TRAKA21
USER GUIDE
MODEL: KC-1-0156

UD0130

07/01/2025

VERSION 2.6

CONTENTS

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 Users, Add Keys or run Reports.

1.1 SUMMARY OF TRAKA21

Traka21's innovative plug and play system provides small to medium size businesses with the very latest in intelligent key management.

Simple, efficient and cost-effective, Traka21 helps trace and account for every key or keyset, which are individually locked in place, ensuring that critical business operations are never jeopardised.

1.2 GLOSSARY OVERVIEW

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 keys(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.

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 the 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 user's permission.

2. TRAKA21 OVERVIEW

The Traka21 system uses touch screen technology for an easy, user friendly interface. 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.

2.1 THE TOUCH SCREEN

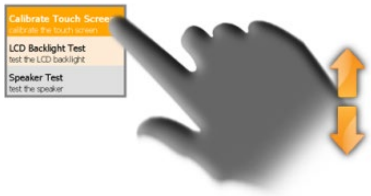
2.1.1 SCREEN SAVER

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.

2.1.2 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 will allow you to scroll through the various options.

2.2 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.

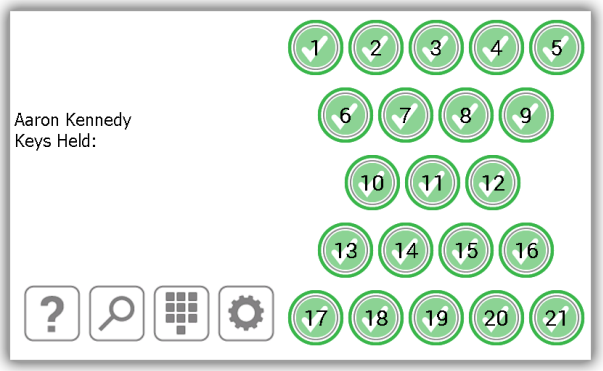
3. USING THE SYSTEM

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

3.1 LOGGING INTO THE SYSTEM

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.



3.2 REMOVING & RETUNING KEYS

3.2.1 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.

3.2.2 RETURNING KEYS

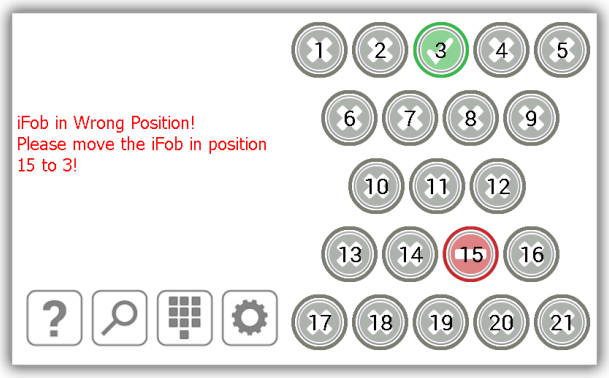
You **must** return the key to the correct receptor slot.

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.

3.3 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.

NOTE: This is a configurable option that can be selected on or off for all users in the general settings of Traka21. Please view section 4.8 for more details.

3.4 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

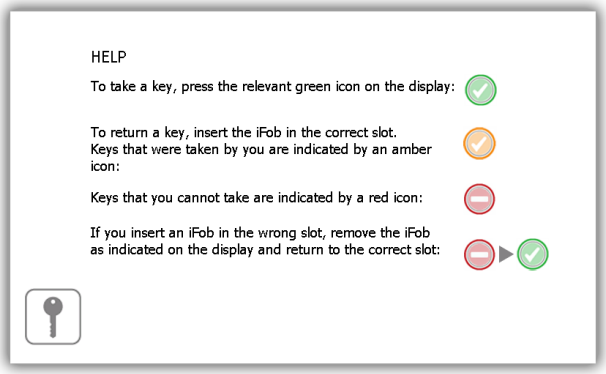
The orange circle with a white tick indicates that the iFob is out of the system to the currently logged in user.

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

3.4.1 HELP

Whilst a user is logged in they can click the help button for information on the iFob status and at what point they can take a key.

1. Click the help button from the logged in screen 
2. The help screen will then appear giving details on which iFobs a user can or can't take.



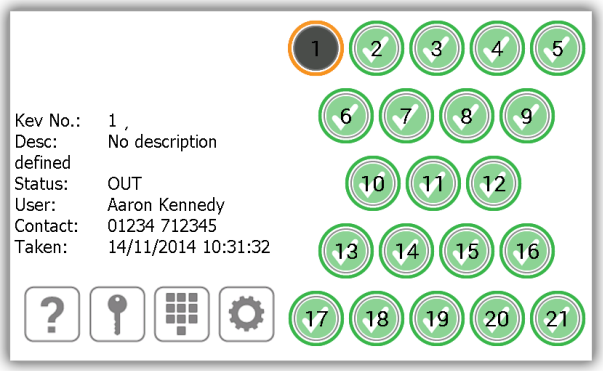
3. To get back to the logged in screen click the keys button 

3.5 IFOB LOOKUP

When a user is logged in they can click the search icon and look up the details of an iFob.

1. Click the search button from the logged in screen 

2. Select which key you wish to search for.



The search will detail the following information...

- The position of the iFob
- Any description assigned to the key(s) on the iFob
- Whether the iFob is in or out of the system
- If the iFob is out of the system, this will display the user who currently has the iFob. If the iFob is in, this will display the user who last returned it.
- The users contact information
- And the date & time it was last taken or returned.

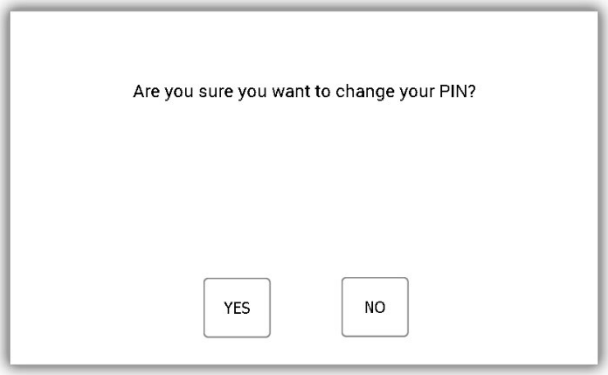
3. To search again, simply select another iFob position.

4. When you are finished click the keys button  and you will be taken back to the logged in screen.

3.6 CHANGE PIN

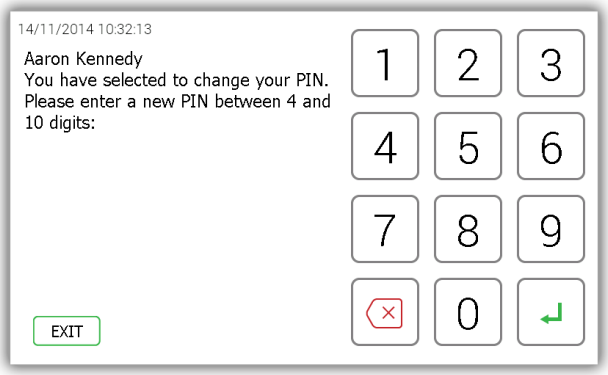
A user can change their PIN by selecting the change PIN button once they have logged in. This option can be turned on and off in the General screen. Refer to section 4.8 'General', for more information on enabling and disabling this option.

1. If available, click the change PIN icon from the logged in screen 
2. A message will appear asking if you wish to change your PIN. Click Yes.

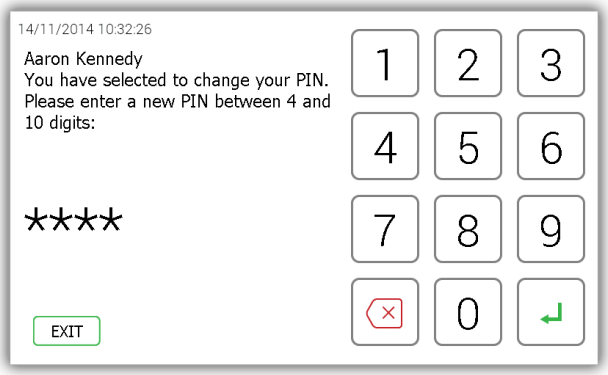


3. Enter your new PIN and click enter ↵.

NOTE: your PIN must be at least four digits long but can be no longer than ten.



4. You will be prompted to enter your new PIN a second time for clarification. Click enter ↵.

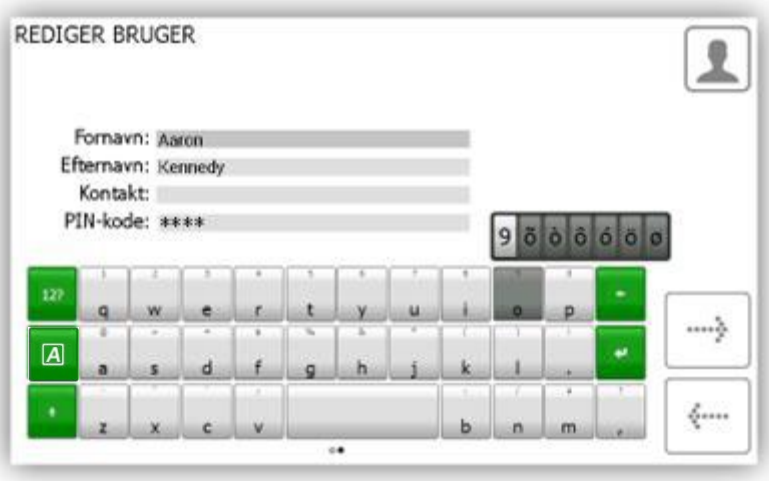


5. A message will be displayed stating your PIN change was successful. You will then be taken back to the login screen.

3.7 KEYBOARD

The Traka21 keyboard supports extra characters that are selectable depending on the language your system is set to. 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.

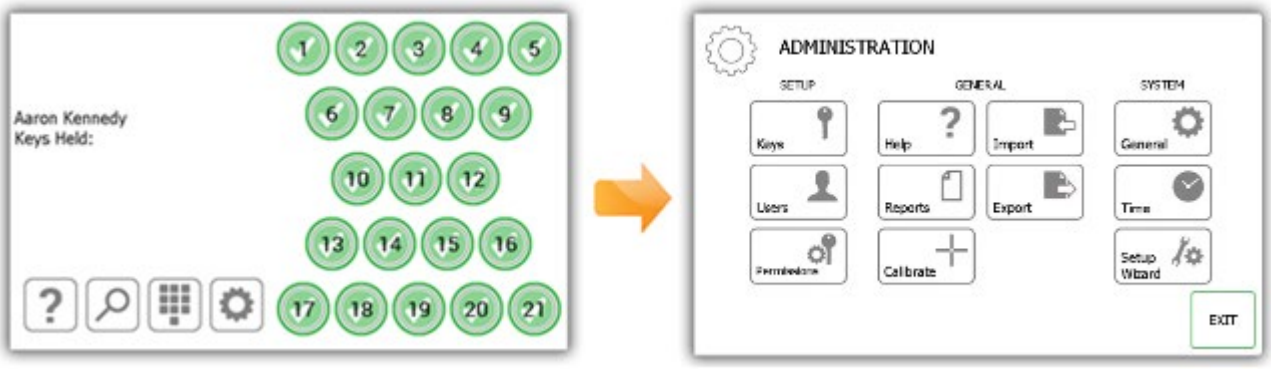
E.g. To get the Danish character "Ø" your system would need to be set to Danish, you would then need to hold down the "O" key and choose a character from the list pop up list.



To change your systems language, please refer to the General settings section.

4. ADMIN MENU

This section of the user guide will take you through the admin menu and all of its features. To access the admin menu, a user with admin access will need to identify themselves at the system and select the admin button.

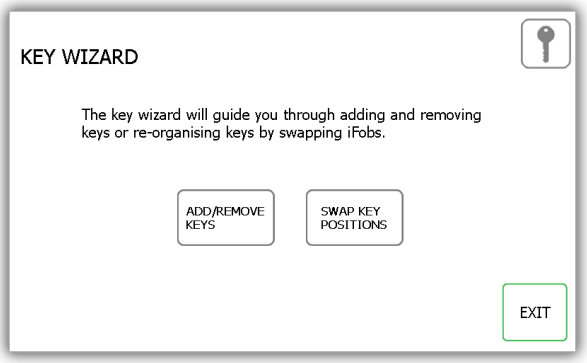


4.1 KEYS

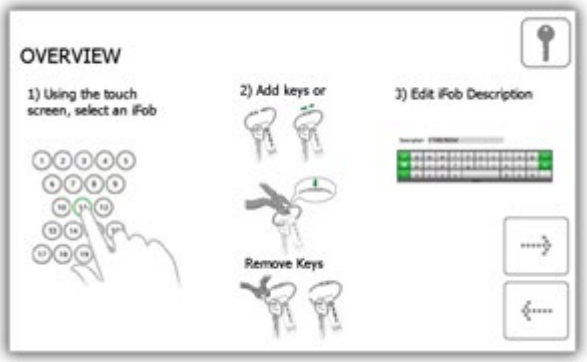
From the admin menu select the Keys button. The key wizard will allow you to add/remove keys to iFobs in the system. You can also use the feature swap key positions, which allow you to reorganise the keys in the system.

4.1.1 ADDING/REMOVING KEYS

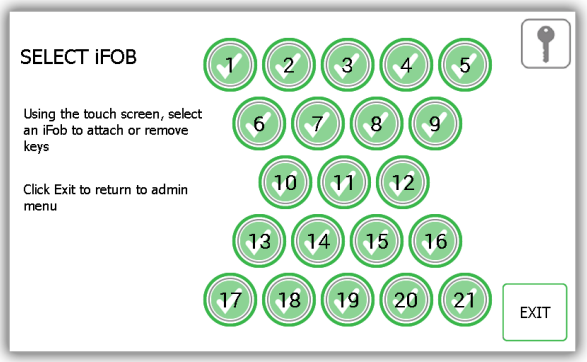
1. Select the Add/Remove Keys button from the key wizard menu.



