

TRAKA21 GETTING STARTED GUIDE MODEL: KC-1-0156

UD0129

07/01/2025

VERSION 1.7

CONTENTS

Contents	1
GDPR Compliance Information	3
1. Introduction	4
2. System and iFob Diagrams	4
2.1 Cabinet Diagram	4
2.1.1 Cabinet Diagram Key	4
2.2 iFob (Intelligent fob) & Key bunch Diagram	5
2.2.1 iFob Diagram Key	5
3. Traka21 Overview	6
3.1 The Touch Screen	6
3.1.1 Screen Saver	6
3.1.2 Touch Commands	6
3.2 User Identification	6
3.3 Keyboard	7
4. Getting Started	8
4.1 Installing and Powering up the System	8
4.2 Setup Wizard	8
5. Logging in and Accessing the Admin Menu	11
6. Adding Keys	13
7. Adding Standard Users	16
8. Using the System	18
8.1 Removing & retuning Keys	18
8.1.1 Removing Keys	18
8.1.2 Returning KEys	19
8.2 iFob in Wrong Slot	20
8.3 iFobs Status Icons	20
9. Reports	21
9.1 Who's Got a Key?	21
9.2 Who's Had a Key?	22

9.3	Exporting Reports	24
10.	Help	26
10.1	Standard User Help	26
10.2	Admin User Help	27
11.	Technical Support	28
12.	End User Licence Agreement – Software	29

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

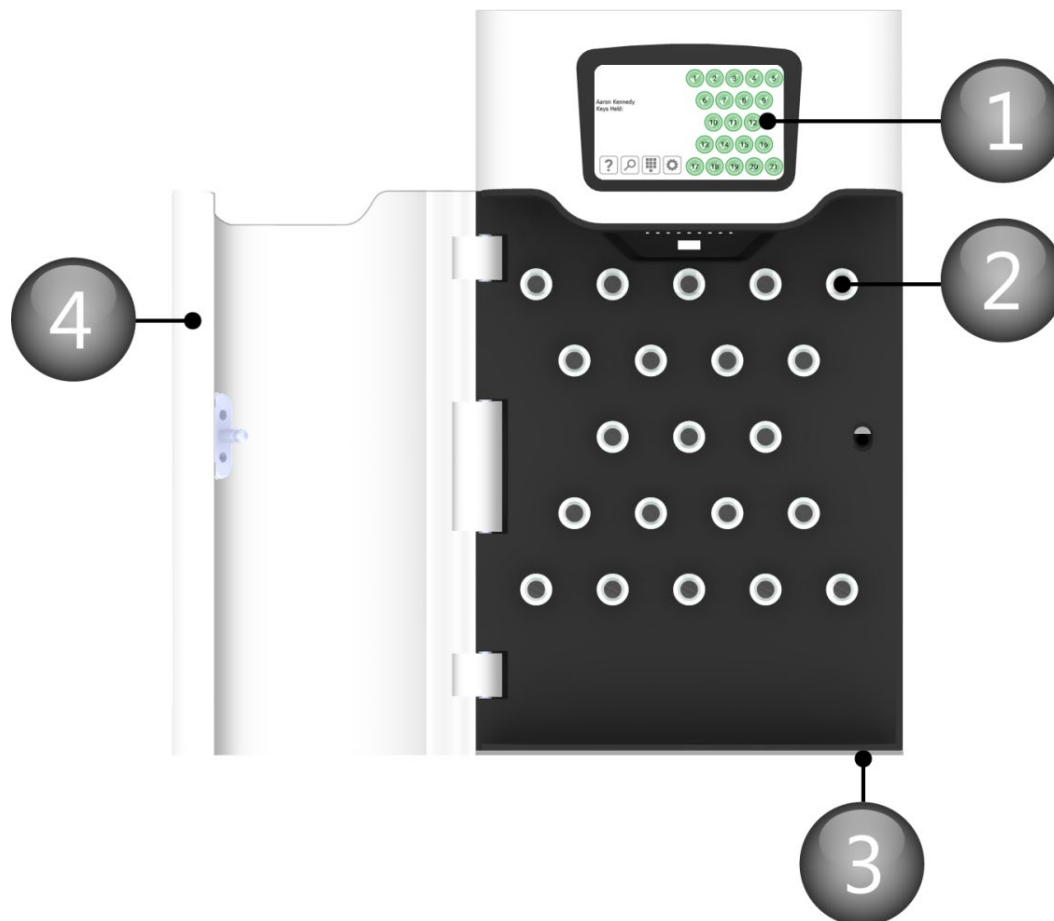
For more information about GDPR in relation to Traka products and systems, please contact GDPR@traka.com

1. INTRODUCTION

This User Guide has been prepared to assist you (the end user) with the operating basics of the Traka21. Please keep this guide handy for those times when you need to remember how to [Add a Standard User](#), [Add Keys](#) or run a [Report](#). This is a precursor to the full Traka21 User Guide (UD0130 – Traka21 User Guide).

