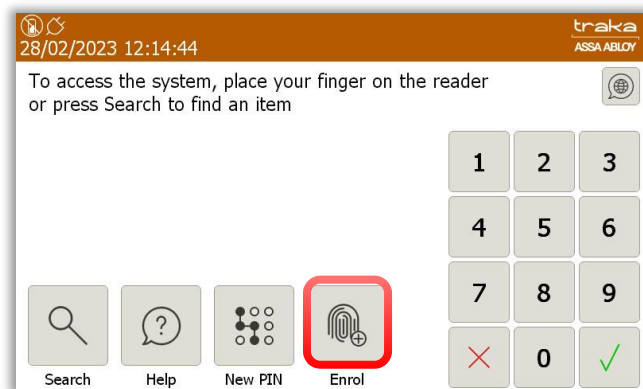
NOTE: The template will not be written to or cleared from the reader until Save is clicked.

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.

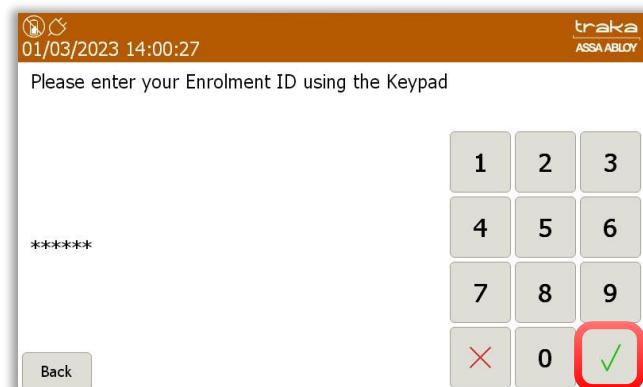
14.5.2 ENROLMENT ID

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 has to 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 field 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.



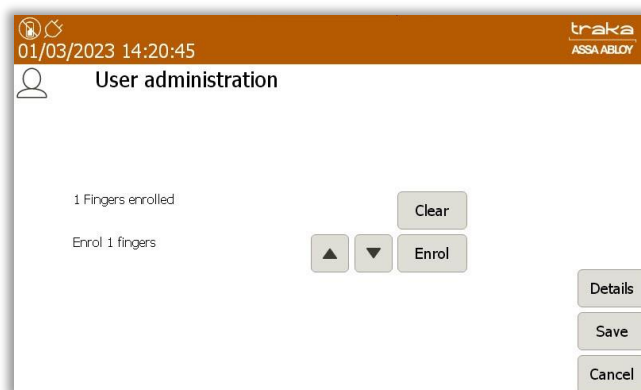
4. The user can now enter their assigned Enrolment ID and press  (enter).



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.

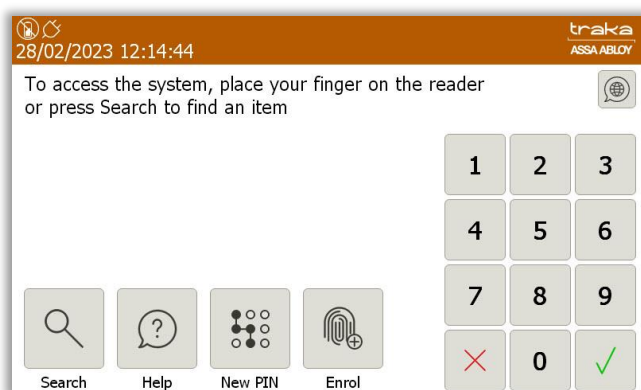


6. If the fingerprint captures are successful, you will be presented with the following screen. The User can now access the system by the method explained in the next section.



14.6 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.



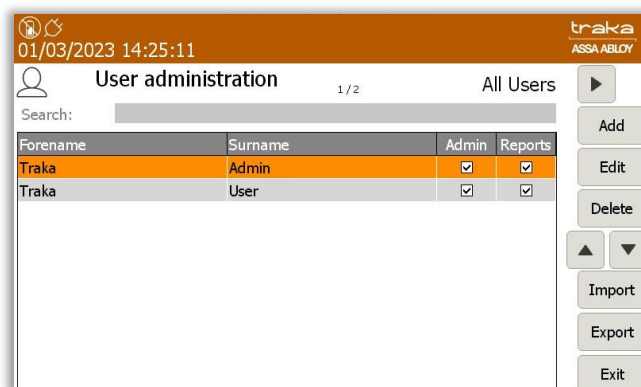
NOTE: When the main login screen is shown, the red light on the reader will NOT illuminate if no users have been enrolled in the database.

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.

14.7 REMOVING A FINGERPRINT TEMPLATE

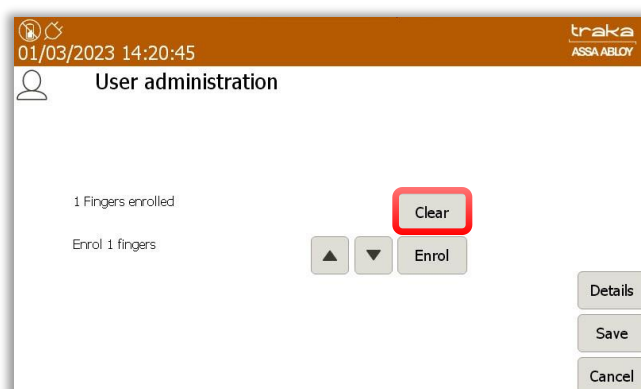
Under GDPR, the organisation must have procedures in place to enable users to withdraw their previous consent for their biometric (finger) data to be used for this process, and users must have been informed of how to initiate this process. Once consent has been withdrawn, the organisation must remove 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.

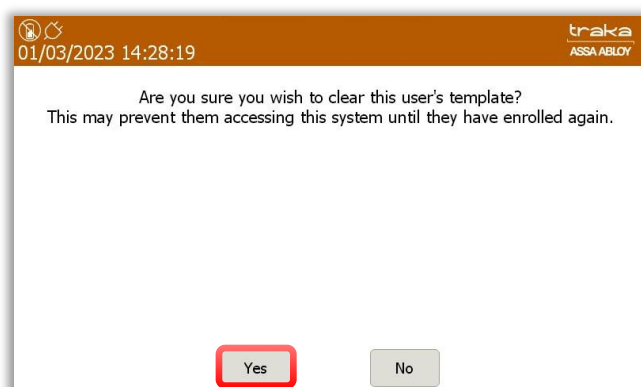
The User Administration page will now display an additional **Clear** button for an enrolled user.



3. Select the **Clear** button.

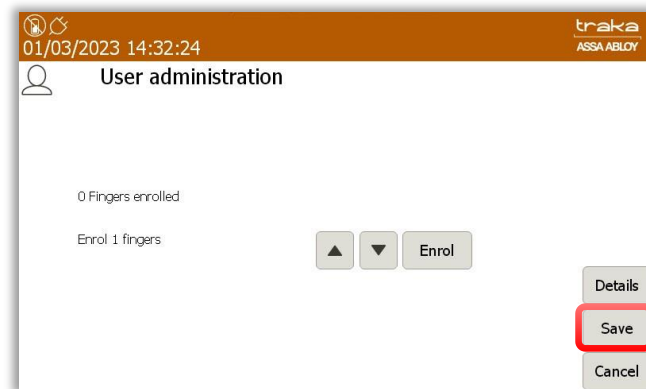
You will be presented with a message warning you that the user may no longer be able to access the system if their template is removed.

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.

- Once completed, select the **Save** button.



14.8 TIPS ON ENROLLING

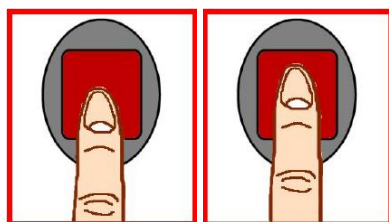
To get the best quality image, one needs to:

- 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!