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.



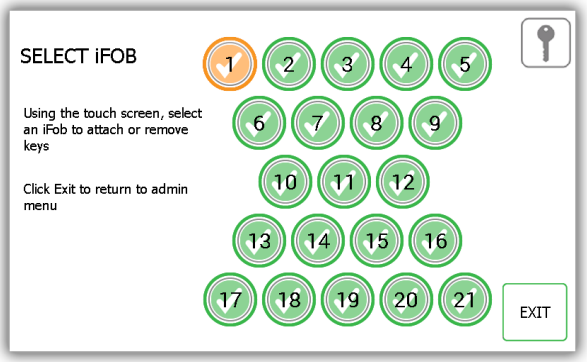
3. Select the desired iFob using the touch screen.



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.

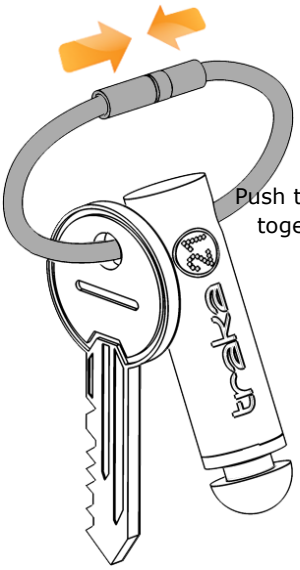


6. Now the iFob is out of the system, you can attach your key(s) using the provided Security Seal.

A

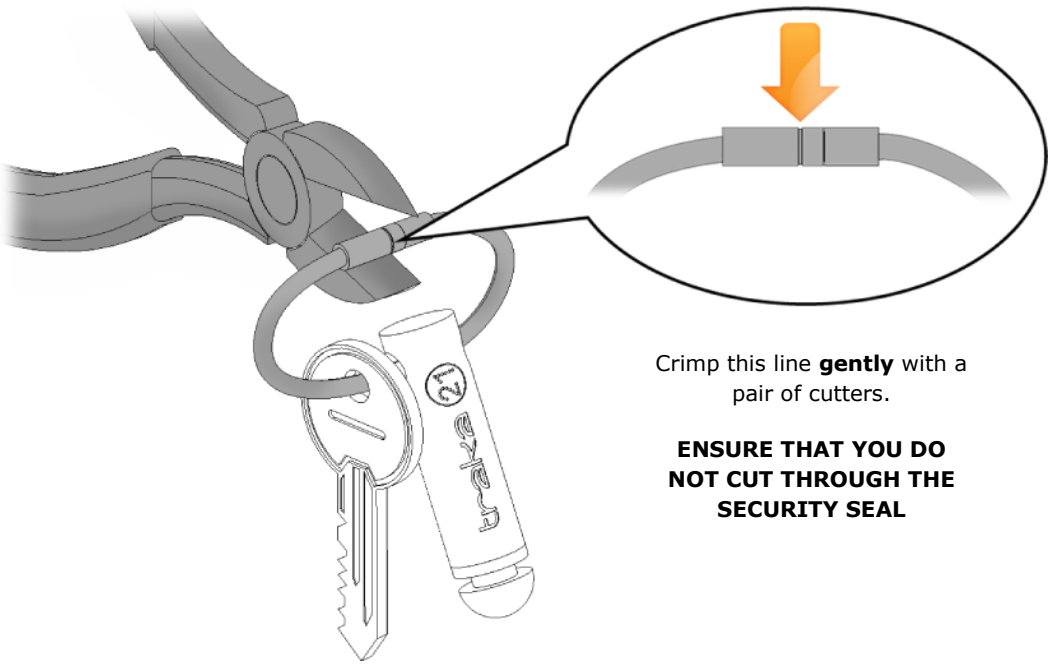
Put you're your key(s) onto the security seal with the iFob.

B



Push the seal together.

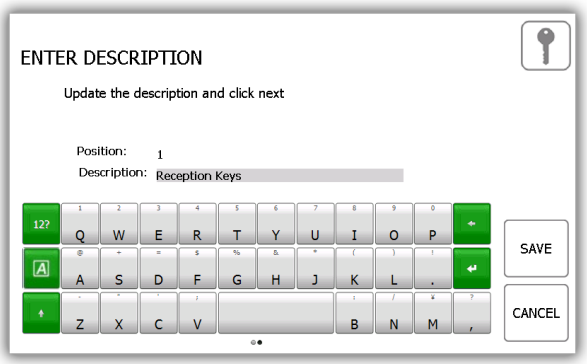
C



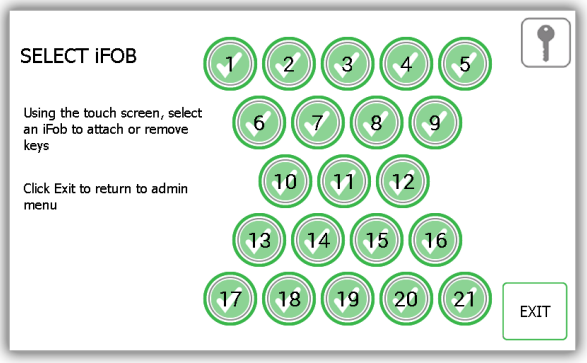
Crimp this line **gently** with a pair of cutters.

ENSURE THAT YOU DO NOT CUT THROUGH THE SECURITY SEAL

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



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



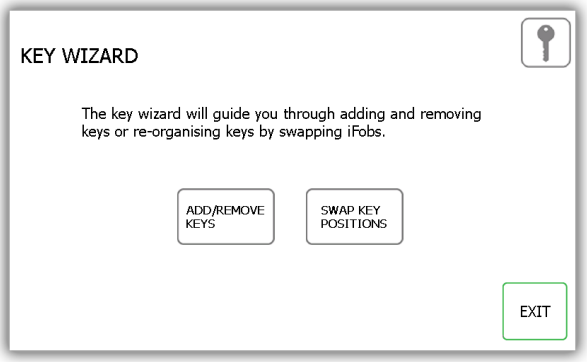
9. To add more keys to an iFob, simply select another iFob from the touch screen.

10. When you are finished adding keys, click the exit button to be taken back to the admin menu or close the door.

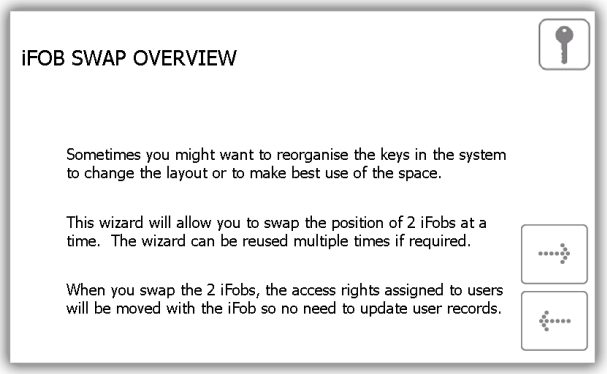
4.1.2 SWAP KEY POSITIONS

The swap key positions feature is very beneficial if you wish to reorganise the keys in the system. Using the swap key feature, you won't need to cut or re-crimp any security seals; the system will reassign the iFobs to new positions.

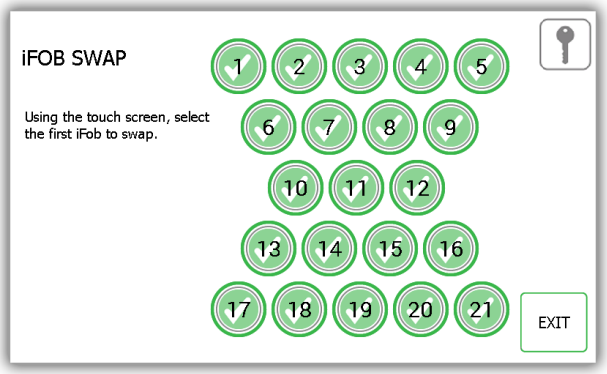
1. Select the Swap Key Positions button from the key wizard menu.



2. The swap key overview will then appear giving you a description of how the feature works. Read this and click the forward arrow.

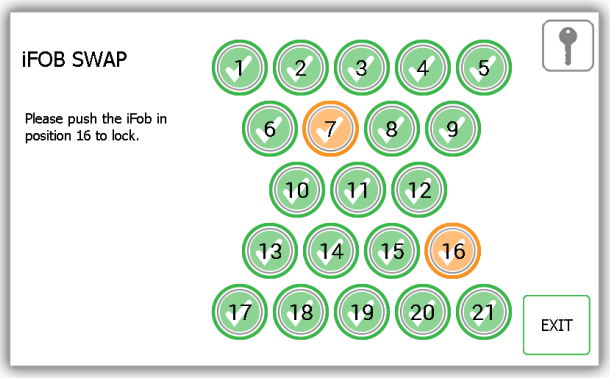


3. Select the first of the two positions you want to swap over.



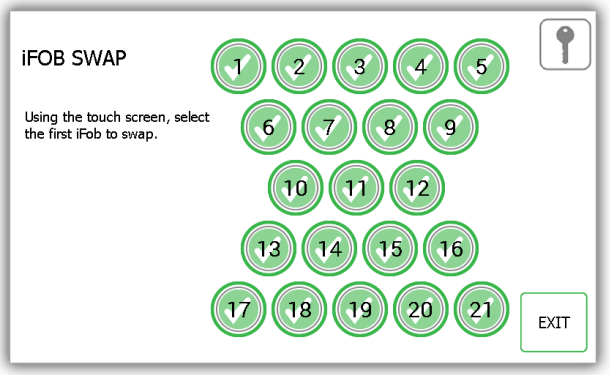
4. The iFob will then release to you. Put it safely to one side.

5. Select the second iFob and it will release from the system.



6. Now that both iFobs are out of the system, you can return them to the system in their new positions.

7. The system will recognise the swap and will accept both iFobs.



8. To swap more Fobs simply being this process again from step 3.

9. When you are finished click the exit button to return to the admin menu or close the door.

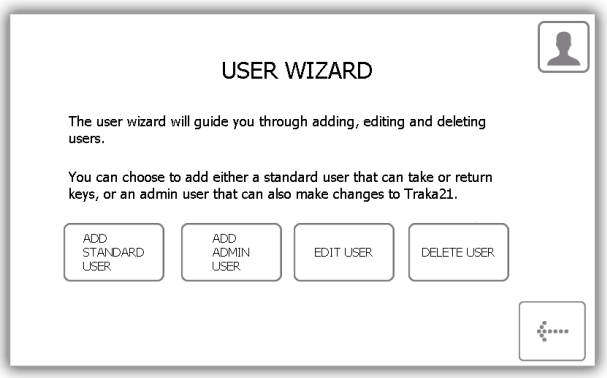
4.2 USERS

From the admin menu click the user's button. To add, edit or delete a user, login to the system and navigate to the admin menu. From the admin menu select the user's button.

4.2.1 ADDING A STANDARD USER

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. When the User Wizard appears you will have many options to choose from.

1. Select the Add Standard User button.

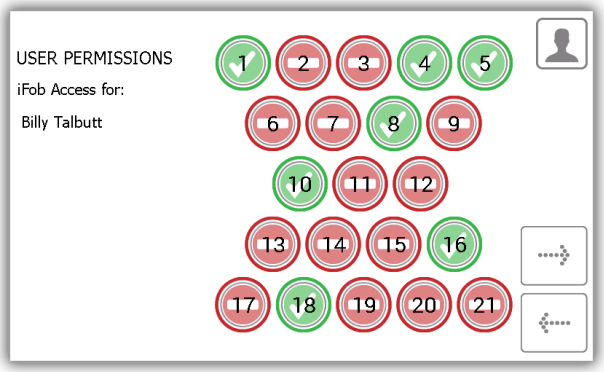


2. The user details window will appear allowing you to enter the user's forename, surname, contact number and PIN. Enter the details and click the forward button.

- **Contact** – This field is for a phone number, fax number, email or any means of contact that the user is reachable by.

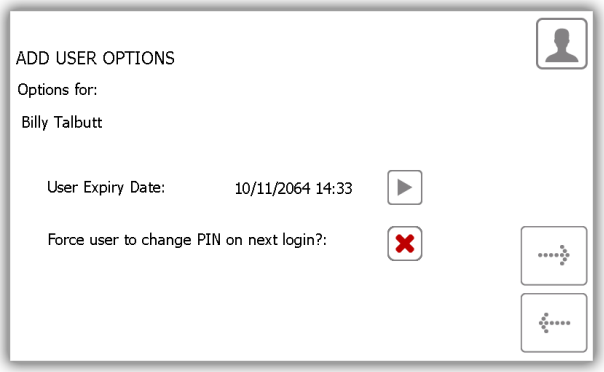
- **PIN** – The PIN (personal identification number) is the numeric password that will grant you access into the system. It must be between four and ten digits long.

3. Next you will need to select the user's permissions. Using the touch screen simply select which iFobs the user will have access to. The green circles with white ticks show positions the user currently has access to. To remove access, simply click the button to turn it to a red circle with a white line. When you have finished 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.



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.

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. From there click exit again to return to the login screen.