2. SYSTEM AND IFOB DIAGRAMS

2.1 CABINET DIAGRAM



2.1.1 CABINET DIAGRAM KEY

1. **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 5" LCD.
2. **Receptor Slot**
The Receptor Slot holds and locks the iFob in place. iFobs are only related to authorised users
3. **Door Override Cam Lock**
This cam lock is a manual override for the cabinet door. Two keys will be supplied with your system; we ask that you do **not** keep these keys in the Traka21. 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 door.
4. **System Door**
Each Traka21 system is provided with a solid metal door for security and durability.

2.2 IFOB (INTELLIGENT FOB) & KEY BUNCH DIAGRAM



2.2.1 IFOB DIAGRAM KEY

1. **iFob**

The iFob is at the heart of any Traka21 system. It is a bullet shaped device made that contains an RFID tag with a unique identification number allowing the system to identify the key(s) attached.

2. **Security Seal**

The Security Seal is used to attach the key(s) to the iFob. Once the seal is crimped, the only way to detach the keys from the iFob is to cut the security seal using a pair of heavy duty cutters

3. TRAKA21 OVERVIEW

The Traka21 system uses touch screen technology for an easy, user friendly interface. The Traka21 does not require the use of a stylus or any other navigation device, to use the system simply click on the desired buttons with your finger.

3.1 THE TOUCH SCREEN

3.1.1 SCREEN SAVER



If the Traka21 system is not active for 30 seconds, then the system will go into 'power save' mode. To use the system again simply press anywhere on the touch screen.

3.1.2 TOUCH COMMANDS



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

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

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

3.2 USER IDENTIFICATION

The Traka21 is a PIN only entry system. The minimum PIN length must be at least four digits long, and the maximum length is ten digits.

3.3 KEYBOARD

The Traka21 keyboard supports extra characters that are selectable depending on the language your system is set too. To show these special characters, you will need to hold down the similar key on the keyboard and it will provide you with a list of special characters to choose from.

E.g. To get the Danish character "Ø" your system would need to be set to Danish, you would then need to hold down the "O" key and choose a character from the list pop up list.



In the next section you will be able to define the language you wish your system to be. To change your systems language after that, please refer to the General settings section in UD0130-Traka21 User Guide.

4. GETTING STARTED

4.1 INSTALLING AND POWERING UP THE SYSTEM

Ensure you have read and completed the Installation Instruction sheet that comes with the Traka21 system. This will give you instructions on how to install the system and switch the power on.

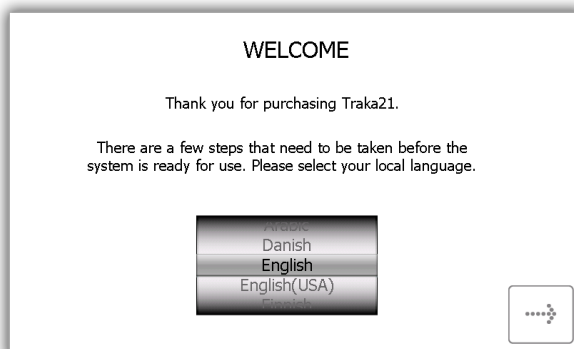
4.2 SETUP WIZARD

Once the system is powered on, you will be taken straight into the Setup Wizard. This wizard will take you through the essential first steps to getting the system up and running.

1. When the system is switched on you will be presented with the loading screen.



2. Once the system has finished initialising, the setup wizard will begin. At the Welcome page select your language and click the forward button.



3. Select the date and time then click the forward button.



- This section shows a breakdown of Traka21 hardware terminology. Read this page and click the forward button.

TERMINOLOGY





System - The term 'System' refers to the Traka21 unit

iFob - The iFob is the heart of the Traka21 system. It contains a small RFID chip which allows the system to identify the key(s) attached.

Security Seal - The Security Seal is used to attach the key(s) to the iFob. Once the seal has been crimped, the only way to detach the keys from the iFob is to cut the security seal using a pair of heavy duty cutters.

- This section explains how the users are added to the system by the administrator from the user wizard and how you can edit a user's access from the permissions section of the admin menu. Read this page and click the forward button.

TERMINOLOGY




Users - Users are added to the system by an Administrator and can either be a standard user or another administrator. This is done from the user wizard in the Admin section of Traka21

Permissions - The Permissions section of the Traka21 allows you to easily identify who has access to what keys and allows you to edit each users permissions

- This page explains the difference between standard and admin users. Read this page and click the forward button.

USERS IN MORE DETAIL

There are two different types of user, Admin users and Standard users.

			
Admin User	✓	✓	✓
Standard User	✗	✗	✓

An Admin User: has access to the Admin menu as well as Reports and Keys

A Standard User: only has access to Keys.

Traka21 must have at least one admin user in the system. The next screen will allow you to create your first admin user

- Standard Users** – Can only remove and return keys. Providing they have been granted access to those keys in their user details.
- Admin Users** – Can access keys, the admin menu and run reports.

- Next you will prompted to add the first admin user of the system. Enter the Forename, Surname, Contact & PIN number into the provided fields. When you are done click the forward button.