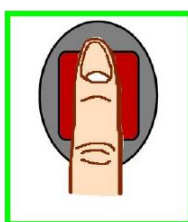
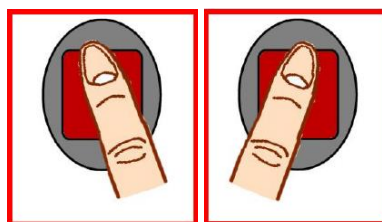
VERY USEFUL TIP: If you are having issues, brush the fingertip along the side of your nose – this adds a fine layer of natural grease to your finger and will get you a much better read!

How to position your finger correctly on the sensor:

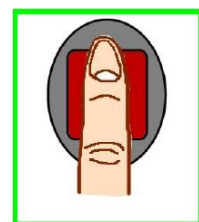
Finger Height



Finger Angle

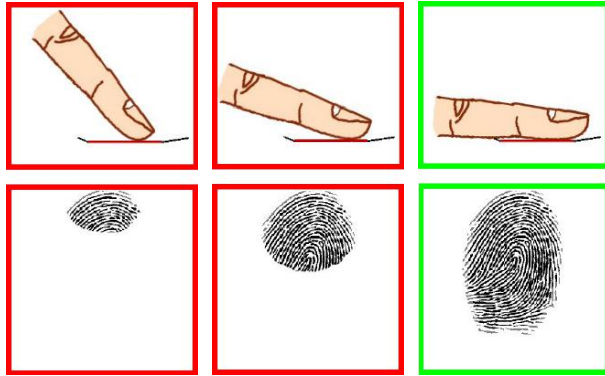


Ideal Position



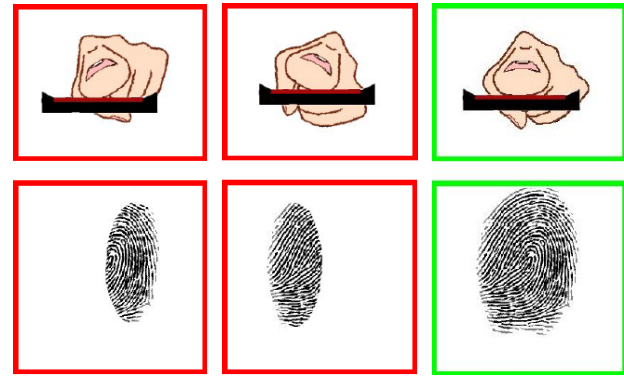
Ideal Position

Finger Inclination



Ideal Position

Finger Rotation



Ideal Position

14.9 FAR

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

If the application continuously displays a 'Press harder' message without a finger placed on the reader, it is likely that the glass requires cleaning, or if the reader is exposed to a bright light source. This is not usually an issue unless it is being used in direct sunlight, or is beneath a light source highlighting dust particles on its glass surface. Should any of the above issues arise; a firm wipe down the glass with a finger will usually solve the problem.

15. 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.

15.1 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.

15.2 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.

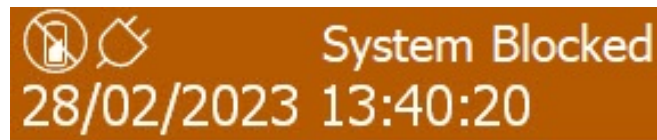
'System in lockdown mode' is displayed in the default system language and also cycles in all other supported languages. This will continue to stay onscreen as long as the system is in lockdown.

System in lockdown mode

システムが現在ブロックされている -
ブロックが解除されたときに再試行してくた



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 as long as 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.



15.2.1 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.

Event Report: 01/03/2023 - 06/03/2023					Filter
When	Event	Who	No.	Item	
06/03/2023 14:39:43	Report Access	Traka Admin			◀
06/03/2023 14:39:41	System Block Mode End	Traka Admin			▲
06/03/2023 14:39:25	System Block Mode	Traka Admin			▼
06/03/2023 14:39:23	User Logged In	Traka Admin			▶
06/03/2023 14:29:55	User Logged Out	Traka User			Export
06/03/2023 14:29:54	Door Closed	Traka User	1		Back
06/03/2023 14:29:51	Door Left Open	Traka User	1		
06/03/2023 14:28:10	Door Opened	Traka User	1		
06/03/2023 14:28:03	User Logged In	Traka User			
06/03/2023 14:28:01	User Logged Out	Traka Admin			
06/03/2023 14:27:32	Admin Access	Traka Admin			
06/03/2023 14:27:30	User Logged In	Traka Admin			

16. RRSS (RANDOM RETURN TO SINGLE SYSTEM)

16.1 SYSTEM REQUIREMENTS

This feature can operate on a standalone Traka Touch system or can be used in conjunction with TrakaWEB. The minimum Traka Touch Application version required is V1.6.0. If used in conjunction with TrakaWEB, the minimum TrakaWEB version required is V2.3.0.

16.2 RRSS OVERVIEW

RRSS (Random Return to Single System) allows any iFob belonging to a system to be returned to any position within that system. It will also support more iFobs than receptor sockets (up to a maximum of 720 iFobs in total). To do this, each iFob is assigned a Unique Index number which stays with the iFob for life.

The RRSS feature works with both Locking and Non-Locking receptor strips, and with systems with and without doors.

You cannot take an item and return it to a different system (that's Random Return to Multiple Systems).

NOTE: To use the RRSS feature you must first have it enabled in the configuration file.

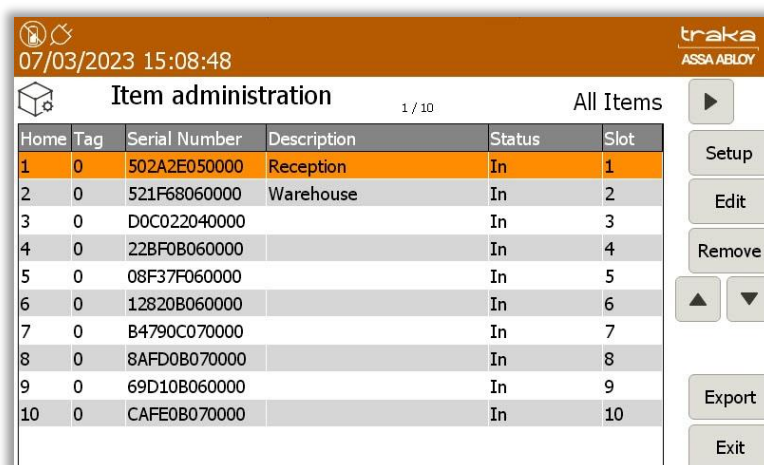
USEFUL TIP: Use the 'I Need To Search' option when removing iFobs for ease of locating required items.

16.3 ITEM SETUP

This setup process can only be performed by an Admin user.

1. Access the system and click **Admin**.
2. Click **Items**.
3. Click **Setup**. The system will ask if you want to deallocate all iFobs that are NOT in the system.
 - a. If you select **YES**, any iFobs not currently in the system will be deallocated. Their Index number will not be reused in case a user has been granted access to that. You will also be unable to have more iFobs than number of positions in the system.
 - b. If you select **NO**, it will allocate any new iFobs it finds in the system. This allows you to have more iFobs allocated to the system than the number of positions in the system.

Once you have made your selection the system will display a list of all allocated items.