4.2.2 ADDING AN ADMIN USER

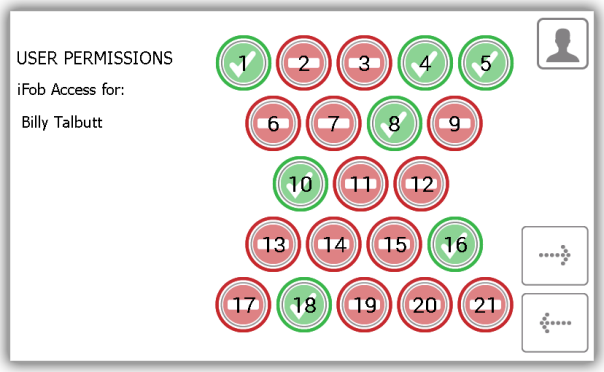
An admin user can remove and return keys as well as access the admin menu and run reports.

1. Select the Add Admin 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.

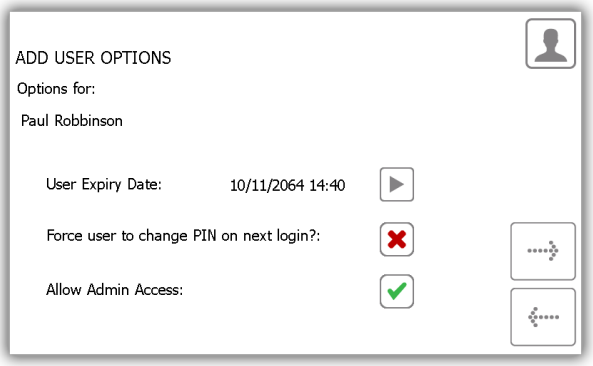
- **Contact** – This field is for a phone number, fax number, email or any means of contact that the user is reachable by.
- **PIN** – The PIN (personal identification number) is the numeric password that will grant you access into the system. It must be between four and ten digits long.

3. Next you will need to select the user's permissions. Using the touch screen simply select which iFobs the user will have access to. The green circles with white ticks show positions the user currently has access to. To remove access, simply click the button to turn it to a red circle with a white line. When you have finished click the forward button.



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.



Select the appropriate features and click the forward arrow.

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

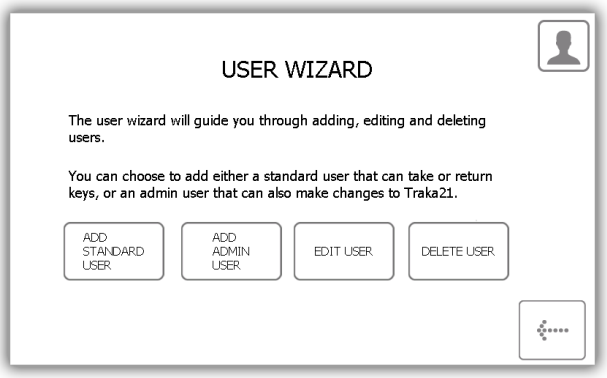
5. If you want to add more users click yes and you will be taken to a new user details screen. Follow steps 2-5 again.

6. 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. From there click exit again to return to the login screen.

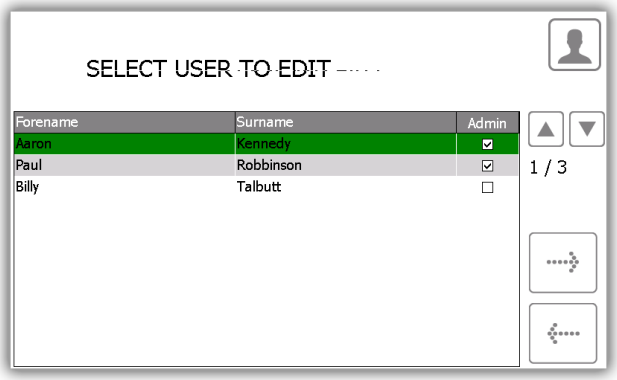
4.2.3 EDIT USERS

You can edit a user's details...

1. Select the Edit User button.

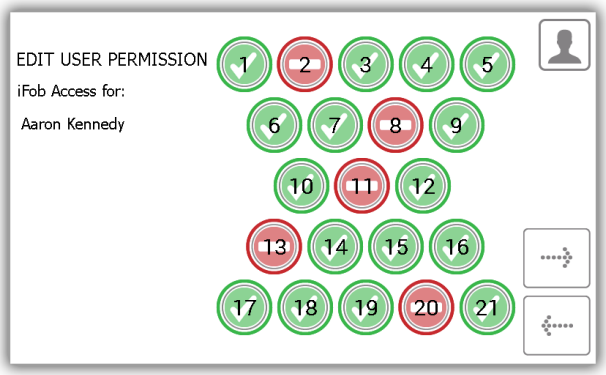


2. The current user list will appear. Highlight the desired user and click the forward button.



3. The user's forename, surname, contact and PIN will then appear. Make any changes you need and click the forward arrow.

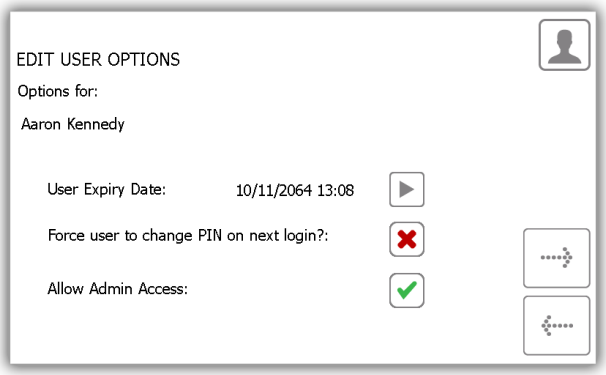
4. Next edit the key permissions by selecting the positions the user may or may not have access to.



5. Next edit the user options. Here you can...

    - Change the expiry date of the user.
    - Select/deselect the force user to change PIN option.
    - Select/deselect Allow admin access option.

    Edit the desired options and click the forward button.



6. The edit is now complete. A message will now appear saying you have successfully edited a user.

7. If you want to edit more users click yes and you will be taken to the user list. Follow steps 2-5 again.

8. When you are finished, click the exit button to return to the admin menu.

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

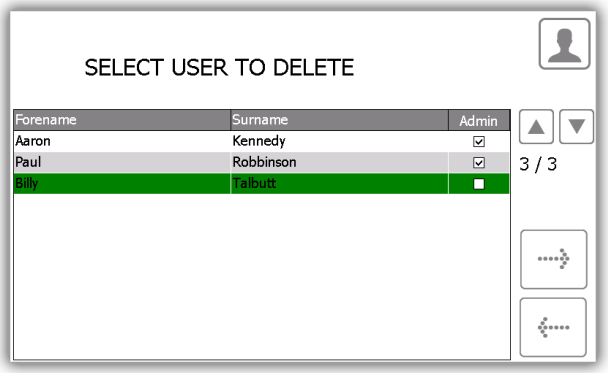
It is also recommended that a back-up of the database is made after the above changes are completed & all previous database back-ups destroyed.

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

You can delete a user from the system...

1. Select the Delete User button.

2. The current user list will appear. Highlight the desire user and click the forward button.



3. A message will appear asking if you wish to delete the user. Click Yes.

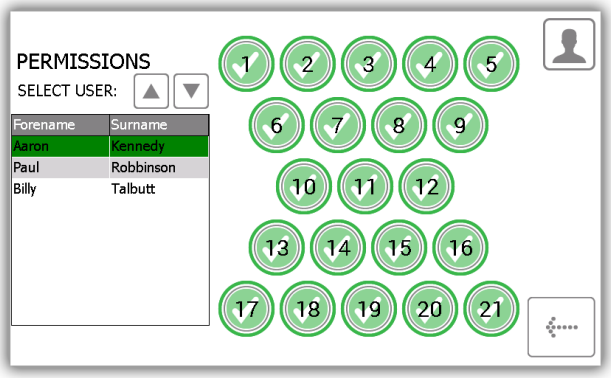
4. The use will now be deleted from the user list.
5. To delete more user repeat steps 2-3.
6. When finished click the back button.

4.3 PERMISSIONS

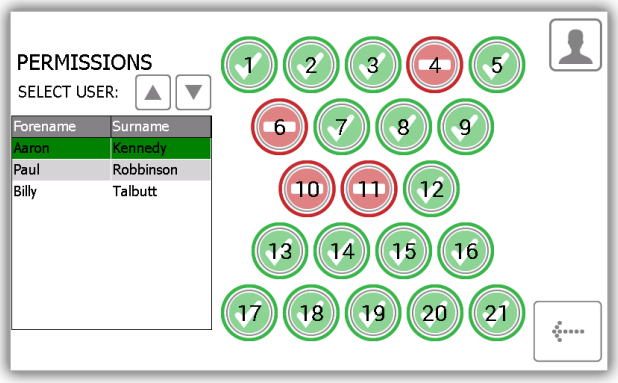
From the admin menu select the permissions button. The permissions section allows you to view all the current users in the system and grant/revoke their access rights without having to edit their individual user details.

1. From the admin menu select the permission button.

2. From the list on the left, highlight the user whose permissions you wish to edit.



3. Simply select the positions you wish the user to have access to.



4. To edit another user simply scroll down and highlight the desired user.

5. To go back to the admin menu click the back button.

4.4 HELP

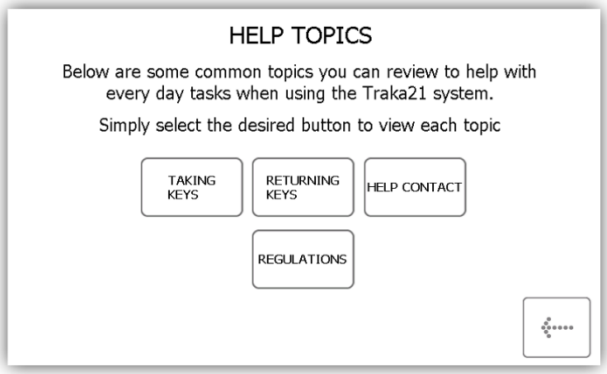
The Traka21 has embedded help topics that will assist you with the everyday tasks of using the system. The help page can be viewed from two locations, the main login screen and the admin menu. Every user will be able to view the help page from the login screen; however it will not have all the topics that are available from the admin menu. This has been done to make it easier for the 'standard users' as they will only be able to view the help topics on actions they can make.

4.4.1 STANDARD USER HELP

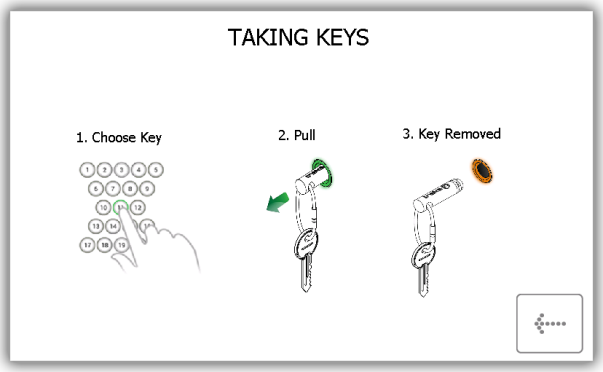
A standard user will only have access to the help topics at the login screen of the Traka21.

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

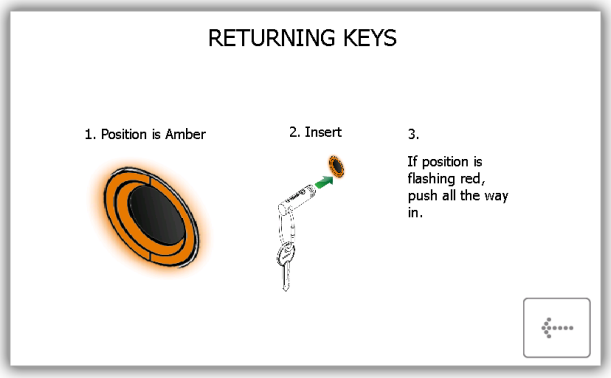
2. When the help screen appears you will have four options to select from.



- **Taking Keys** - Will give you a pictorial overview in three steps on how to remove a key from the system.

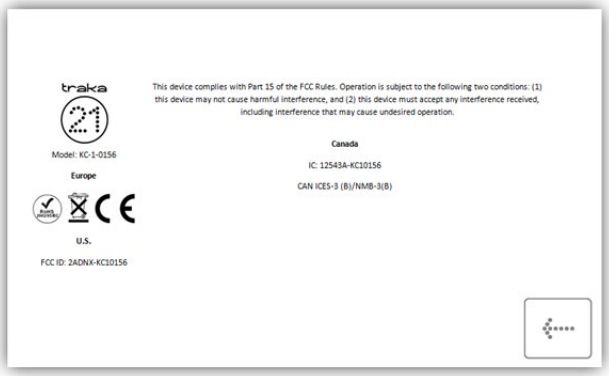


- **Returning Keys** - Will give you a pictorial overview in three steps on how to return a key to the system.



- **Help Contact** - Will display contact details if you need technical assistance. The details shown here can be changed by the admin user.

- **Regulations** – This page will give you all the information on the compliances that the Traka21 adheres to.



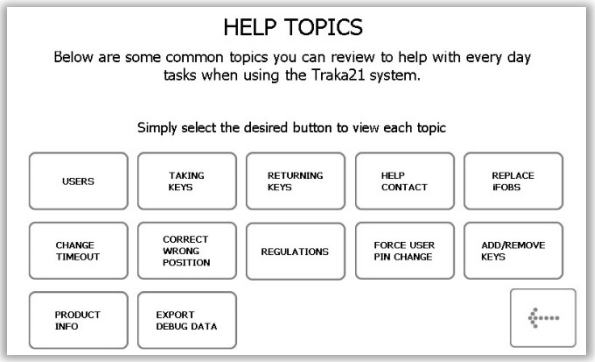
3. Select the desired button to open the topic.