ADD FIRST ADMIN USER

Forename:

Surname:

Contact:

PIN:



- **Contact** – This field is for a phone number, fax number, email or any means of contact that the user is reachable by.
 - **PIN** – The PIN (personal identification number) is the numeric password that will grant you access into the system. It must be between four and ten digits long.
8. The basic setup is now complete. This window will give instructions on what you need to do next. You will need to identify the following...
- What keys you would like in the system.
 - Who will use those keys.
 - Who will have access to those keys.

BASIC SETUP COMPLETE

WHATS NEXT?

Keys		Identify what keys you want to put into the system
Users		Identify who will use the system
Permissions		Identify who will have access to what



9. The final page of the setup wizard will show how to login to the system and navigate to the administration menu. Click the forward button to begin.

NEXT STEPS

To add keys, users and permissions ...

1. Enter your PIN at the login screen



2. Click the Admin icon to get to the Admin screen



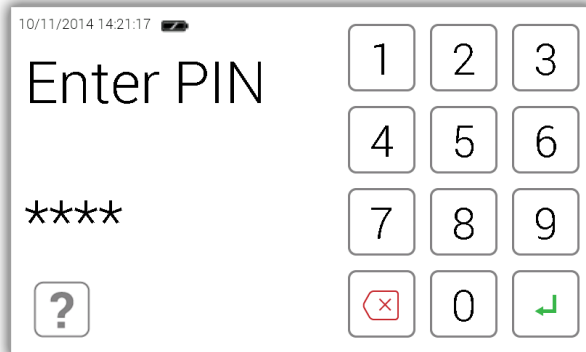
3. From the Admin screen you can choose to setup Keys, Users and Permissions



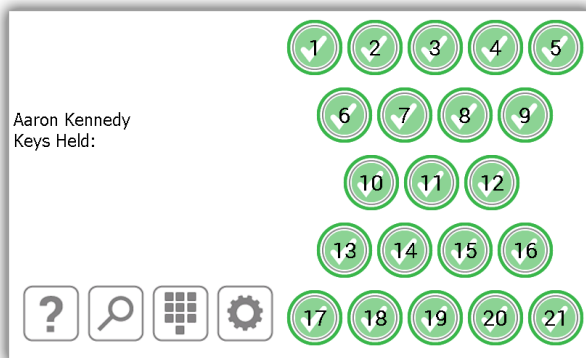

5. LOGGING IN AND ACCESSING THE ADMIN MENU

When the setup wizard is complete you will be taken to the login screen.

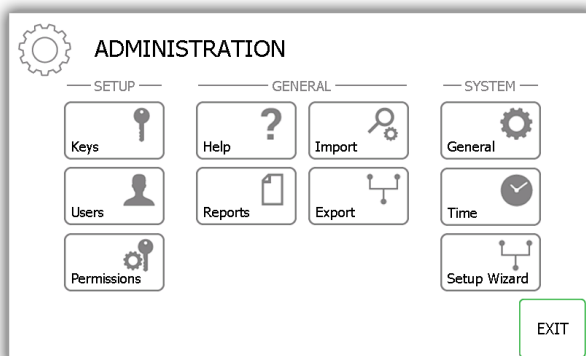
1. Touch the screen to bring the system out of power save mode.
2. Enter your PIN.



3. Press  (enter) to confirm your PIN.
4. The door will then open allowing you access to the keys.
5. Verify your name on the touch screen.



6. Select the admin button .

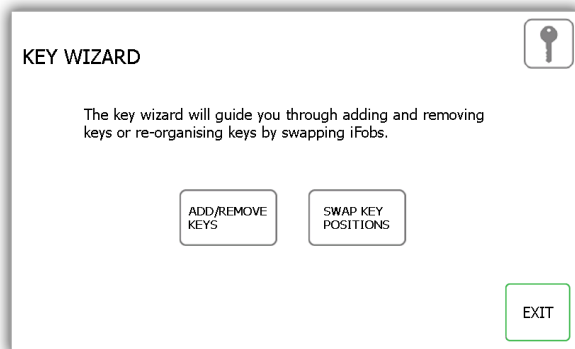


7. From the admin menu select either the Keys or Users button to add keys and users to the system. Please refer to the relevant sections below (Section 6 Adding Keys, Section 7 Adding Users).

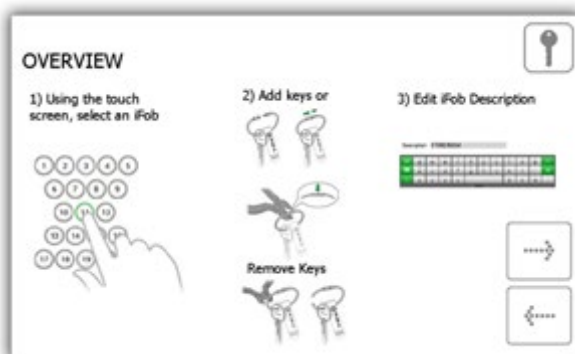
6. ADDING KEYS

Next you can add keys to the iFobs in the system. When the Key Wizard appears you will be given two options to select from.