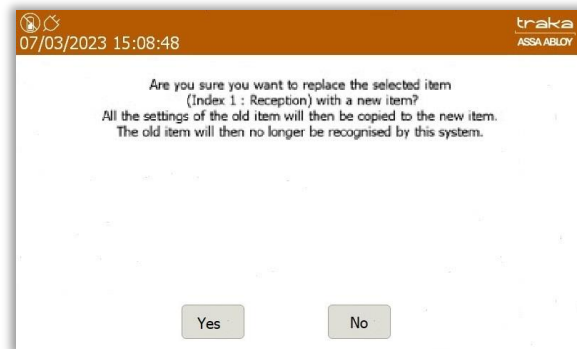
Home	Tag	Serial Number	Description	Status	Slot
1	0	502A2E050000	Reception	In	1
2	0	521F68060000	Warehouse	In	2
3	0	D0C022040000		In	3
4	0	22BF0B060000		In	4
5	0	08F37F060000		In	5
6	0	12820B060000		In	6
7	0	B4790C070000		In	7
8	0	8AFD0B070000		In	8
9	0	69D10B060000		In	9
10	0	CAFE0B070000		In	10

16.4 ITEM REPLACEMENT

From time to time, you may be required to replace an iFob that has become lost or damaged. During the replacement process, any settings including the Index number and Description will be copied across to the new item.

The Item Replacement process can only be performed by an Admin User.

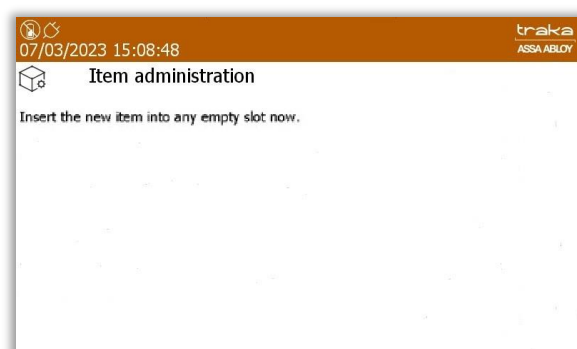
1. Access the system and click **Admin**.
2. Click **Items**.
3. Select the item you wish to replace and click **Replace**. The system will then ask you to confirm.



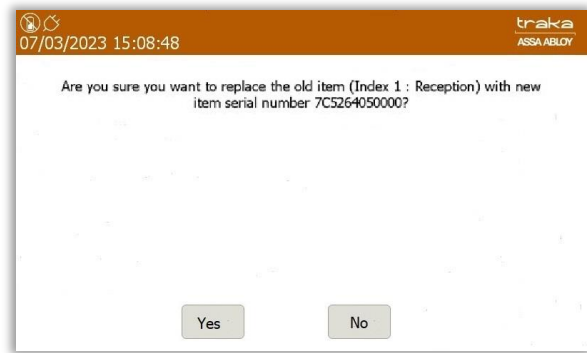
4. Click **Yes**. The system door will open and ask you to remove the item (if the item is in the system). Once you have removed the item, transfer any keys or items from the old iFob to the new iFob.



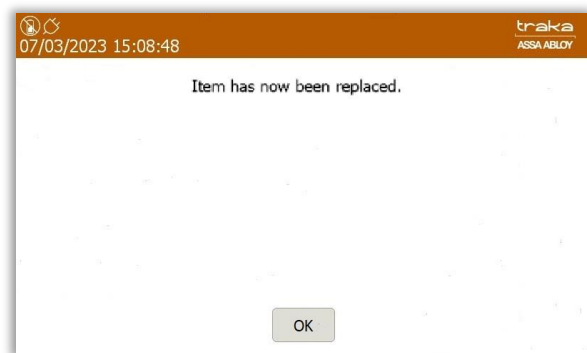
5. The system will now ask you to insert the new item. This cannot be an item that is already allocated to this system.



6. Insert the new iFob. The system will ask you to confirm that you want to continue.



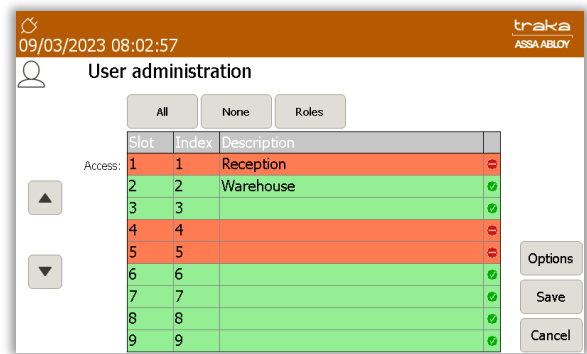
7. Select **Yes**. The system will confirm that the item has been replaced, and an 'Item Replaced' event will be generated.



16.5 GRANTING ACCESS TO ITEMS

The process for granting access to items can only be performed by an admin user.

1. Access the system and click **Admin**.
2. Click **Users**.
3. Select the required User and click **Edit** and then **Access**. A list of all items will be displayed.

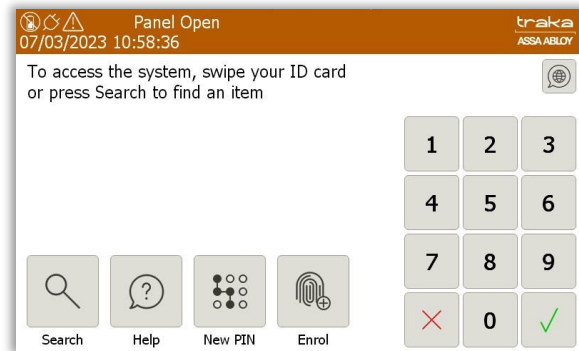


4. Select the items you wish the user to have access to. All items the user has access to will be highlighted in green with a tick. Once finished click **Save**.

17. TAMPER SWITCHES

There are up to 3 tamper switches fitted to Traka Touch Systems 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. Currently only the S-Touch system supports all 3 tamper switches.

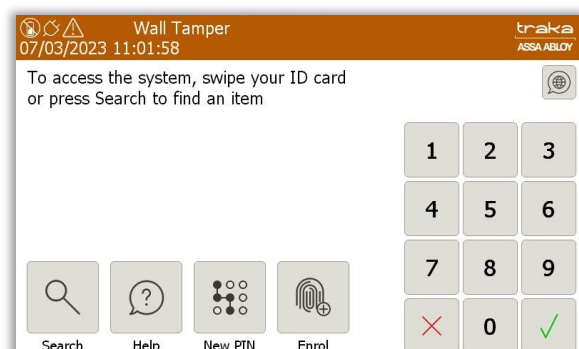
- **Tamper Switch 1** – fitted to the rear of the Control Panel and is activated when the Control Panel is opened. This will return a 'Panel Opened' event and a 'Panel Closed' event once the Control Panel has been closed.



- **Tamper Switch 2** – fitted behind the Receptor Strip Frame on an S-Series and is activated when the Receptor Panel is opened. This will return a 'Receptor Panel Open' event and a 'Receptor Panel Closed' event once the Receptor Panel has been closed.



- **Tamper Switch 3** – fitted to the rear of the cabinet and is activated when the system is removed from the wall. This will return a 'Wall Tamper' event and a 'Wall Tamper End' event when the system is back against the wall.



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 in order to assist you with all aspects of the Feature Options available for TrakaWEB and how to use them in conjunction with your Traka Touch Key Cabinet or Locker system.

NOTE: Except for Location Logging, all other Feature Options are not available on Systems using RRMS.

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 & UD0260 – TrakaWEB Version 4 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.

18.8 FUEL, DISTANCE & LOCATION LOGGING

Fuel, Distance & Location Logging are individual cost options which can be used to assist fleet managers with day-to-day management of their vehicles. Each feature can be used independently or in combination. They can be purchased individually and also be turned on or off as required.