4. To return to the help screen, click the back button.

4.4.2 ADMIN USER HELP

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

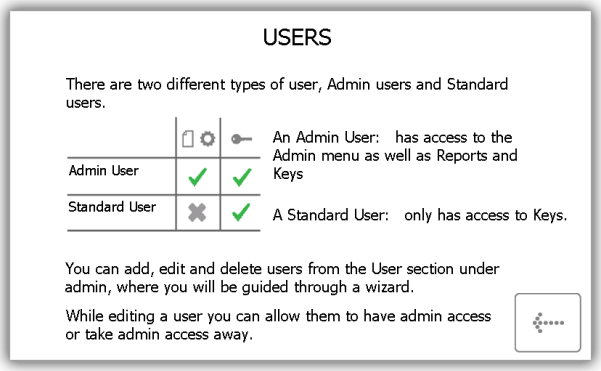
1. From the admin menu select the help button.
2. The full list of help topics will then appear.



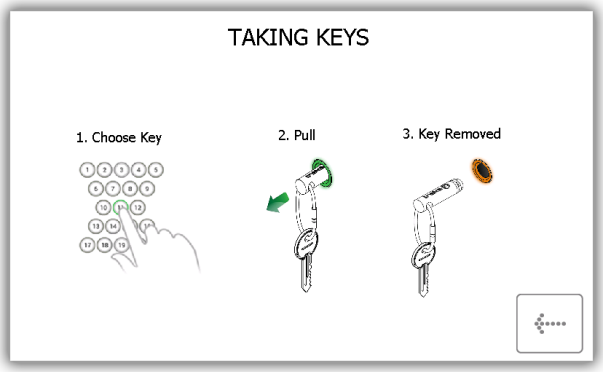
- **Users** - Explains the difference between standard and admin users and the access they each have.

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

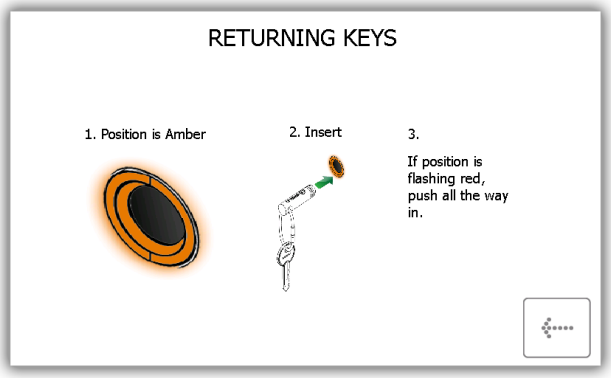
  An admin user has access to all aspects of the Traka21 system, users, keys, admin menu and reports.



- **Taking Keys** - Will give you a pictorial overview on how to remove a key from the system.



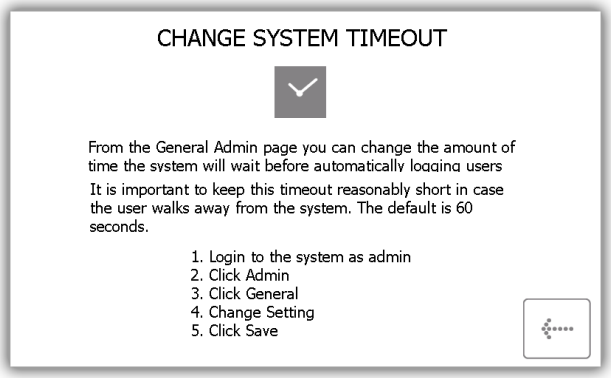
- **Returning Keys** - Will give you a pictorial overview on how to return a key to the system.



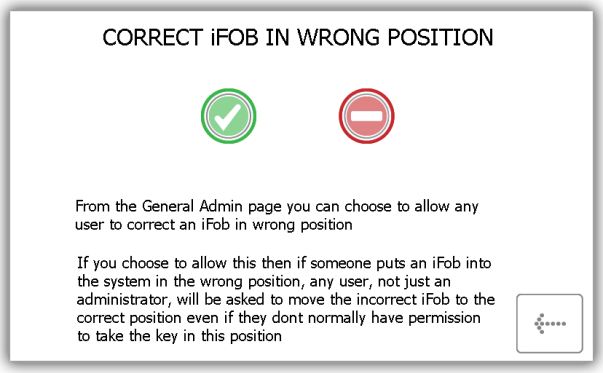
- **Help Contact** – Will allow you to enter new details that change the help section that is displayed to the standard user.

- **Replace iFobs** – How to replace a broken/lost iFob.
  i) Login to the system as an admin.
  ii) Insert the new iFob into the position you want to assign it to.
  iii) The system will ask you if want to assign this new iFob to this position.
  iv) Choose Yes to start using the new iFob in this position.

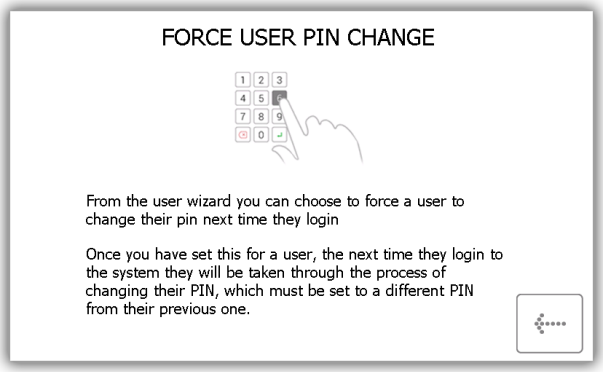
- **Change Timeout –** The timeout is a user definable period of time that when reached will send the system into power save mode. This can be changed in the general settings under the admin menu.



- **Correct Wrong Position** - Explains how you can allow a user to correct an iFob in Wrong Slot. This is definable from the general section.



- **Force User to Change PIN** – when creating or editing a user, the admin user can select an option called force user to change PIN. This will force that user to change their PIN when they next login.



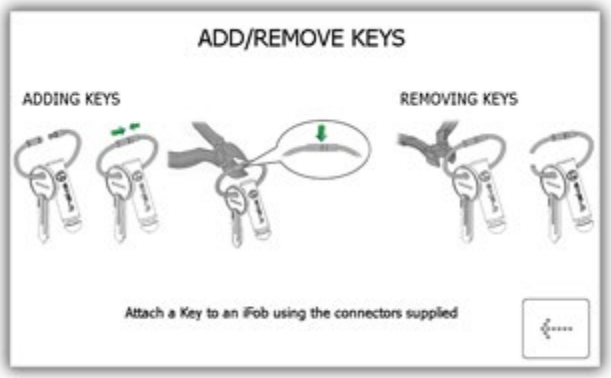
- **Add/Remove Keys -** Will show you how to add/remove keys to security seals.

  To add keys

  i) Put your key(s) onto the security seal with the iFob.
  ii) Push the seal together
  iii) Crimp the highlighted line **gently** with a pair of cutters. **ENSURE THAT YOU DO NOT CUT THROUGH THE SECURITY SEAL.**

To remove keys

i) Using a pair of heavy duty cutters, cut the security seal to remove the keys and the iFob.



- **Product Info –** Will provide information about the Traka21 system as well as a report on 'Disk Usage'.

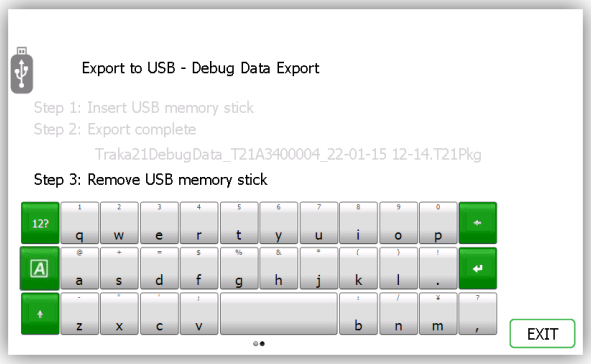
- **Export Debug Data** - Selecting this button will begin a process that exports a zipped debug file to a USB memory stick which you can later send back to Traka for evaluation.

i) The system will immediately prompt you to insert a USB memory stick.

ii) After inserting a USB stick, you can rename the file. Once finished click the enter button.

iii) After inserting a USB stick, you can rename the file. Once finished click the enter button.

iv) When the export is complete you can remove the memory stick



v) The memory stick can now be put into a computer and the .Pkg file can be removed from the USB drive and sent to Traka for analysis.

3. Select the desired button to open the topic.

4. To return to the help screen, click the back button.

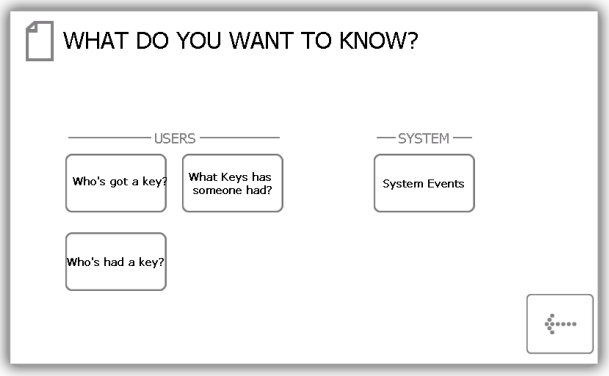
4.5 REPORTS

From the admin menu select the reports button. Reports allow you to view all the transactions and events that have occurred at the system.

4.5.1 WHO'S GOT A KEY?

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

1. From the admin menu select the reports button.
2. In the Users category, select the 'Who's got a Key?' button.



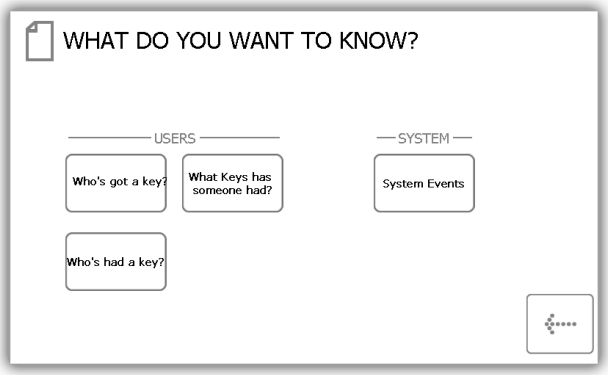
3. Traka21 will then generate a list of all the users who currently have any iFob's out of the system.

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

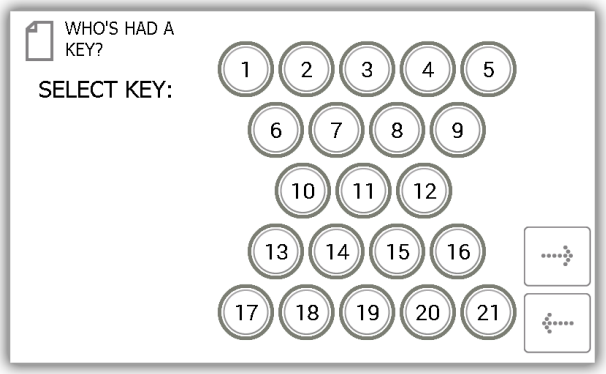
4.5.2 WHO'S HAD A KEY?

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

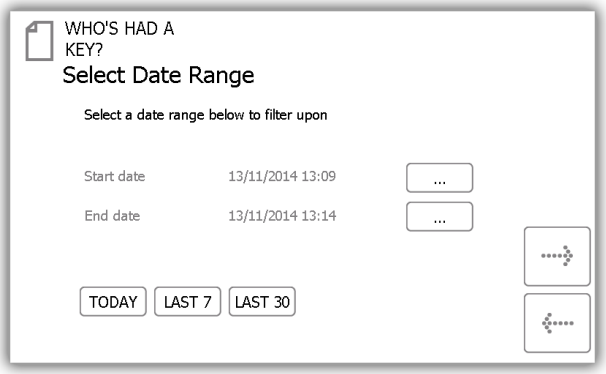
1. From the admin menu select the reports button.
2. In the Users category, select the 'Who's had a Key?' button.



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



4. 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.

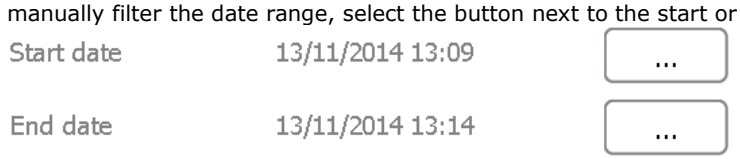


The pre-sets buttons will automatically select the date range for you as follows...

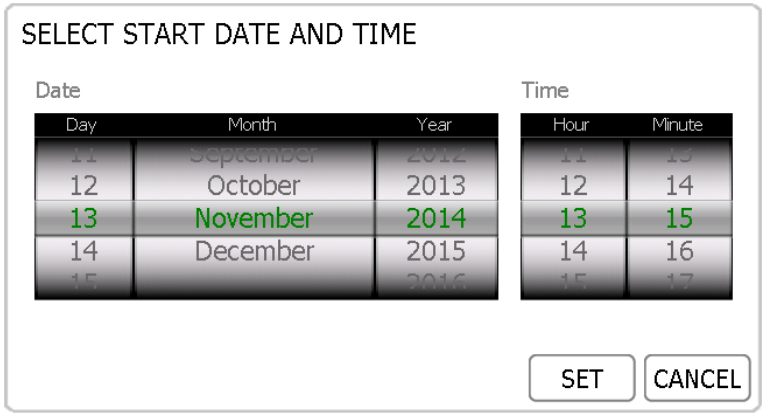
- The '**Today'** button will provide data for selected report beginning at 00:00 of today's date and end at the current time you are running the report.
- The '**Last 7'** button will provide data for the selected report from the last seven days.

- 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.