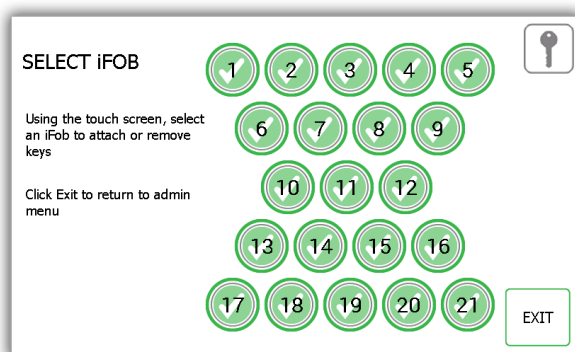
1. Select the Add/Remove Keys button from the key wizard menu.



2. The overview screen will appear providing you instructions on how to add keys to an iFob. Read these instructions and click the forward button.



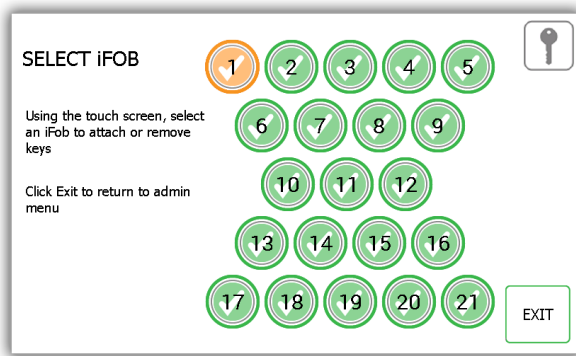
3. Select the desired iFob using the touch screen.



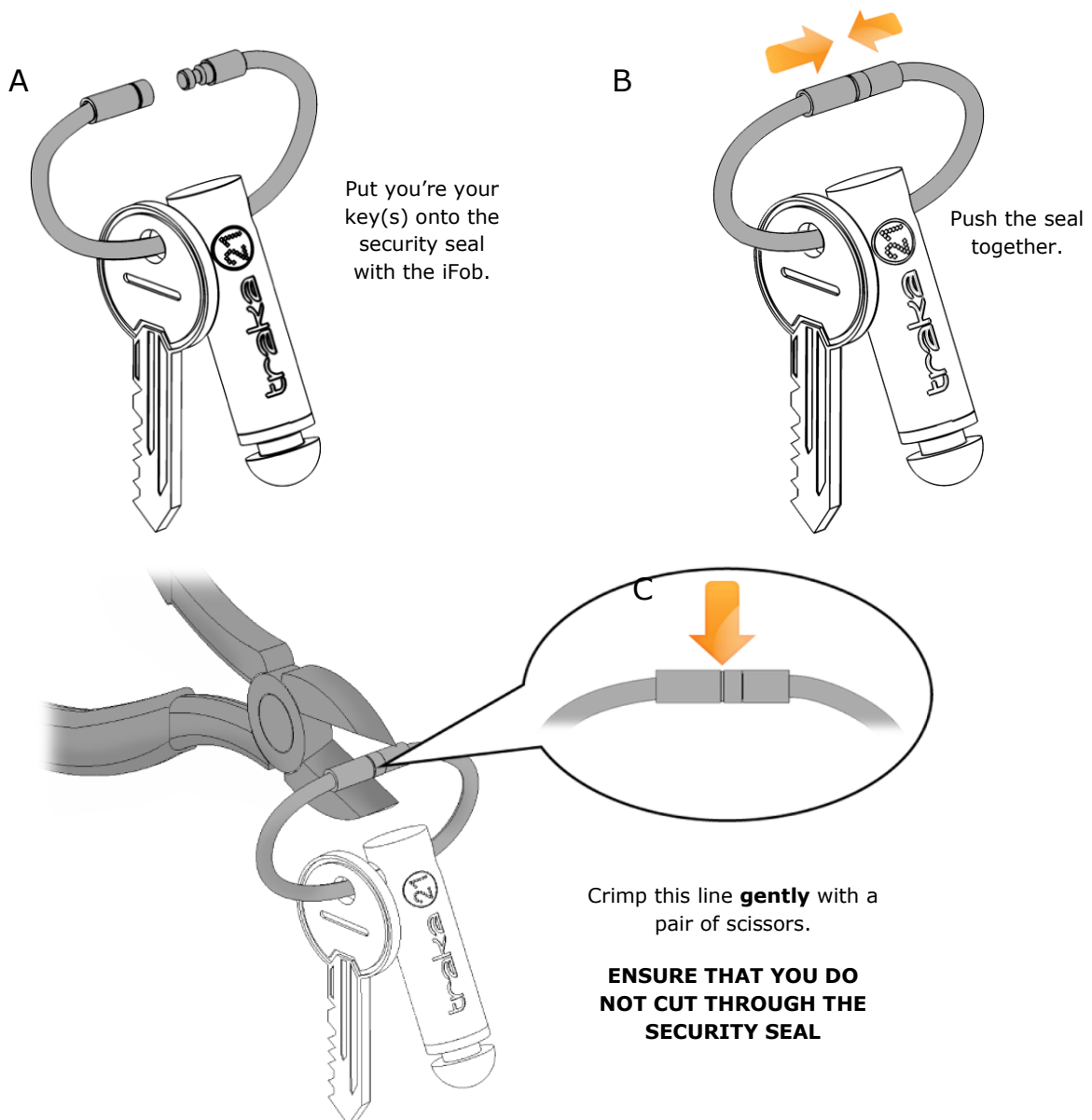
4. The iFob will then be released from the system.