Users with access to the system will be granted a key to a vehicle, then after returning the key to the system, they will be requested to enter information regarding the fuel usage, the distance travelled, or time duration of journey, and the vehicle's current location. The next user to remove that key will be shown information as to the current location of the vehicle.

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.

18.9 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.

18.10 RANDOM RETURN TO MULTIPLE SYSTEMS (RRMS)

Random Return to Multiple Systems (RRMS) is a cost option feature that allows Items to be taken from one key control system to another that are connected to the same TrakaWEB instance.

RRMS is available for Traka Touch key cabinets being managed with TrakaWEB Professional Plus. If enabled for a cabinet, RRMS applies to the entire cabinet. Access rights will be based on categories of fobs ("Access Groups") rather than individual fobs. RRMS cannot be used with any other optional Traka Touch or TrakaWEB functionality, or with the User Import Spreadsheet feature. Searches, Status enquiries and some Reports work very differently on systems with RRMS.

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

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 ACCESS SCHEDULES

Access Schedules is a cost option that is used within TrakaWEB to impose time restrictions on iFobs/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 iFobs/items when the schedule is active. Outside of this time, they will have access to no iFobs/items at all.
- The access restrictions will not prevent a user from returning an item, only taking it.
- Locking receptor strips on key cabinets and locker doors will physically restrict access to items however, non-Locking receptor strips are unable to enforce this.
- If an Item is physically removed outside of the allowed access schedule (e.g., on a non-locking system) then an 'Item Removed outside Schedule' event will be recorded.
- A schedule restriction can be overridden on an Item (not a user) by a special role called 'Item Access Schedule Override'.
- Software permissions will control who can administer the access schedules.

NOTE: A best practice would be to keep users and item/iFobs in separate Access Schedules to avoid potential confusion.

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**.

18.13 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.

18.14 TEMPORARY KEY STORE (TKS)

Temporary Key Store is a cost option feature that will allow a user to temporarily deposit their keys into a different cabinet to that which the keys were removed from.

The Temporary Key Store cabinet maybe used in a situation where taking keys is against compliance such as outside of work premises or areas considered to be of high-risk. In conditions such as these, the keys maybe placed in the Temporary Key Store cabinet to keep track of their location and retrieved later as required.

An override option can be assigned to a user in TrakaWEB, which will enable them to remove iFobs from the Temporary Key Store regardless of them being granted access. This will generate a 'Temporary Key Store Override' event which will appear in the activity report. However, Real Time Activity will not show any 'Temporary Key Store Override' events unless activated from Activity Types in the Software Settings menu. An 'Activity Trigger' can also be set within TrakaWEB to generate an Email Notification.

Due to the nature of the Temporary Key Store functionality, there is no Search option available on Traka Touch.

For a full overview of Temporary Key Store, please refer to **UD0018 – TrakaWEB User Guide & UD0260 – TrakaWEB Version 4 User Guide.**

18.15 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.**

18.16 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.**

18.17 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. GENERAL MAINTENANCE

19.1 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.

19.1.1 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.

19.1.2 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.

19.1.3 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.

19.1.4 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.

19.2 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 Mk3 Control Board located on the back of the Control Panel.

1. To power **Off** the system press and hold the button highlighted below for 2 seconds, until all the LED's on the Traka Control Board go out.

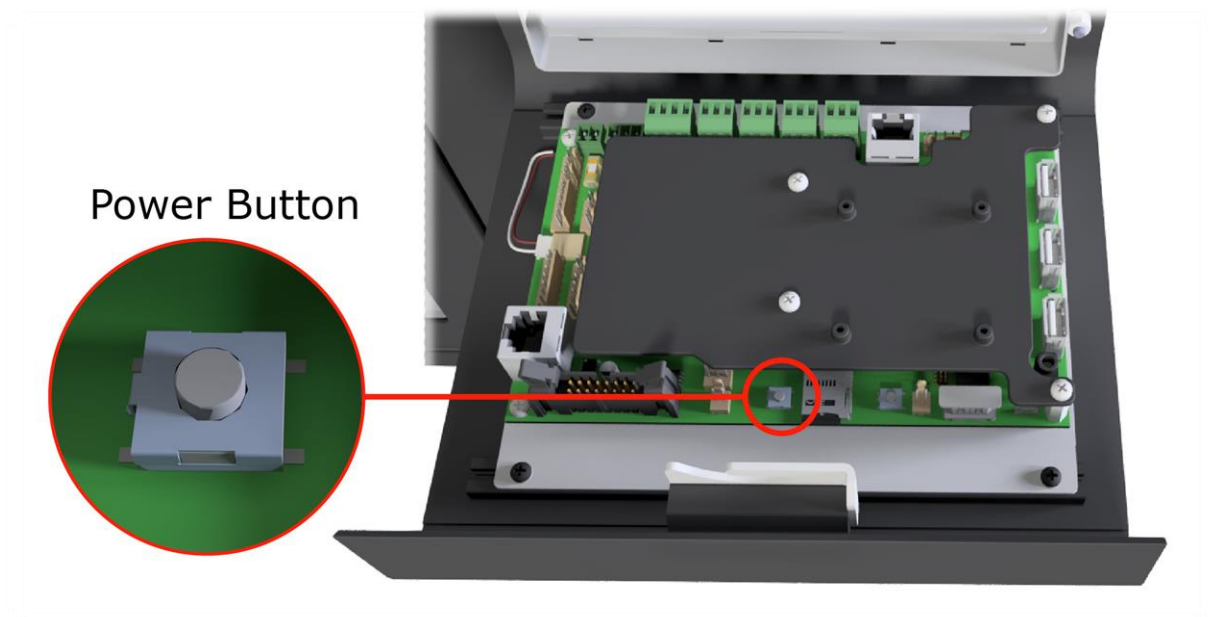


Figure 11 – Power button in a Traka Touch Pro Key Cabinet

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

19.3 MANUALLY OPENING THE DOOR FOR EMERGENCY ACCESS

19.3.1 TRAKA TOUCH PRO V

1. Located on the top of the cabinet is an override cam lock. Insert your Master override key into the cam lock and turn until the lock fires and the door opens.



Figure 12 – Opening Control Panel on Touch Pro V

19.3.2 TRAKA TOUCH PRO M, S & L

1. Located on the top of the cabinet is an override cam lock. Insert your Master override key into the cam lock and turn until the lock fires and the door opens.

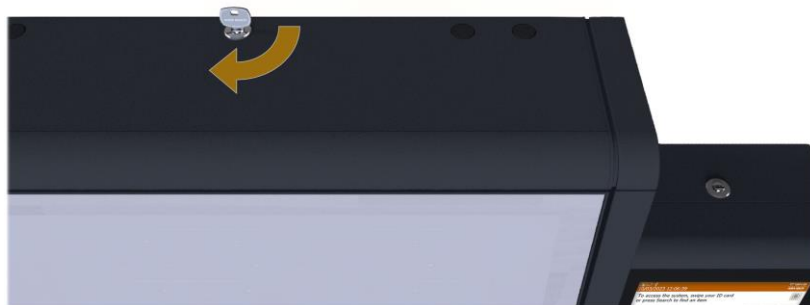


Figure 13 – Opening Cabinet Door on Touch Pro M, S & L

2. The door will now release allowing access to the receptor strip frame.

19.3.3 OPENING THE RECEPTOR STRIP FRAME(S)

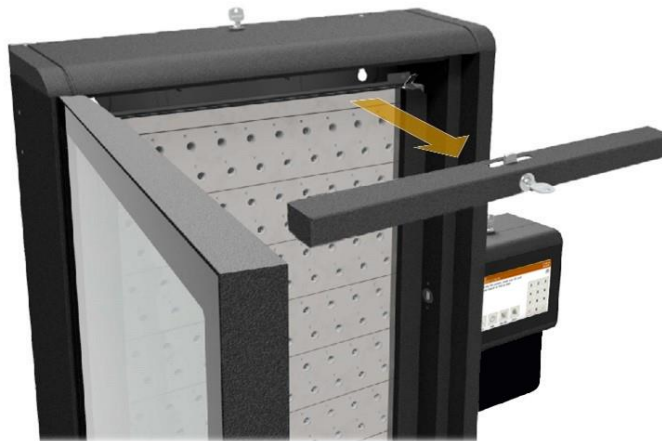
To enable the cabinet to be fitted to the wall you must first remove the Receptor Strip Frame. If your system has extension cabinets, the Receptor Strip Frame(s) in the extension(s) must also be removed.