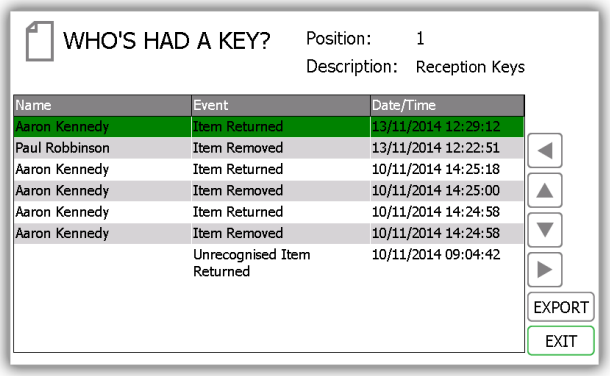


A scrollable control will now allow you select the exact date and time you wish to run the report on.



5. Once you have selected your desired date range, click the forward button.
6. 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.

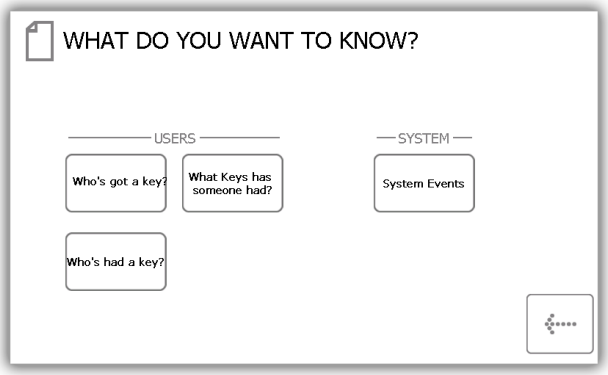


7. You can export this information to a USB memory stick if you wish by clicking the Export button. Please review the Exporting Reports topic at the end of this section for more details.

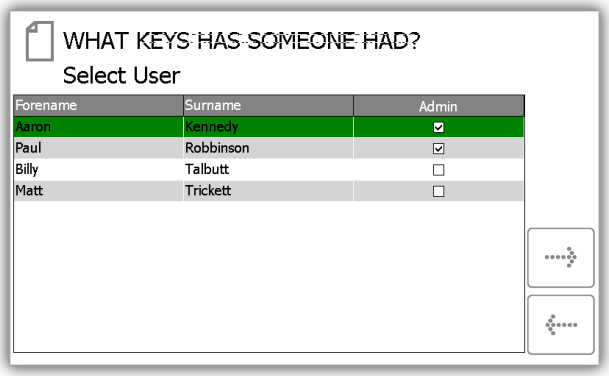
4.5.3 WHAT KEYS HAS SOMEONE HAD?

This report will allow you to see all the keys a particular user has had out of the system.

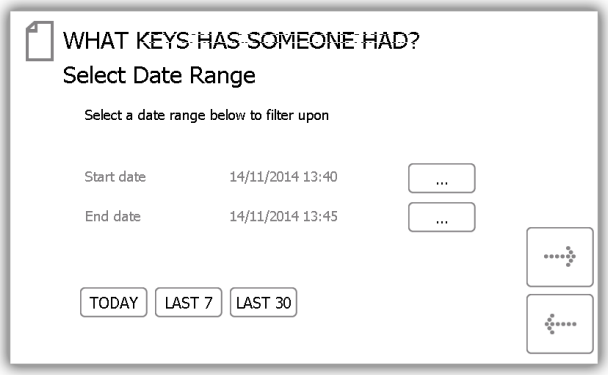
1. From the admin menu select the reports button.
2. In the Users category, select the 'What Keys Has Someone Had?' button.



3. The current user list will then be displayed. Select the desired user and click the forward arrow.



4. 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.

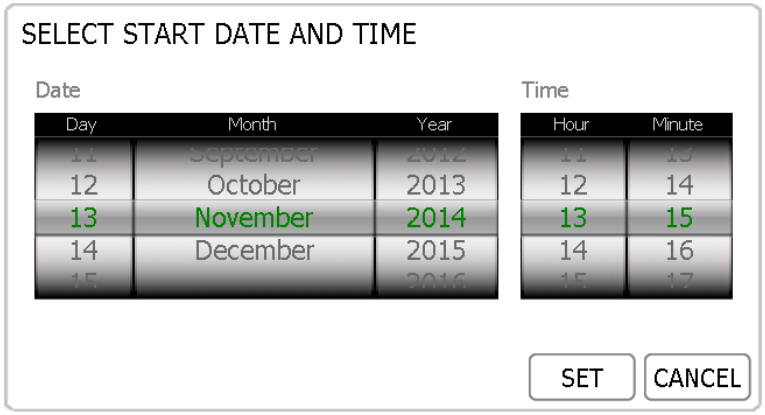


The pre-set buttons will automatically select the date range for you as follows...

- 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.
- The '**All'** button will provide data for the selected report from 01/01/2010 00:00 to ensure all events and transactions are audited.

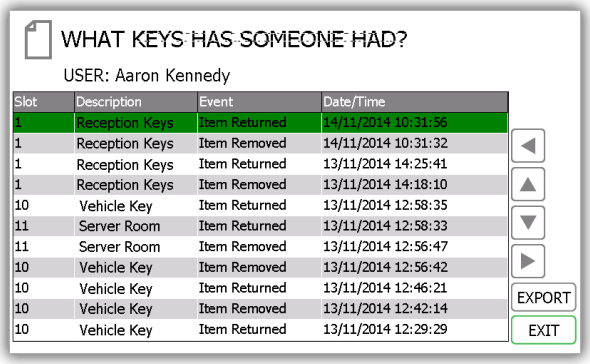
To manually filter the date range, select the button next to the start or end date.

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



5. Once you have selected your desired date range, click the forward button.
6. The report will now generate and display all the keys the specified user has removed between the selected date range.

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

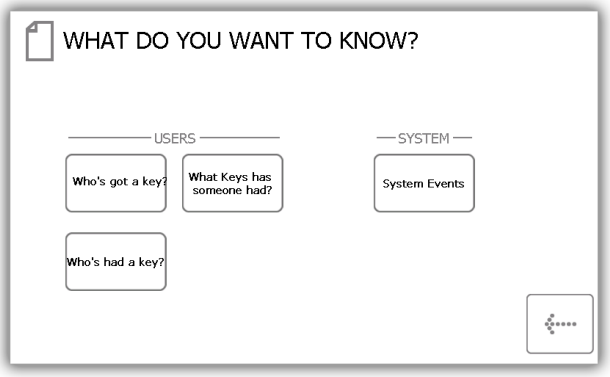


7. You can export this information to a USB memory stick if you wish by clicking the Export button. Please review the Exporting Reports topic at the end of this section for more details.

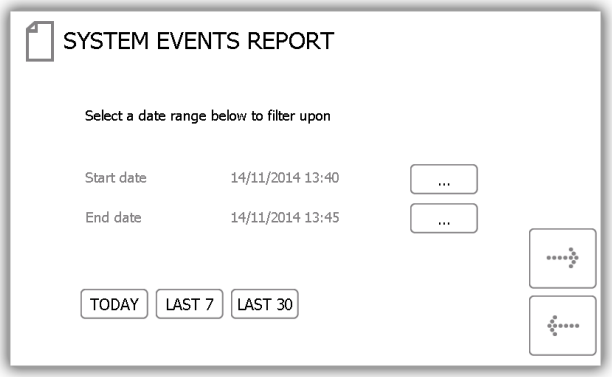
4.5.4 SYSTEM EVENTS

This report will allow you to see all system related events e.g. admin access, reports access, door opened manually etc.

1. From the admin menu select the reports button.
2. In the System category, select the 'System Events' button.



3. 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.

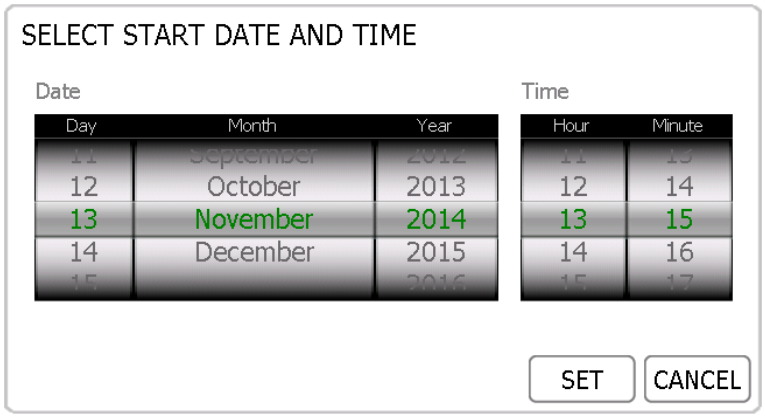


The pre-set buttons will automatically select the date range for you as follows...

- 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.

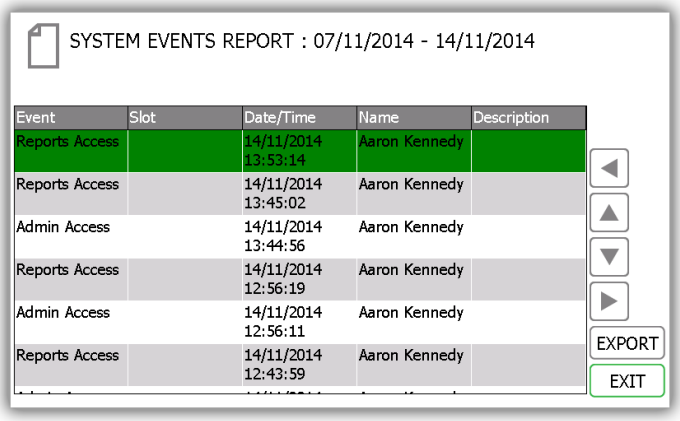
A scrollable control will now allow you select the exact date and time you wish to run the report on.



8. Once you have selected your desired date range, click the forward button.

9. The report will now generate and display all the events that have happened at the system between the selected date range. E.g. Report Access, Admin Access, Door Open, Door Closed, USB Inserted etc.

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



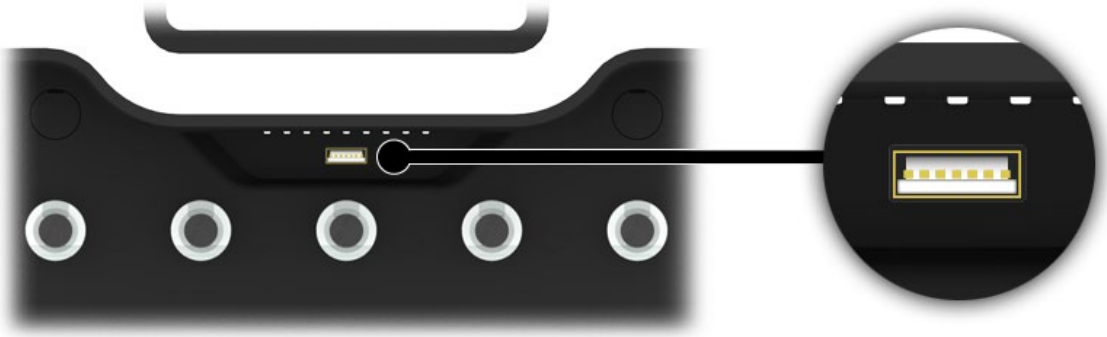
10. You can export this information to a USB memory stick if you wish by clicking the Export button. Please review the Exporting Reports topic at the end of this section for more details.

4.5.5 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.

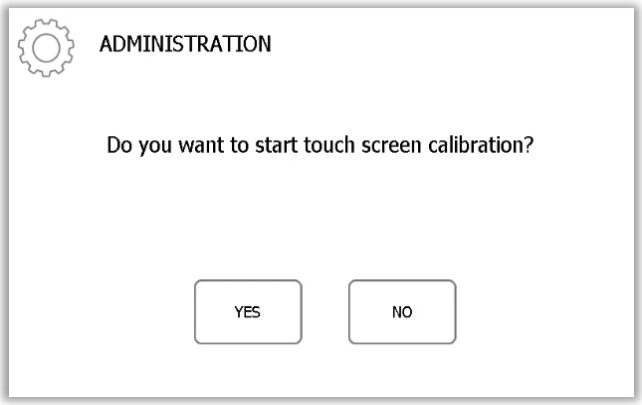
NOTE: Do note remove the memory stick whilst the data is transferring. You may corrupt or even loose the data.

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.

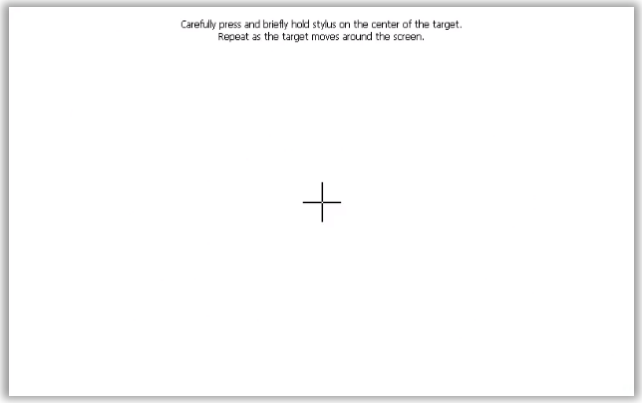
4.6 CALIBRATE

From the admin menu select the calibrate button to perform the calibration of the Traka21 touch screen. To use this function, select the YES button on the screen.



Next touch each point on the screen indicated with a cross. The cross will move around the screen until you have touched all the calibration points.

NOTE: It is recommended that you use a 'Touch Screen Stylus' for this procedure. Do not use anything sharp that could damage the screen.



Once the calibration procedure is finished, the following screen is presented. Tap the screen once more to register and save the calibration data. If you do not tap within 30 seconds then the new calibration data will not be saved.