NOTE: If at any time you wish to exit the Key Wizard, close the door or select the Exit button.

5. Remove the iFob from the system. The touch screen will display an orange 'removed' icon for the iFob you have taken.



6. Now the iFob is out of the system, you can attach your key(s) using the provided Security Seal.



7. You will be prompted to enter a description for the key(s). Click save when you have finished.

ENTER DESCRIPTION

Update the description and click next

Position: 1

Description: Reception Keys

123 Q W E R T Y U I O P

A S D F G H J K L

Z X C V B N M ,

SAVE

CANCEL

8. Return the iFob to the system. The orange 'removed' icon will now become green again as you have returned it to the system.

SELECT iFOB

Using the touch screen, select an iFob to attach or remove keys

Click Exit to return to admin menu

1 2 3 4 5

6 7 8 9

10 11 12

13 14 15 16

17 18 19 20 21

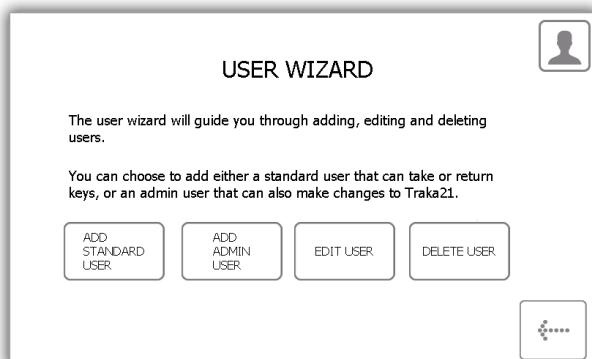
EXIT

9. To add more keys to an iFob, simply select another iFob from the touch screen.
10. When you are finished adding keys, click the exit button to be taken back to the admin menu.
11. Select the User button next and refer to the Adding user section below.

7. ADDING STANDARD USERS

A standard user does not have access to the admin menu or any reports. This user will only be able to remove and return keys.

1. Select the Add Standard User button.

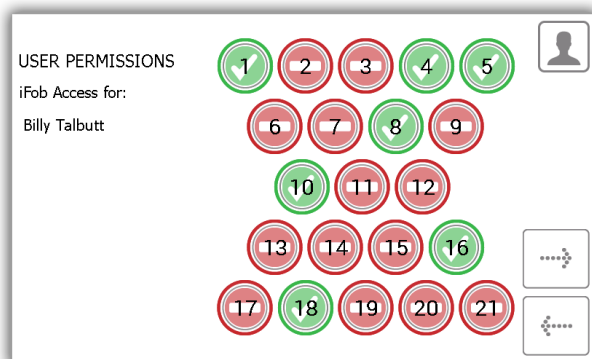


2. The user details window will appear allowing you to enter the user's forename, surname, contact number and PIN. Enter the details and click the forward button.



- **Contact** – This field is for a phone number, fax number, email or any means of contact that the user is reachable by.
- **PIN** – The PIN (personal identification number) is the numeric password that will grant you access into the system

3. Next you will need to select the user's permissions. Using the touch screen simply select which iFobs the user will have access too. The green ticks show the user currently has access to the iFob and the red line indicated that they do not. Once you have finished granting access, click the forward button.



4. At the options page you can set the following...

- User Expiry Date – Here you can set the date and time the users profile expires and becomes inactive at the system.
- Force user to change PIN on next login? – enabling this option will force the user to change their PIN when they next attempt to log onto the system.



ADD USER OPTIONS

Options for:
Billy Talbutt

User Expiry Date: 10/11/2064 14:33 

Force user to change PIN on next login?: 

Select the appropriate features and click the forward arrow.

5. The user wizard is now complete. A message will appear stating that you have successfully added a user.



USER WIZARD - COMPLETE

You have successfully added a user.

Would you like to add another?

YES NO EXIT

6. If you want to add more users click yes and you will be taken to a new user details screen. Follow steps 2-5 again.
7. If you are finished and do not want to add any more users click no and you will be taken back to the Admin menu.

8. USING THE SYSTEM

To use the Traka21 a user with the correct credentials must login at the system.

8.1 REMOVING & RETUNING KEYS

8.1.1 REMOVING KEYS

Removing a key is a **one handed operation**.

1. **Enter** your PIN at the system.
2. The door will open.
3. **Authorised** iFob slots will be illuminated **green**.
Unauthorised iFob slots will be illuminted **red**.
4. **Press** the on screen button for the iFob you wish to remove.
5. **Wait** for the “**click**” (unlocking iFob).
6. **Remove** iFob.



8.1.2 RETURNING KEYS

You **must** return the key to the correct receptor slot.