NOTE: For the Touch Pro M & S there is only one single receptor strip frame present. However, the Touch Pro L will have three. With the Touch Pro L, the receptor frames must be opened in the order from top to bottom. This is to prevent overhanging keys from being trapped on the frame closure.

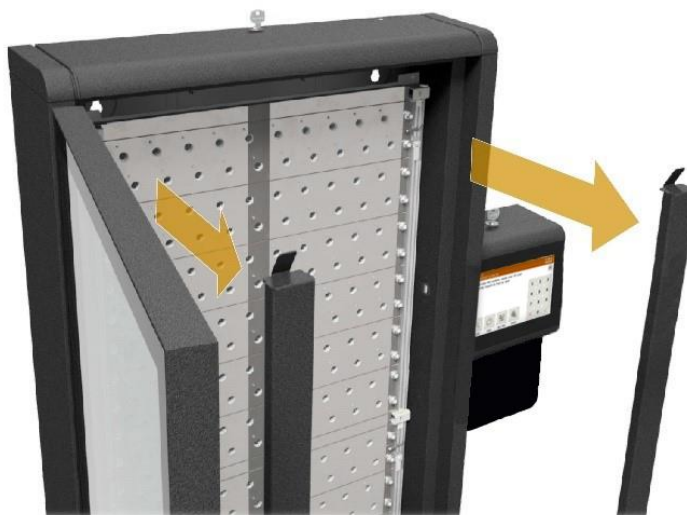
1. Place the Master Key in the lock in the top bracket and turn it clockwise to unlock.



2. Remove the top bracket with the Master Key thereby unlocking two side channel panels.



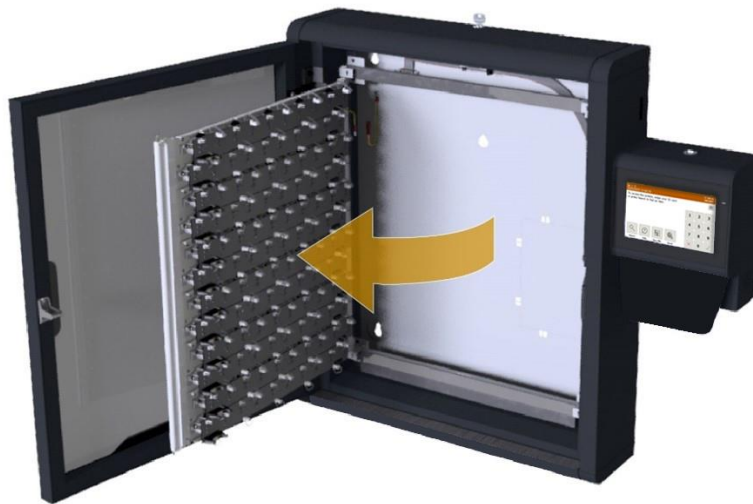
3. Remove the two side channel panels by lifting them off their locating pins and pulling them outwards.



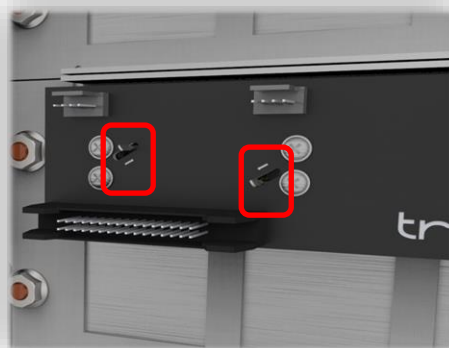
4. Next unlock the two hinge pins (top and bottom) on the right side of the receptor frame.



5. The receptor strip frame will now swing open using the two left side hinge pins. With the Touch Pro L, the receptor frames must be opened in the order from top to bottom. This is to prevent overhanging keys from being trapped on the frame closure.



6. Access to the back of the Receptor strip frame is now possible and manual emergency key release can be performed by sliding the release lever appropriate for the key that is required.



7. Once you have performed the manual emergency release, close the receptor strip frame, and ensure the hinge pins are fully engaged into the frame.

19.4 REPLACING IFOBS

From time to time, you will 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.

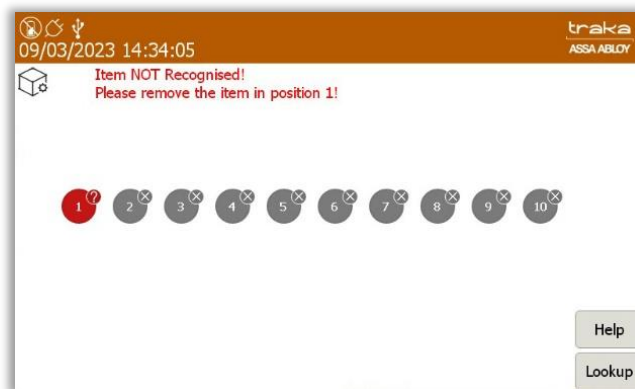
The Traka Touch System works on fixed item replacement basis which means iFobs must be returned to the positions from where they were taken. By default, the system will not know where an iFob should go therefore the iFob serial number must be associated with the position in the system.

NOTE: If your system is a random return system a different process must be followed for replacing iFobs. Please refer to the RRSS section.

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

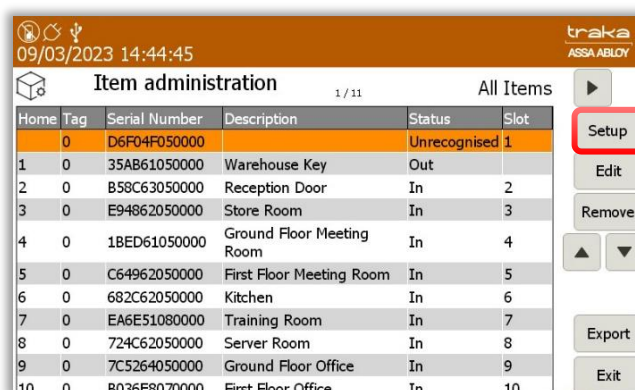
NOTE: The user must be an administrator and have access to all the iFobs in the system.

2. Select the **I Know What I Want** 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.

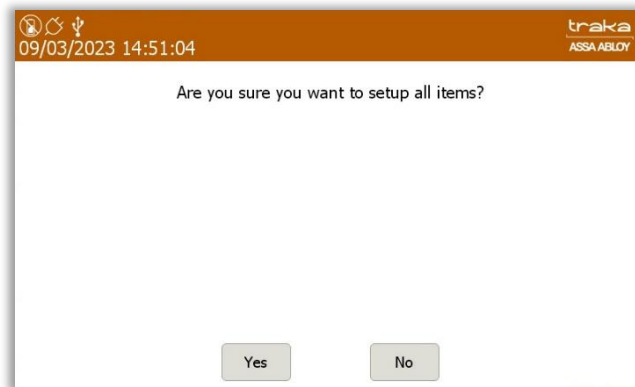


NOTE: If you have multiple items that need to be replaced then repeat steps 1 to 4 for each of them before moving on to step 5.