4.7 IMPORT

It is possible to export and import users key descriptions and permissions to a USB memory stick from the Traka21 application. The import feature is useful if you wish to add large lists of users or keys in one go.

To use the import feature, you would first need to enter all the required user/key details into a Traka Spreadsheet. To obtain the Spreadsheet, you must export your current user/key lists and use the Spreadsheet that it provides you with (note that it is not possible to use a previous exported current user/key list, so always export a new list to edit). Please review the section 'Export 4.7' for more details.

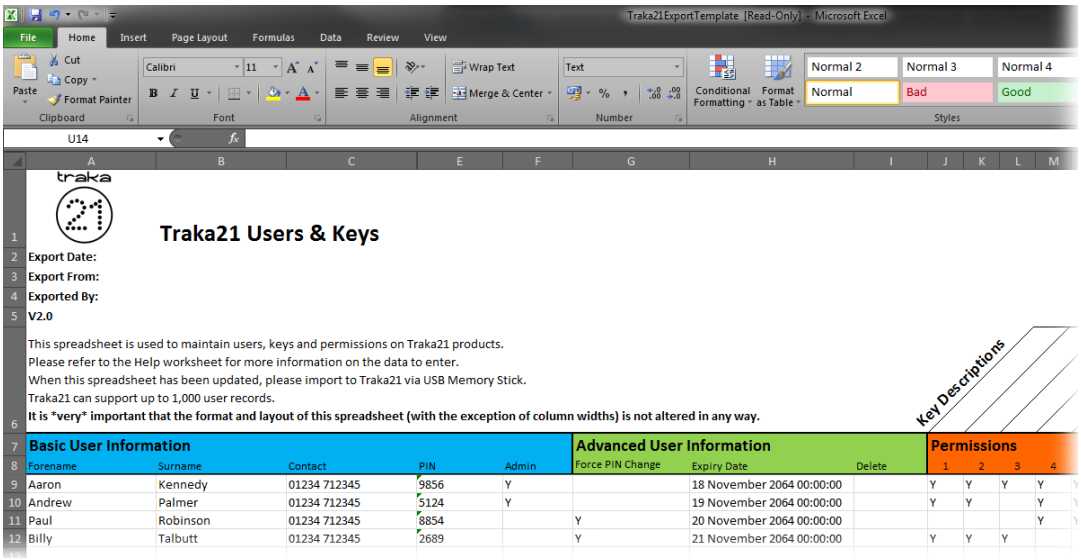
NOTE: Traka21 can support up to one thousand (1000) users.

4.7.1 ENTERING DETAILS INTO THE SPREADSEET

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

1. Download or export the Spreadsheet as mentioned above in section 'Export 4.7'.

2. Open the Spreadsheet on a PC.



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

Basic User Information					Advanced User Information			Permissions				
Forename	Surname	Contact	PIN	Admin	Force PIN Change	Expiry Date	Delete	1	2	3	4	5
Aaron	Kennedy	01234 712345	9856	Y		18 November 2064 00:00:00		Y	Y	Y	Y	Y
Andrew	Palmer	01234 712345	5124	Y		19 November 2064 00:00:00		Y	Y		Y	Y
Paul	Robinson	01234 712345	8854		Y	20 November 2064 00:00:00					Y	Y
Billy	Talbutt	01234 712345	2689		Y	21 November 2064 00:00:00		Y	Y	Y		

Key Permissions

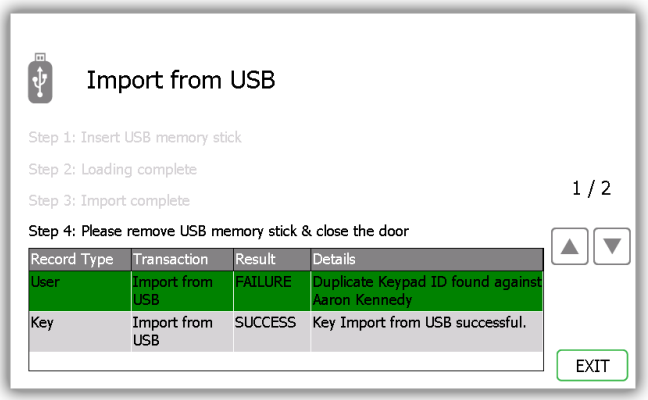
To grant a user access to a key simply put a 'Y' in the corresponding column. You can also assign a description to a key by double clicking above the desired position and entering a description of your choice.

4. When finished save the Spreadsheet onto a memory stick.

4.7.2 FAQ'S

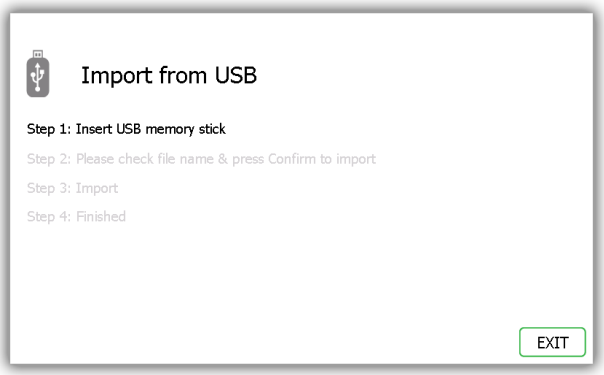
Overwriting Users – When you enter a user's details into the Spreadsheet and that user already exists in the Traka21, the user credentials from the Spreadsheet will be taken as the most recent edits and will overwrite the systems information.

Duplicate PIN's – If a user being imported has the same PIN 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.

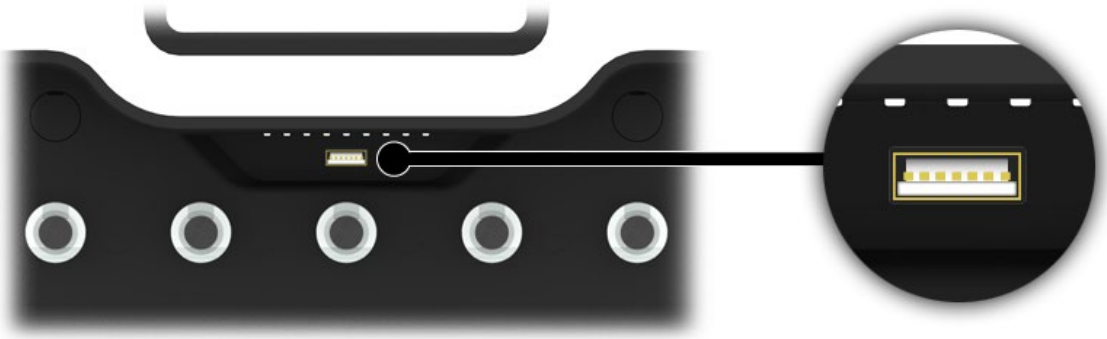


4.7.3 IMPORTING THE INFORMATION TO TRAKA21

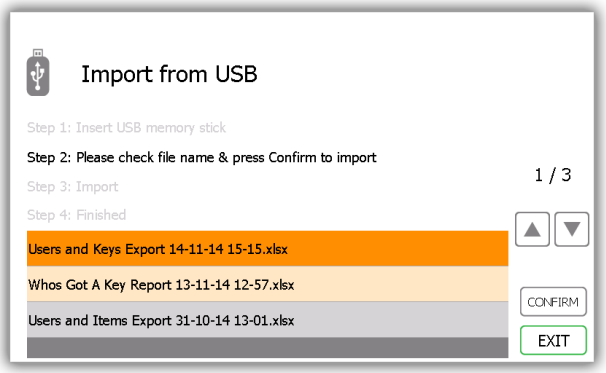
1. Navigate to the admin menu and select the import button.



2. Insert the USB stick into the system.

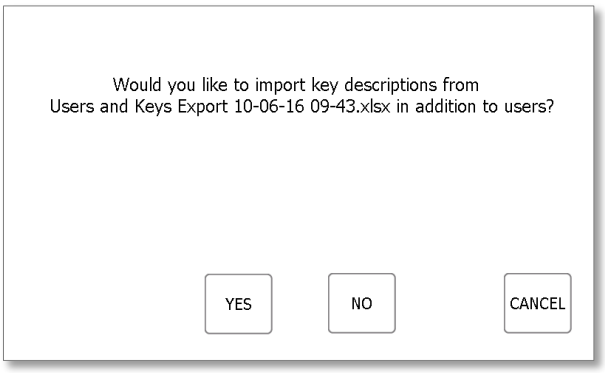


3. Traka21 will display a list of compatible files on the USB stick and prompt you to select one. Make your selection and click confirm.

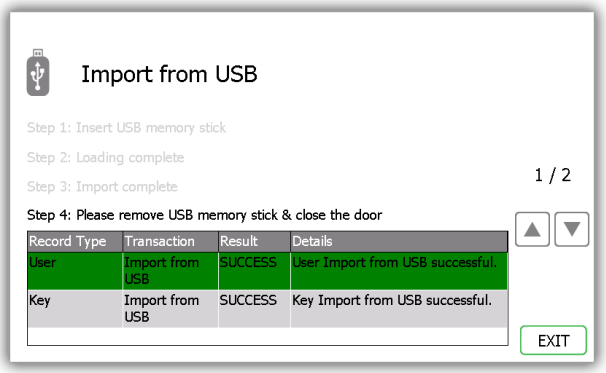


4. The system will ask if you would like to import the new data into the system. Click Yes to proceed, or cancel to go back to the Import menu

NOTE: This will overwrite any information in the system.



5. Once complete the table will display the records that were imported and if it was a success. All the new users/key details will now be in the Traka21 system. You can now remove the USB memory stick.



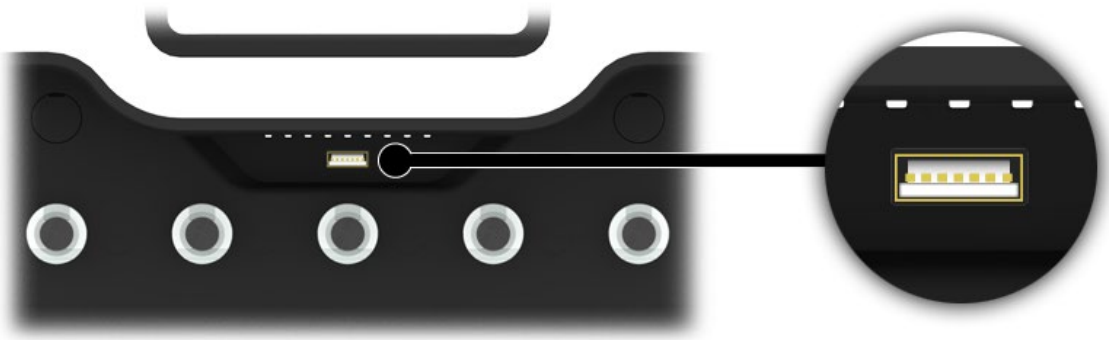
6. Click the exit button to go back to the admin menu. From there click exit again to be taken back to the login screen.

4.8 EXPORT

It is possible to export and import users to a USB memory stick from the Traka21 application. When using the export feature, Traka21 it will export the current user and key details to a Spreadsheet on a USB memory Stick. The Spreadsheet can then be updated and imported to update the system.

1. Navigate to the admin menu and select the export button.

2. Insert the USB stick into the system.



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

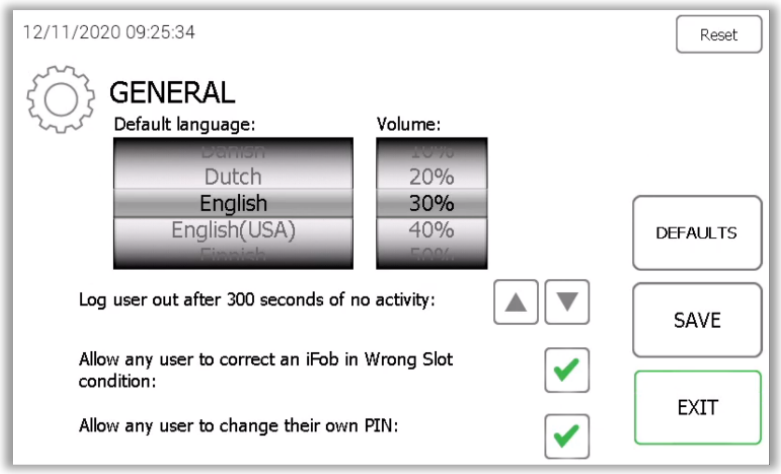
4. Once the exporting process has finished you can remove the USB stick.

5. Click the exit button to go back to the admin menu, from there click exit again to be taken back to the login screen.

4.9 GENERAL

The general screen allows you to access the common settings of the Traka21 system.

1. From the admin menu select the general button.



2. From here you can select the following options.

   a. Default language
   Simply scroll through to find the desired language. See the table at the bottom of this page for all the available languages.
   b. Volume
   Scroll through to adjust the volume of all Traka21 sounds to the desired level.
   c. Log user out after xx or no activity
   This feature allows you to define the amount of time it takes for the system to log the user out after no activity. Using the directional arrows select the appropriate time in increments of 1 second.
   d. Allow any user to correct an iFob in Wrong Slot
   iFob in wrong slot condition – By default this option is enabled which means if an iFob is in the wrong position, any user, not just an administrator, will be asked to move the incorrect iFob to the correct position even is they don't normally have permission to take the key.
   e. Allow any user to change their own PIN
   If this option is enabled, then the 'change PIN' button will be available on the Key Release screen. Refer to section 3.6, 'Change PIN', for more information.