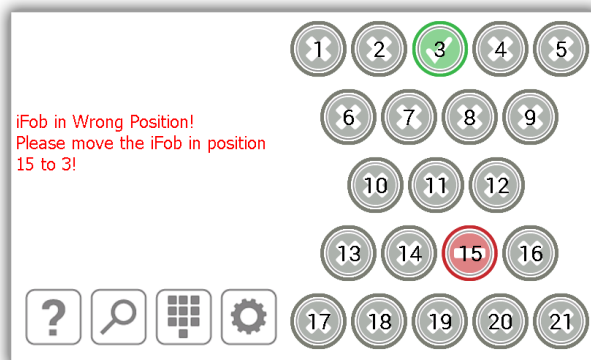
1. **Enter** your PIN at the system.
2. The door will open.
3. **Positions illuminated Orange** indicate the iFobs held by the current user.
4. **Insert** iFob into matching receptor slot.

NOTE: If you return the iFob to the incorrect slot, the touch screen will notify you and request that you remove the key and return it to the correct slot as indicated. The positions in the system will also illuminate and guide you to the correct position.



8.2 IFOB IN WRONG SLOT

When an iFob is returned to the incorrect position the system will prompt you to remove the iFob from the incorrect position and return it to the correct position.



In addition to the touch screen giving you instructions, the receptor positions will illuminate and guide you to the correct slot as shown below.



8.3 IFOBS STATUS ICONS

Please see below descriptions of each iFob status in the Traka21 system.



The green circle with a white tick symbol indicates that the user has access to the iFob.



The red circle with a white line shows that the user does not have access to the iFob



The orange circle with a white tick indicates that the iFob is out of the system to the currently logged in user.



The grey circle with a white cross shows that the iFob is out of the system to another user.

9. REPORTS

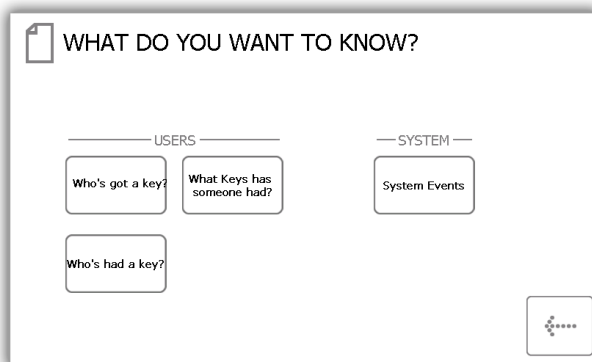
Reports allow you to view all the transactions and events that have occurred at the system. To access reports, a user with admin permissions must access the admin menu

For more information on reports Traka21 has to offer please read the latest version of UD0130 – Traka21 User Guide.

9.1 WHO'S GOT A KEY?

This report will show you who currently has what keys out of the system.

1. Enter your PIN at the system.
2. The door will then open.
3. Select the Admin button.
4. From the admin menu select the reports button.
5. In the Users category, select the 'Who's got a Key?' button.



6. Traka21 will then generate a list of all the users who currently have any iFob's out of the system.

A screenshot of a report titled "WHO'S GOT A KEY?". It displays a table with four columns: Slot, Description, Current User, and Time Taken. The first row is highlighted in green. To the right of the table are navigation buttons: a left arrow, an up arrow, a down arrow, and a right arrow. At the bottom right are "EXPORT" and "EXIT" buttons.

Slot	Description	Current User	Time Taken
1	Reception Keys	Paul Robinson	13/11/2014 12:22:51
2	Car Park Keys	Aaron Kennedy	13/11/2014 12:22:14
3	Research & Developm	Aaron Kennedy	13/11/2014 12:22:18
4	Forklift Truck	Billy Talbutt	13/11/2014 12:23:13
9	Office Keys	Paul Robinson	13/11/2014 12:22:42
10	Vehicle Key	Billy Talbutt	13/11/2014 12:23:10
12	Store Room	Aaron Kennedy	13/11/2014 12:22:23
17	Safe Key	Paul Robinson	13/11/2014 12:22:47

7. You can export this information to a USB memory stick if you wish by clicking the Export button. Please review the Exporting Reports topic at the end of this section for more details.

9.2 WHO'S HAD A KEY?

This report will allow you to see the history of a particular key, i.e. which users have had it out of the system.

1. Enter your PIN at the system.
2. The door will then open.
3. Select the Admin button.
4. From the admin menu select the reports button.
5. In the Users category, select the 'Who's had a Key?' button.

WHAT DO YOU WANT TO KNOW?

—USERS—

Who's got a key?

What Keys has someone had?

Who's had a key?

—SYSTEM—

System Events

Navigation icons: back, forward, search, etc.

6. Select the key you wish to view the history of and click the forward button.

WHO'S HAD A KEY?

SELECT KEY:

Grid of 21 keys (1-21):

- Row 1: 1, 2, 3, 4, 5
- Row 2: 6, 7, 8, 9
- Row 3: 10, 11, 12
- Row 4: 13, 14, 15, 16
- Row 5: 17, 18, 19, 20, 21

Navigation icons: back, forward, search, etc.

7. Next you will need to filter your results by selecting a data range. You can manually enter a start and end date or use the pre-set buttons at the bottom to automatically enter the date range for you.

WHO'S HAD A KEY?

Select Date Range

Select a date range below to filter upon

Start date: 13/11/2014 13:09

End date: 13/11/2014 13:14

Navigation icons: back, forward, search, etc.

Pre-set buttons: TODAY, LAST 7, LAST 30

The pre-set buttons will automatically select the date range for you as follows...