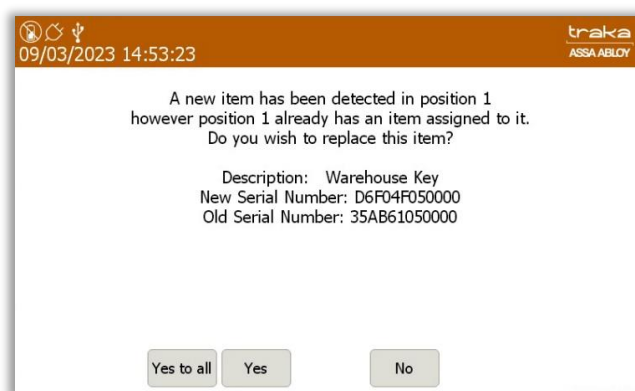
5. Identify yourself once again at the Traka System by entering your Keypad ID or swiping your Card.
6. Select the **Admin** button.
7. You will then be taken to the Administration screen. Click the **Items** button.
8. The item list will then display the new items status as 'unrecognised'. Select the **Setup** button.



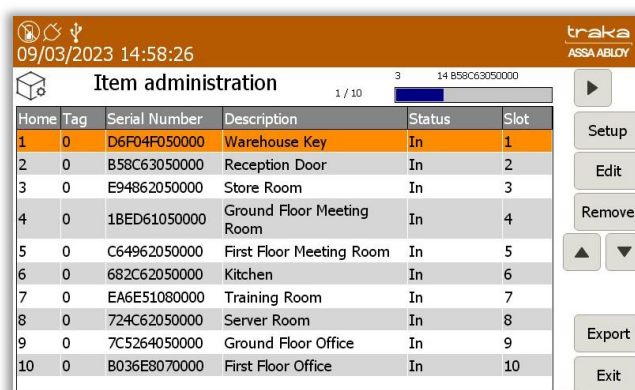
9. You will be asked if you wish to setup all items, click the **Yes** button.



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 **'I Know What I Want'** button if applicable.

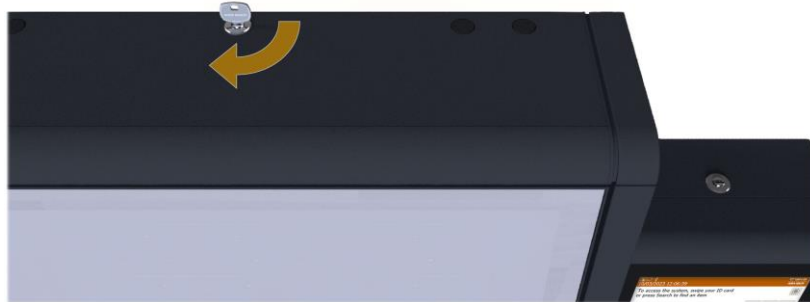
The LCD will now show you all the items in the cabinet. Ensure the item you replaced now has the 'item in System' symbol  and can be removed.

19.5 ACCESSING THE SYSTEM

1. If the Touch Pro system is operational, access the system using keypad, fingerprint or Swipe card.

NOTE: If the door requires manual access, a master key will be required to open it.

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



OR

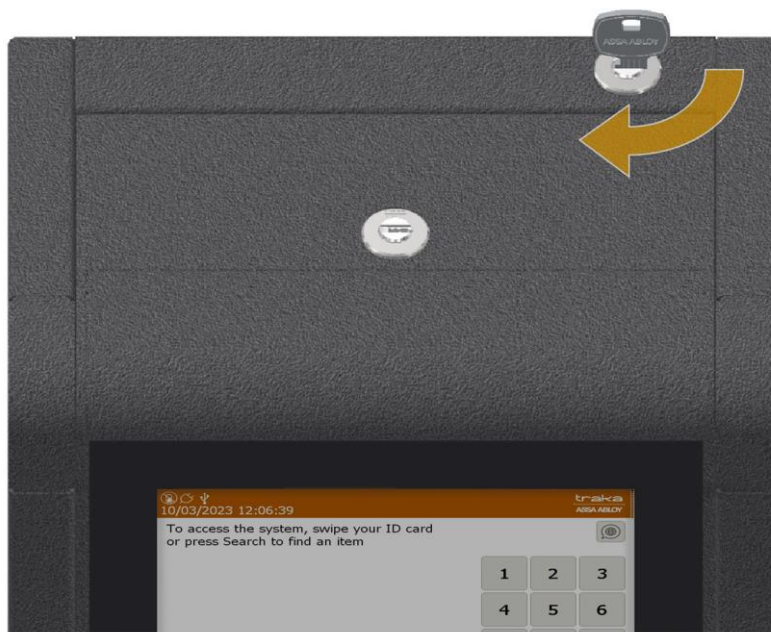


Figure 14 – Opening Cabinet Door

19.6 SERIAL NUMBER/RATING PLATE LOCATION

19.6.1 TRAKA TOUCH PRO V

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



Figure 15 – Location of the Rating Plate on Touch Pro V

19.6.2 TRAKA TOUCH PRO M, S & L

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

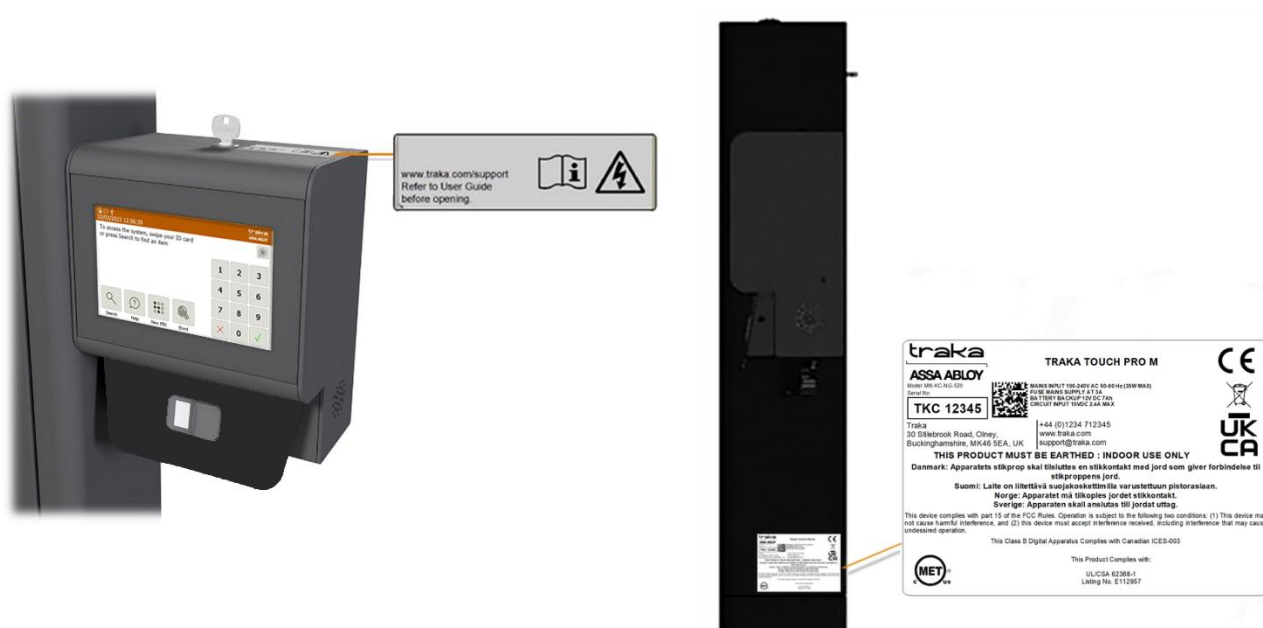


Figure 16 – Location of the Rating Plate on Touch Pro M, S & L

Please note, that the following graphical symbols, that are found on or inside the Touch Pro 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.