3. To reset the system, see the instructions on the next page for more information.

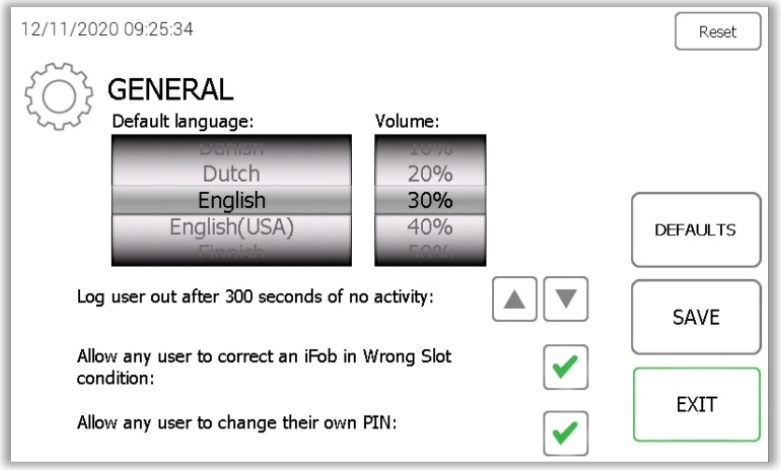
4. To set the general menu options back to the default setting, click the default button.

5. Click the save button.

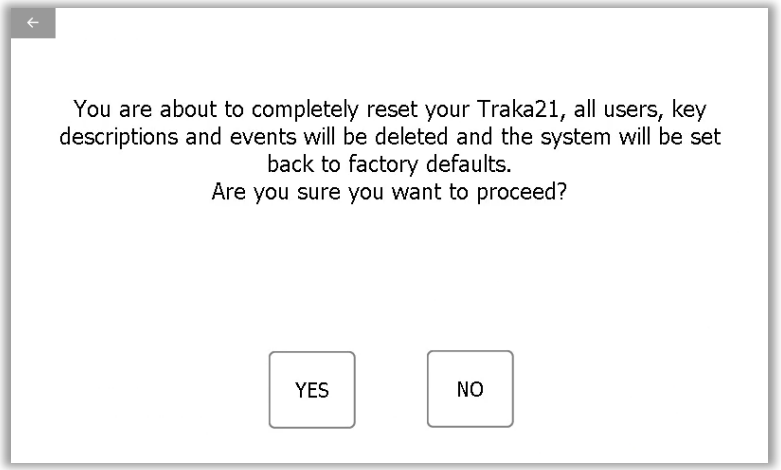
6. When finished click the back button to go back to the admin menu. From there click the exit button to go back to the login screen.

Default Language	Default Language
English (GB)	**Hebrew**
English (US)	**Italian**
Arabic	**Japanese**
Czech	**Norwegian**
Danish	**Polish**
Dutch	**Russian**
Finnish	**Spanish**
French	**Swedish**
German	**Portuguese**

Select the reset button to completely reset the Traka21 system.



You will next see a page that warns you that all user, key descriptions and events will be deleted, and the system will be set back to factory defaults if you proceed.



If you decide to proceed the following screen is displayed while the reset process is taking place.

Once the Traka21 system has been reset then it will need to be completely set up from the beginning once again.

4.10 TIME

Here you can set the date and time of the system.

1. From the admin menu select the time button.

2. To change the date and time simply scroll through the menus and click the save button to keep you changes.

3. When you have finished, click the back button to go to the admin menu. From there, click exit to return to the login screen.

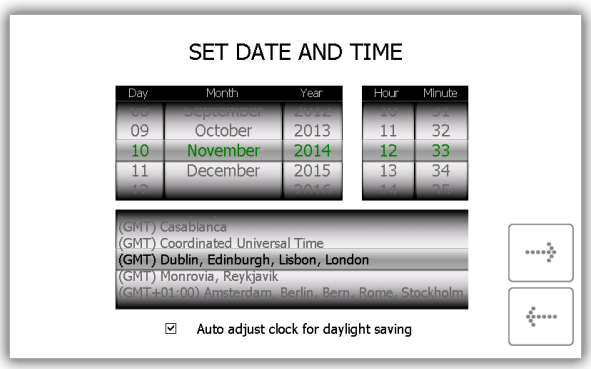
4.11 SETUP WIZARD

From the admin menu select the setup wizard. The setup wizard option will mimic the initial setup that occurred when the Traka21 was first switched on. It will allow you to reselect the language and the date & time of the system. It will also show you all of the information screens you saw when you setting up the system originally.

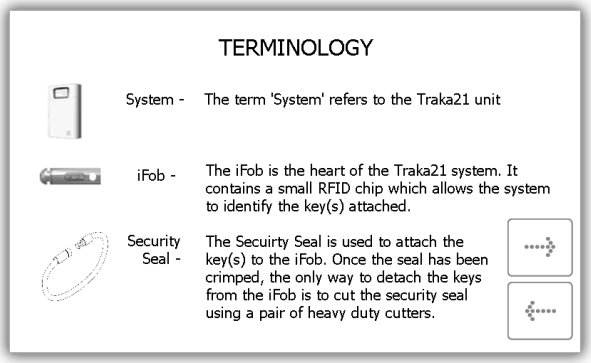
NOTE: you will not be able to add an admin user in this setup wizard.

1. From the admin menu click the Setup Wizard button.

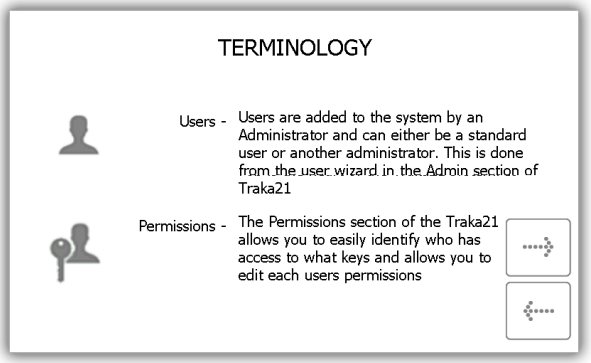
2. Next reselect the date, time & time zone and click the forward button.



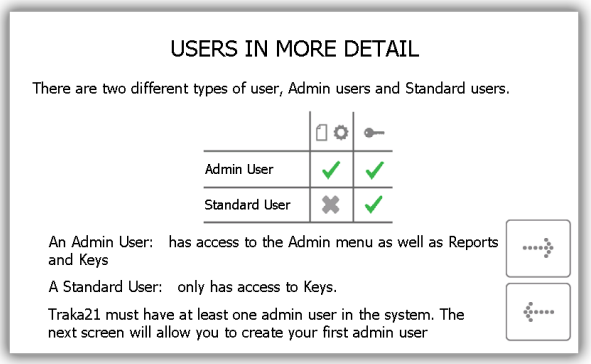
3. The next two pages are a breakdown of Traka21 terminology. Read this page and click the forward button.



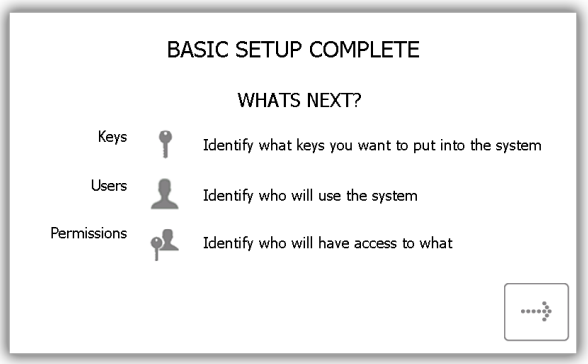
4. Read the second terminology page and click the forward button.



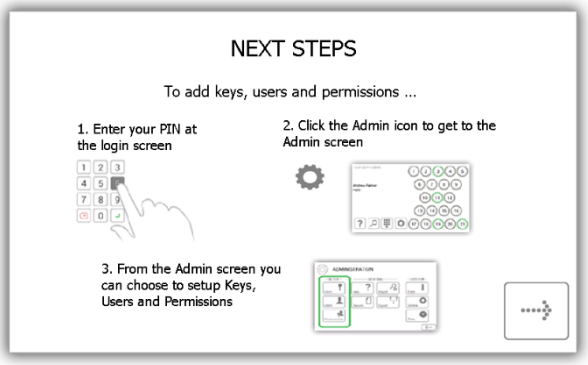
5. This page explains the difference between standard and admin users. Read this page and click the forward button.



6. The basic setup is now complete. This window will give instructions on what you need to do next. Read this then click the forward button.



7. 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.

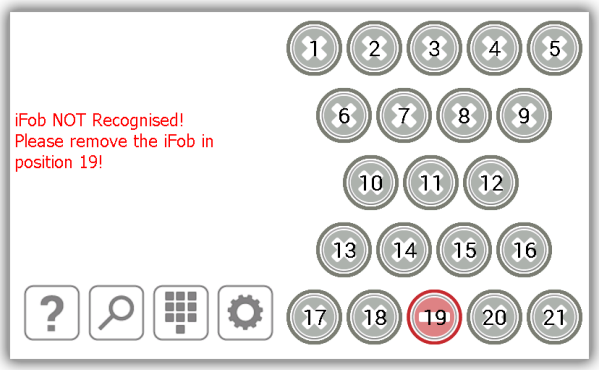


5. REPLACING IFOBS

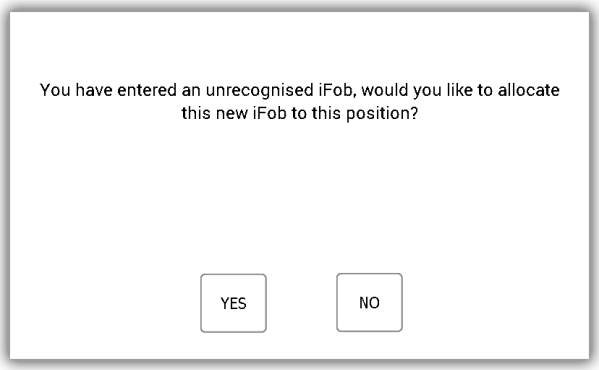
If the need to replace an iFob should arise i.e. an iFob has been broken or lost, you should follow the steps below to replace the old iFob with a new one.

NOTE: As the Traka21 is provided with 21 iFobs you will need to order more iFobs from Traka or your distributor/supplier.

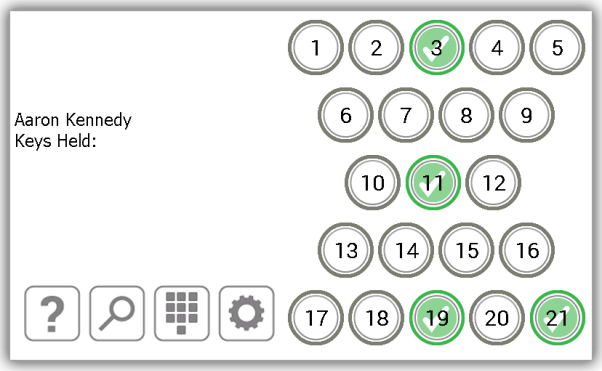
1. An administrator will need to login to the system.
2. Insert the new iFob into the position you want to assign it to.



3. The system will ask if you want to assign this new iFob to the position.



4. Click Yes, and the iFob will immediately become usable.



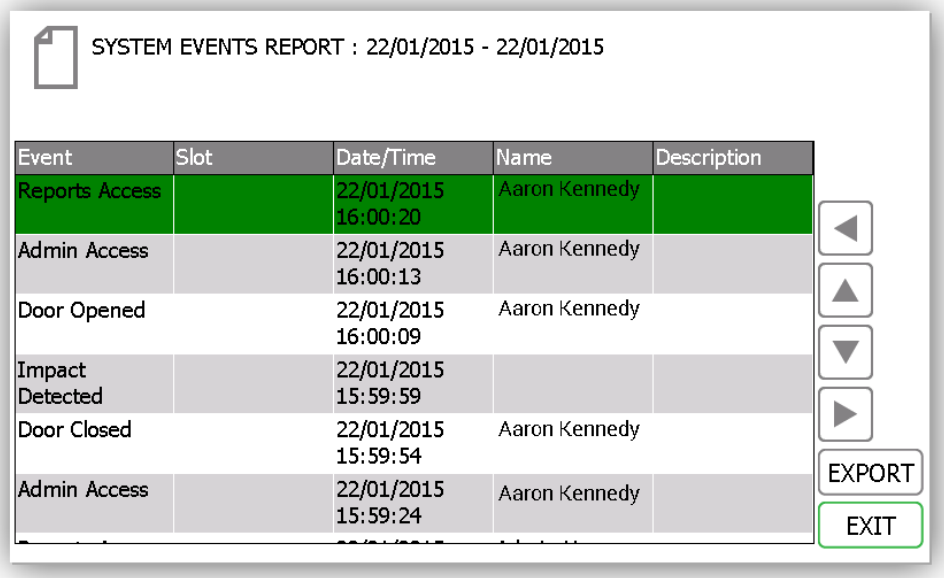
6. SYSTEM IMPACT ALARM

The Traka21 has a built in alarm system that will automatically sound when the system detects an impact. This alarm will last for two minutes before it stops on its own. It can only be deactivated before the two minutes are up when a user with valid log in credentials access the system.

6.1 SYSTEM EVENTS REPORT

Once an impact is detected the system will record a system event.

1. To view this report log into the system as an administrator.
2. Select the Admin button.
3. Select the Reports button.
4. From here click the System Events button.
5. Please review the System Events topic for details on how to run this particular report.
6. Once the report has been generated you will notice an event named Impact Detected.