TODAY

LAST 7

LAST 30

- The **'Today'** button will provide data for selected report beginning at 00:00 of today's date and end at the current time you are running the report.
- The **'Last 7'** button will provide data for the selected report from the last seven days.
- The **'Last 30'** button will provide data for the selected report from the past 30 days.

To manually filter the date range, select the button next to the start or end date.

Start date

13/11/2014 13:09

...

End date

13/11/2014 13:14

...

A scrollable control will now allow you select the exact date and time you wish to run the report on.

SELECT START DATE AND TIME

Date

Day	Month	Year
11	September	2012
12	October	2013
13	November	2014
14	December	2015
15		2016

Time

Hour	Minute
11	13
12	14
13	15
14	16
15	17

SET

CANCEL

- Once you have selected your desired date range, click the forward button.
- The report will now generate and display the list of users who have removed the selected key with the date range.

NOTE: The key position is noted at the top of the page each time the report is run. E.g. position 1.

WHO'S HAD A KEY?

Position: 1

Description: Reception Keys

Name	Event	Date/Time
Aaron Kennedy	Item Returned	13/11/2014 12:29:12
Paul Robinson	Item Removed	13/11/2014 12:22:51
Aaron Kennedy	Item Returned	10/11/2014 14:25:18
Aaron Kennedy	Item Removed	10/11/2014 14:25:00
Aaron Kennedy	Item Returned	10/11/2014 14:24:58
Aaron Kennedy	Item Removed	10/11/2014 14:24:58
	Unrecognised Item Returned	10/11/2014 09:04:42

◀

▲

▼

▶

EXPORT

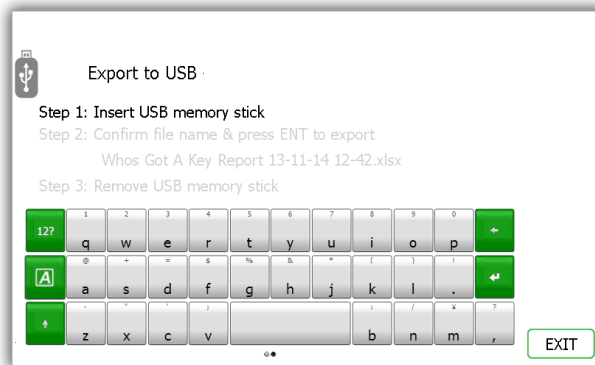
EXIT

- You can export this information to a USB memory stick if you wish by clicking the Export button. Please review the Exporting Reports topic at the end of this section for more details.

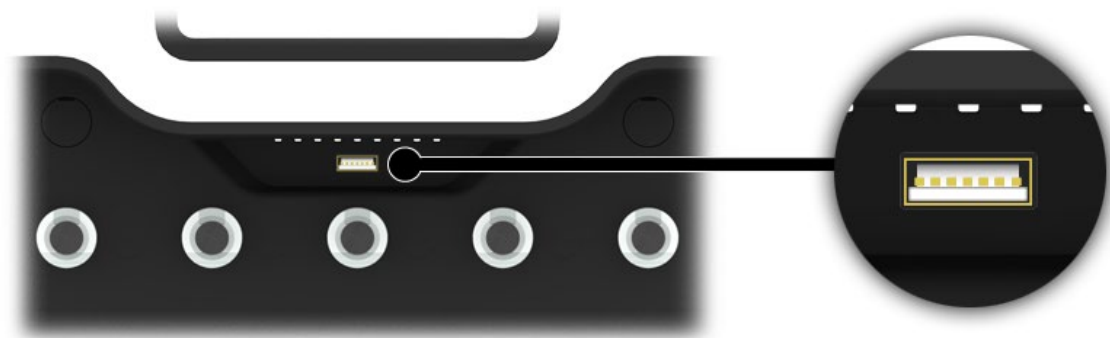
9.3 EXPORTING REPORTS

Once you have run a report you can export the data to a USB memory stick.

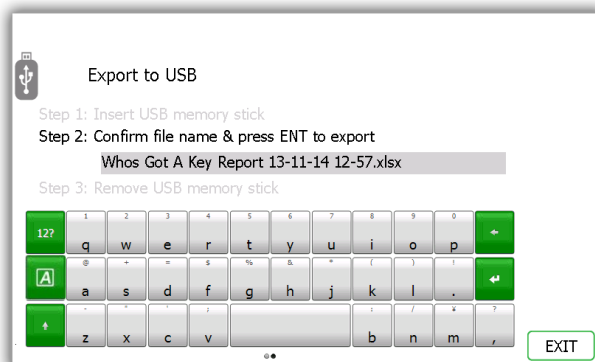
1. Run a report as instructed in the previous sections.
2. On the results page there is a button in the bottom right hand called Export.
3. Click the Export button and a new screen will appear prompting you to enter a USB memory stick.



4. Insert a USB memory stick into the slot on the system.



5. Type a filename and select enter  to begin the exporting process.



NOTE: Do not remove the memory stick whilst the data is transferring. You may corrupt or even loose the data.

6. Once the data is finished transferring to the USB memory stick, a message will appear informing you that you can remove it from the system.