19.7 BATTERY CONNECTION/DISCONNECTION

Traka provide a backup battery already connected with every Touch System in the UK. If for any reason you need to connect/disconnect the battery, please see the battery location and connection details below.

WARNING: All Traka Systems have two power sources, Mains and Battery. Before installing or servicing a Traka System, please ensure both Mains and Battery power sources are disconnected.

19.7.1 TRAKA TOUCH PRO V BATTERY LOCATION

1. Manually open the cabinet door by inserting the Master Key into the override door release lock on top of the unit.



Figure 17 – Opening the Control Pod

2. Manually open the Control pod by inserting the Master Key into the second override release lock on top of the cabinet, making sure that you support the pod.



Figure 18 – Pulling down the Control Panel to reveal the battery

3. The battery is located behind the panel, secured in place with a bracket.

19.7.2 TRAKA TOUCH PRO M, S & L BATTERY LOCATION

1. Insert your Master override key into the cam lock and turn until the lock fires and the door opens.
2. Make sure that you support the Control Panel to stop it falling.



Figure 19 – Opening the Control Pod

3. Open the Control Pod by pulling down the front fascia.



Figure 20 – Pulling down the Control Panel to reveal the battery

4. You will see the battery inside the Control Pod. You will need a 3mm nut Allen key to remove the two screws securing the battery bracket to get to the battery.



Figure 21 - Location of fixing screws on the battery bracket

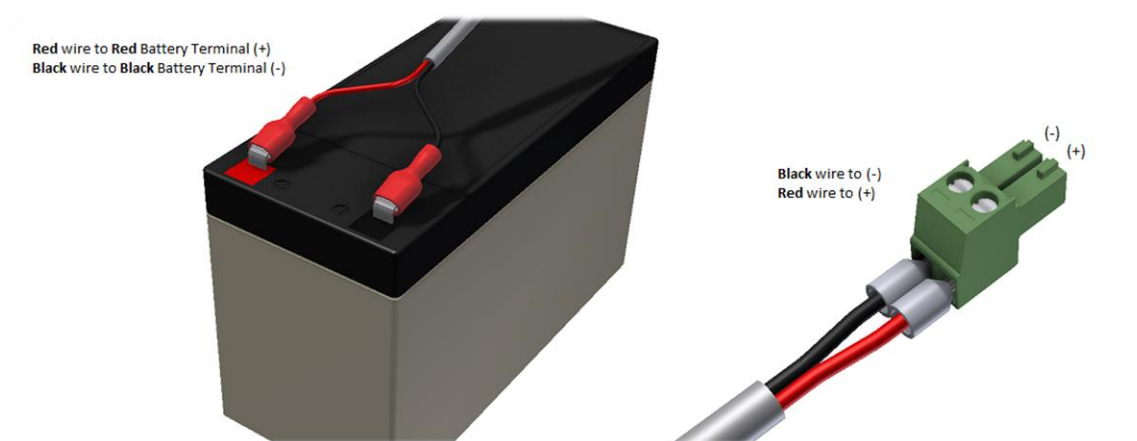
19.7.3 BATTERY CONNECTION DETAILS

The following diagram shows the connection details for the Traka Touch Pro Backup Battery. For details on where to connect the battery to the Traka Mk3 Control Board refer to the 'Traka Touch PCB' section.

NOTE: Depending on your system type the battery may differ slightly from the image below. However, the connection details remain the same.

For Battery disconnection, carefully disconnect the spade connectors from the battery.

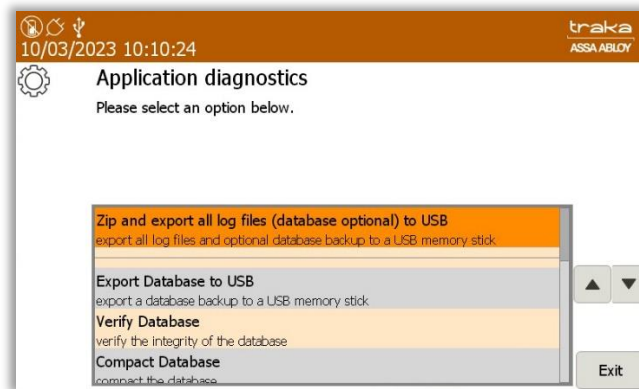
WARNING: Never disconnect the wires from the green connector whilst the cable is still connected to the battery terminals.



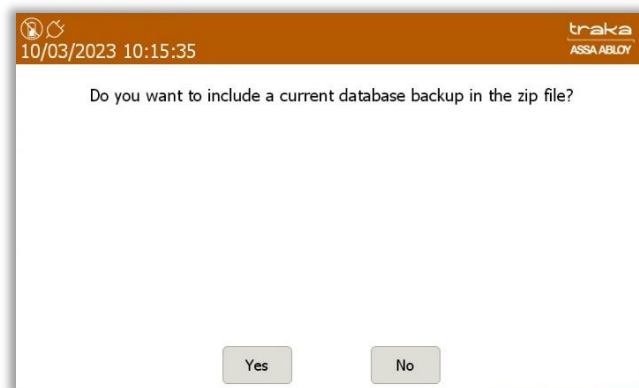
NOTE: Ensure that the spade connectors are pushed fully onto the battery terminals. It is recommended that insulation tape is wrapped around the battery to fully cover any exposed parts of the battery terminals.

19.8 ZIP AND EXPORT ALL LOG FILES AND SQL CE DATABASE TO USB

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.



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.



20. PRODUCT DISCONNECTION

20.1 MAINS DISCONNECTION

In the event of an emergency, completely disconnect the system from the mains following the steps below:

- If the product is connected to a non-switched fused spur, remove the fuse from the spur.
- If the product is wired to a plug and connected to a power outlet, disconnect the plug from the power outlet.
- In the case of a battery being fitted there are two power sources to disconnect before any service or maintenance work is carried out.

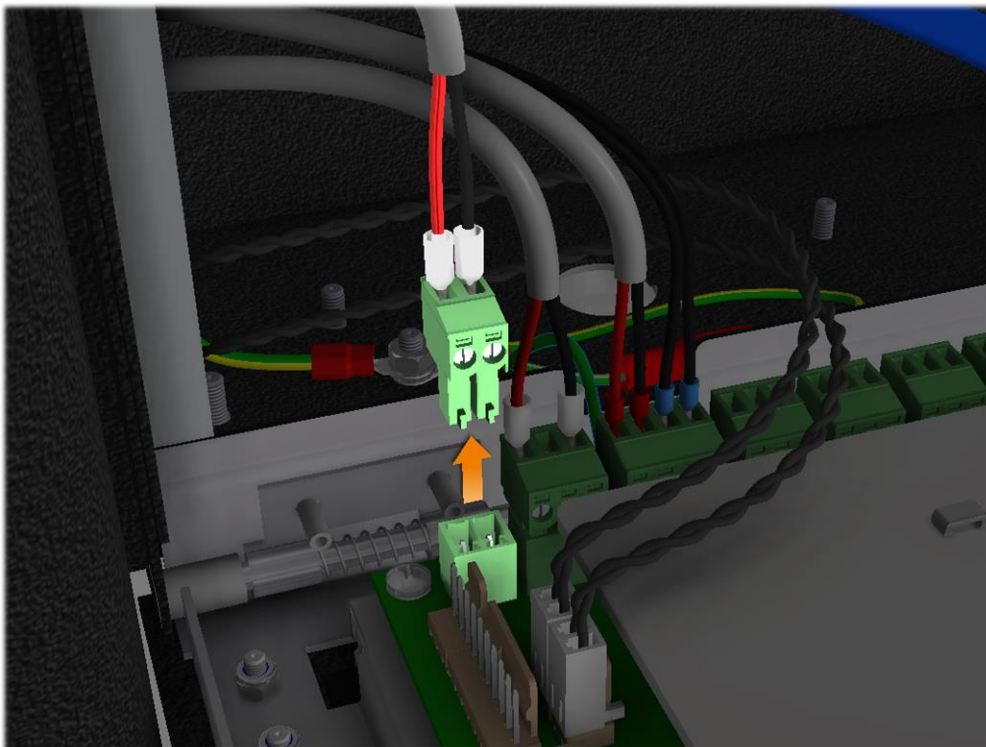
NOTE: To safely power down and prevent the risk of data loss the system must be switched off as described in the '[Powering On/Off the System](#)' section. Only disconnect directly from the mains in an emergency.

20.2 BATTERY DISCONNECTION

The battery is connected to the Traka Touch PCB located on the back of the control panel.

For Battery disconnection, carefully disconnect the connector from the Traka Touch PCB.

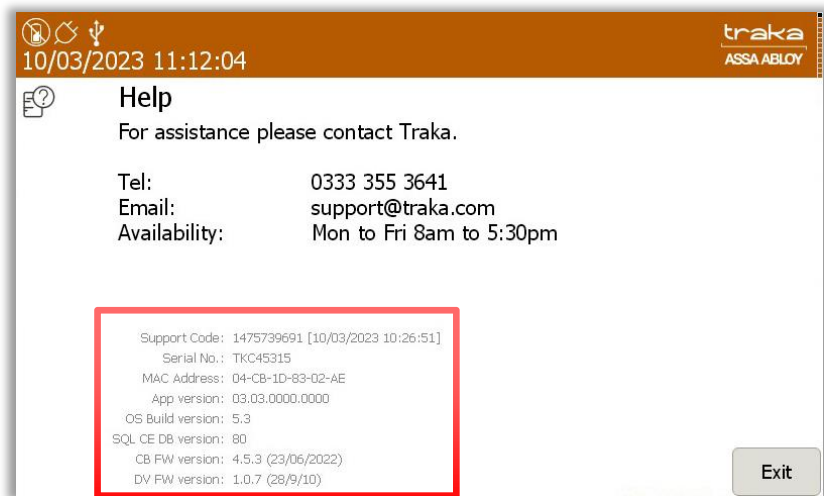
WARNING: Never disconnect the wires from the green connector whilst the cable is still connected to the battery terminals.



21. 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.

22. END USER LICENCE AGREEMENT – EMBEDDED SOFTWARE

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

1. Definitions

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

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

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

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

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

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

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

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

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

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

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

2. Licence

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

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

3. Patents, Designs and Copyright

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

4. Restrictions
- 4.1 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to disclose the contents or code of the Embedded Software to any third party. The Customer may take such copies of the Embedded Software as is necessary for the purpose of back-up security and agrees that all copies shall be kept confidential and subject to the terms of this EULA.
- 4.2 Except as expressly set out in this EULA or as permitted by law, the Customer agrees not to lease, rent, sub-license, loan, sell or otherwise redistribute the whole or any part of the Embedded Software. The Customer may, however, rent, lease or sell the Hardware, provided that: (a) any rental, leasing or sale must include the Hardware and all of the Embedded Software, including all its component parts, original media, printed materials and this EULA; (b) the Customer does not retain any copies of the Embedded Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the Hardware reads and agrees to accept the terms and conditions of this EULA.
- 4.3 The Customer agrees not to modify, disassemble, reverse engineer, derive the source code of, decrypt, create derivative works or decompile the whole or any part of the Embedded Software nor attempt to do so save to the extent expressly permitted by law.
- 4.4 The Customer will not attempt to ascertain or list the source programs or source code relating to the Embedded Software.
- 4.5 The Customer will notify the Company as soon as it becomes aware of any unauthorised use of the Embedded Software by any person.
5. Warranty
- 5.1 The Company believes that to the best of its knowledge the Embedded Software has been thoroughly tested for freedom from arithmetic or logical defects in the Embedded Software and that it will function and perform substantially in accordance with the functions described in the Documentation.
- 5.2 If at any time during the Warranty Period, the Customer becomes aware of a breach of the warranty at Clause 5.1, the Customer will:
- 5.2.1 promptly notify the Supplier of any defect which it believes to exist, such notice to be given prior to the expiry of the Warranty Period, with all details and information which may assist in diagnosing and correcting the defect; and
- 5.2.2 provide any facilities, information and assistance which the Supplier may reasonably request to aid the diagnosis of the alleged defect and co-operate with the Supplier in these activities.
- 5.3 If the Supplier is unable to ascertain or correct the defect with the Embedded Software as notified by the Customer in accordance with Clause 5.2, the Supplier (if not the Company) shall notify the Company.
- 5.4 The Company reserves the right to charge the Customer at its prevailing rates for any effort expended in tracing apparent defects which prove not to be defects covered under this Clause 5.
- 5.5 In the event of a proven breach of the warranty in Clause 5.1 during the Warranty Period, the Supplier (or Company (as the case may be)) will either:
- 5.5.1 repair, or at its option replace, the Embedded Software (or the relevant part of it); or
- 5.5.2 correct the Documentation to reflect the proper performance of the Software where it is determined by the Company (acting reasonably) that the Software is functioning correctly but is not properly described in the Documentation.
- 5.6 The repair or replacement of the Embedded Software under Clause 5.5 will not be available to the Customer if:
- 5.6.1 the defect in the Embedded Software is attributable to failure or breakdown or interference of any third party, or software or hardware not supplied subject to this EULA;

- 5.6.2 the Customer is in breach of this EULA;
- 5.6.3 the Customer fails to operate the Hardware properly or fails to follow the instructions or recommendations of the Company as set out in the Documentation with respect to the Embedded Software;
- 5.6.4 the Customer interferes with, modifies, or fails to secure the Embedded Software otherwise than in accordance with the terms of this EULA;

6. Training

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

7. Limit of Liability

- 7.1 Subject to Clause 7.2 and 7.3, the Company's maximum aggregate liability in connection with this EULA or the use of the Embedded Software will be limited to the lower of:
 - 7.1.1 any applicable limitation of liability set out in the Commercial Terms; or
 - 7.1.2 £100,000 or 100% of the price paid for the Hardware, whichever is lower.
- 7.2 Subject to Clause 7.3, the Company accepts no liability for any:
 - 7.2.1 loss of business, loss of revenue, loss of profits, loss of goodwill, loss of use, loss of data or loss of any economic liability; or
 - 7.2.2 indirect or consequential losses, however caused, arising in connection with this EULA or the use of the Embedded Software.
- 7.3 The Company makes no attempt to exclude liability relating to or arising from death or personal injury caused by the Company's negligence or the negligence of any employee, agent or contractor of the Company or liability for fraud or fraudulent misrepresentation, or for any other liability for which it would be unlawful to exclude or limit liability.

8. Disposal

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

9. Force Majeure

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

10. Termination

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

11. Consequences of Termination

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

12. Communications and Notices

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

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

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

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

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

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

13. Assignment

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

14. Waiver

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

15. Severance

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

16. Rights of Third Parties

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

17. Law

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

Data Protection Laws

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

17.3 In limited circumstances, the Company may have access to data stored on the Hardware which may include usernames 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.

Copyright © 1997 - 2024 ASSA ABLOY Global Solution UK Ltd trading as Traka.

All rights reserved.

All brand or product names are trademarks of their respective holders.

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.