7. You can now close the door to finish or click the Exit button to go back to the Reports menu.

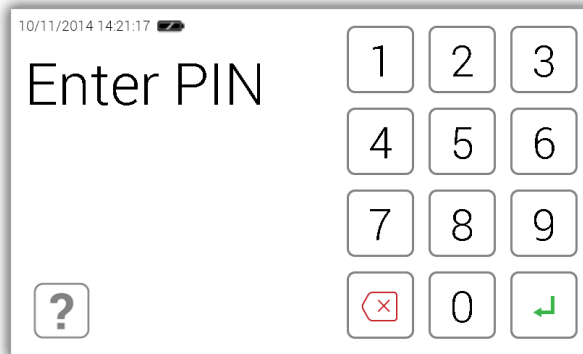
10. HELP

The Traka21 has embedded help topics that will assist you with the everyday tasks of using the system. The help page can be viewed from two locations, the main login screen and the admin menu. Every user will be able to view the help page from the login screen but it will have limited help topics available. If an admin user access the help page in the admin menu there are many more topics

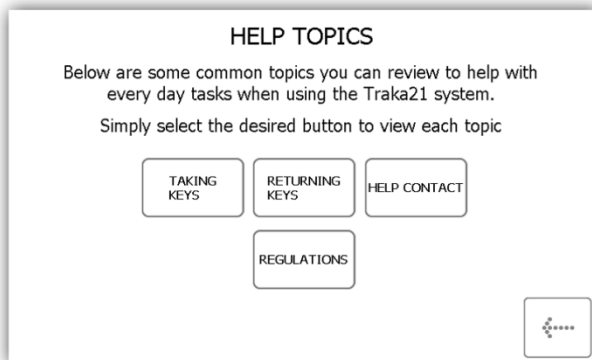
10.1 STANDARD USER HELP

A standard user will only have access to the help topics at the login screen of the Traka21.

1. From the main login screen select the help button.



2. When the help screen appears you will have three options to select from.



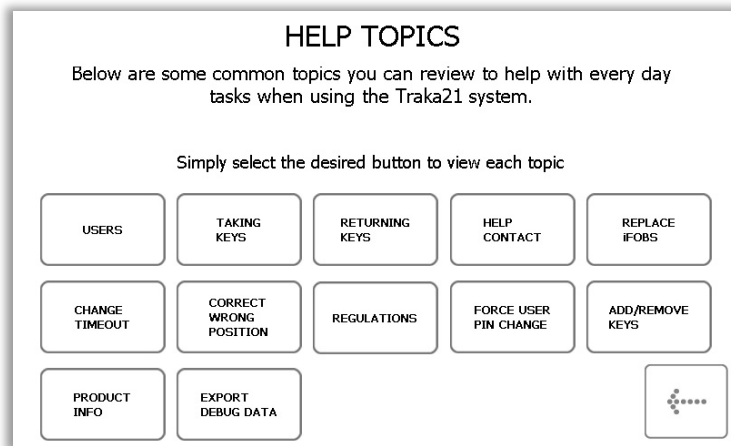
- **Taking Keys** - Will give you a pictorial overview on how to remove a key from the system.
- **Returning Keys** - Will give you a pictorial overview on how to return a key to the system.
- **Help Contact** - Will display contact details if you need technical assistance.
- **Regulations** - This page will give you all the information on the compliances that the Traka21 adheres to.

3. Select the desired button to open the topic.
4. To return to the help screen, click the back button.

10.2 ADMIN USER HELP

An admin user will be able to see all of the help topics in the system.

1. Enter your PIN at the system.
2. The door will then open.
3. Select the Admin button.
4. From the admin menu select the help button.
5. The full list of help topics will then appear.



- **Users** - Explains the difference between standard and admin users and the access they each have.
- **Taking Keys** - Will give you a pictorial overview on how to remove a key from the system.
- **Returning Keys** - Will give you a pictorial overview on how to return a key to the system.
- **Help Contact** - Will display contact details if you need technical assistance.
- **Add/Remove Keys** - Will show you how to add/remove keys to security seals.
- **Change Timeout** - Explains what the system timeout is and how to change it.
- **Correct Wrong Position** - explains how you can allow a user to correct an iFob that has been incorrectly returned.
- **Replace iFobs** - Explains how to replace an iFob in the system.
- **Force User to Change PIN** - Explains how you can force a user to change their PIN.
- **Unrecognised iFobs** - Shows what the system will do when an unrecognised iFob is put into the system.
- **Product Info** - Provides information about the Traka21 system.
- **Export Debug Data** - Selecting this button will begin a process that exports a zipped debug file to a USB memory stick which you can later send back to Traka for evaluation.

6. Select the desired button to open the topic.
7. To return to the help screen, click the back button.

NOTE: For more information on each of these topics please review the latest version of UD0130 – Traka21 User Guide.

11. TECHNICAL SUPPORT

If you need technical support, please visit the Traka21 website.

www.traka21.com

12. END USER LICENCE AGREEMENT – SOFTWARE

Please refer to the policies section of the Traka web site for the most up-to-date information concerning Traka's software EULA:

<https://www.traka.com/global/en/about/policies>