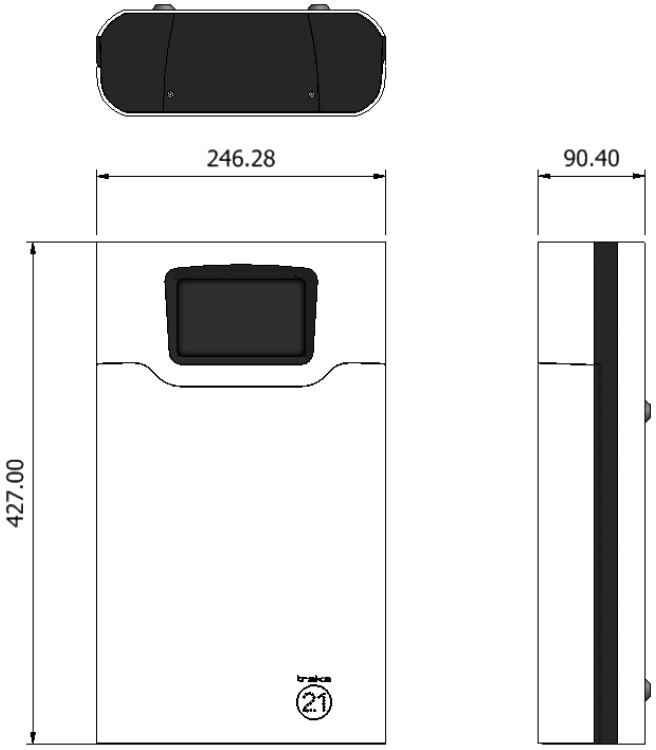
7. TRAKA21 TECHNICAL DETAILS

Model: KC-1-0156

7.1 SYSTEM SIZE

Please see below a list and diagram of the Traka21's height, width and depth.

- Height – 427.00mm
- Width – 246.28mm
- Depth – 90.40mm



7.2 SYSTEM WEIGHT

Traka21 with iFobs (without keys or optional battery) is 3.94Kg. Optional battery is an additional 0.63 Kg.

7.3 OPERATING TEMPERATURE RANGE & ALTITUDE

Operating temperature range: 0°C to +40°C (32°F to 104°C) at 95% relative humidity non-condensing
Maximum operating altitude: 2,000m

7.4 POWER DETAILS

Traka21 uses a 15 ~ 24W AC-DC Single Output power supply. Please see the technical details below.

- Input – 100-240VAC, 50-60Hz, 0.7A
- Output – 15V ⎓ 1.6A
- Safety Standards – UL60950-1, CSA C22.2, TUV EN60950 -1, CCC GB4943 approved

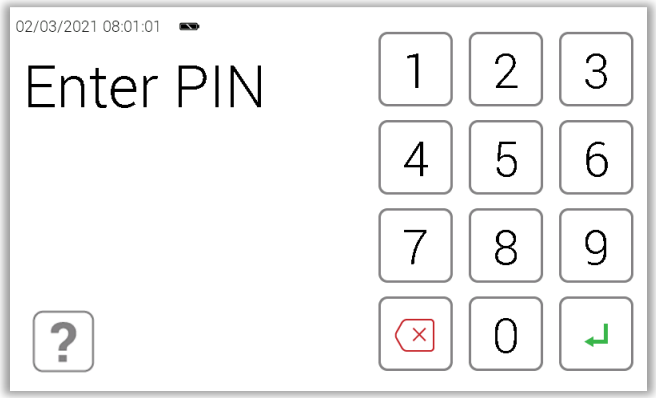
8. BACKUP BATTERY

The Traka21 is supplied with an optional backup battery with systems inside the UK. A system outside the UK will need to source a battery using the information in the Battery Specification section below.

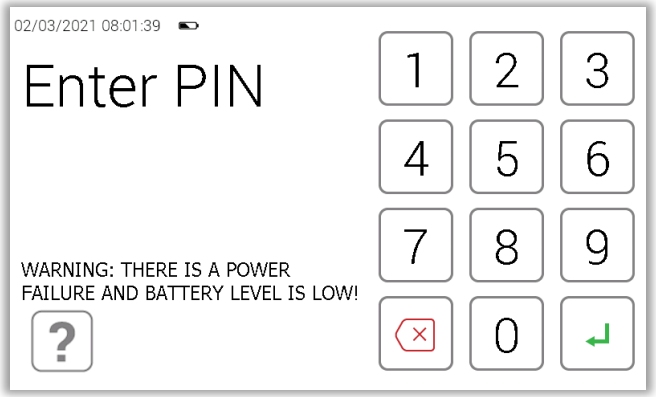
8.1 BATTERY STATUS

The battery status can be determined from the log in screen of Traka21. The status of the battery is displayed in the follow ways.

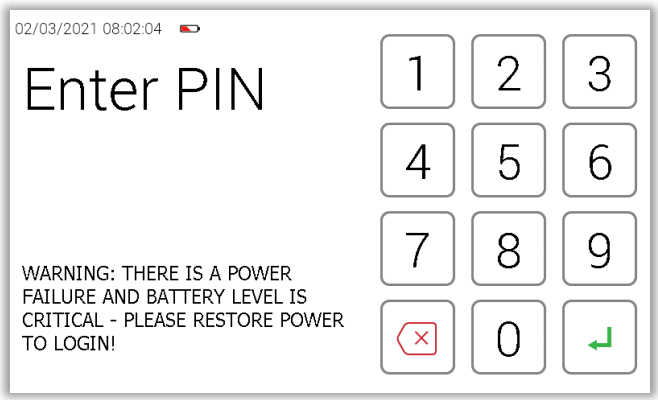
- The battery is full



- The battery is low



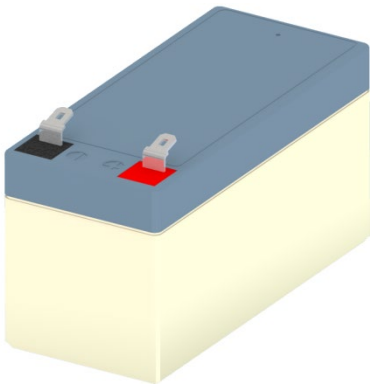
- The battery is critical



8.2 BATTERY SPECIFICATION

The backup battery is kept charged by the system when running from the mains so that it is ready to be used should there be a power failure.

The battery usually has a service life of 5 years. If it needs replacement, use a 12V, 1.2AH Valve Regulated Lead Acid Battery approved for IEC 61056-1 or equivalent.



NOTE: Please remember the following safety guidelines for battery disposal and storage:

Do not replace the battery with an incorrect type.

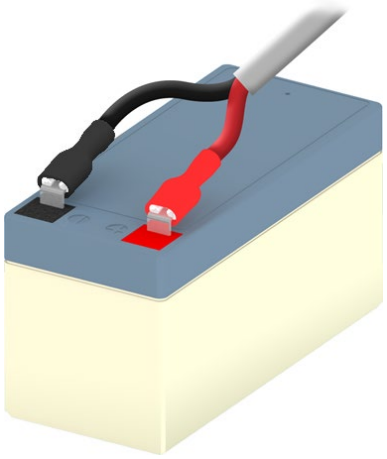
Do not dispose of the battery into a fire or a hot oven, or mechanically crush or cut a battery, as this can result in an explosion.

Do not leave the battery in an extremely high-temperature environment, as this can result in an explosion or the leakage of flammable liquid or gas.

8.3 BATTERY CONNECTION CODE

Connect the **Red Connector** to the **Red Battery Terminal** (indicated with the **+** symbol)

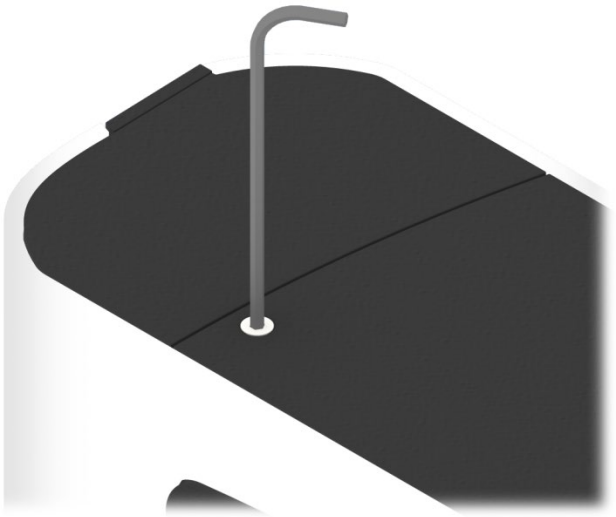
Connect the **Blue Connector** to the **Black Battery Terminal** (indicated with the **–** symbol)



8.4 BATTERY INSTALLATION

To install the battery you will need to remove the top panel of the system.

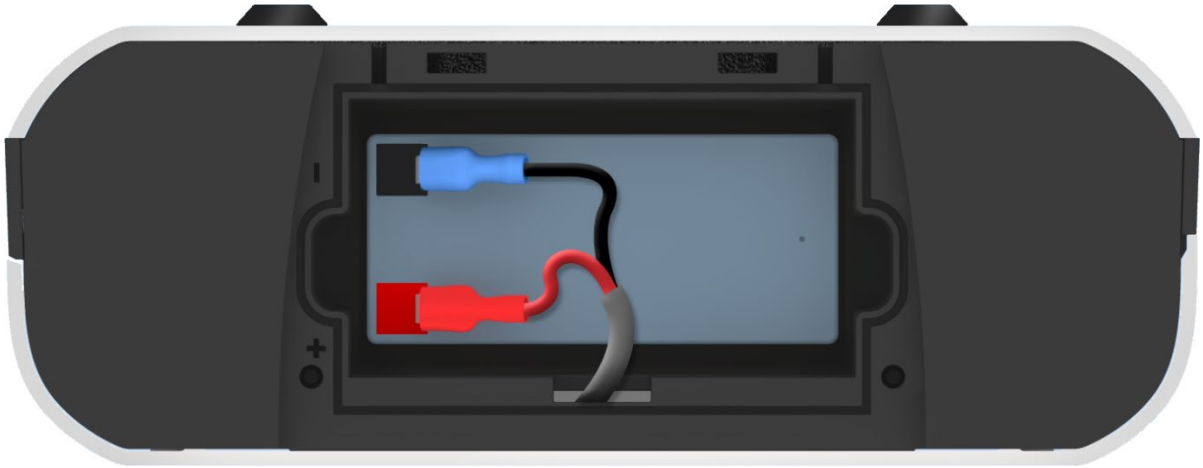
1. Unscrew the cover plate using a 2mm Allen Key.



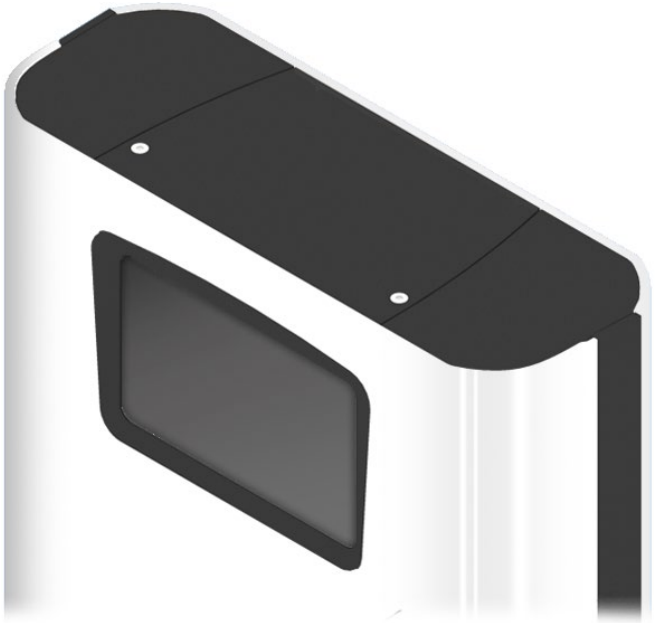
2. Remove the cover plate and screws.

3. Place the battery inside the compartment. Inside the system, embedded into the material are + and – symbols to help you properly orientate the battery correctly. The red terminal of the battery should face the + and the black terminal should face the -.

4. Connect the battery to the battery cable. Use the connection code in the section above for guidance.



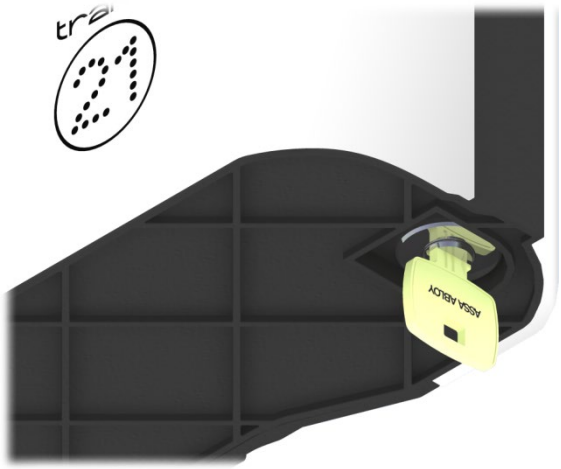
5. Replace the cover and screws using the 2mm Allen Key.



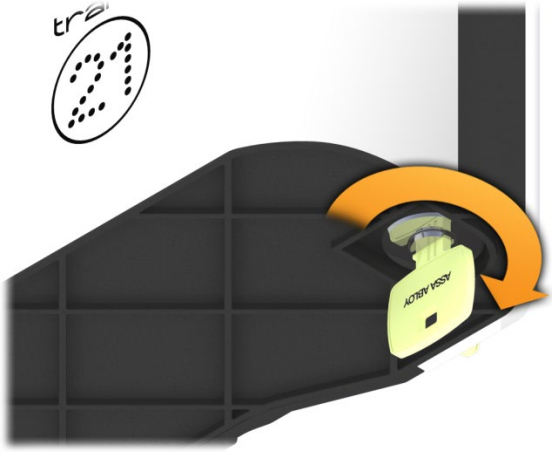
9. HOW TO REMOVE KEYS IN A POWER FAILURE

If there should be a power failure and your system does not have a battery. You will need to manually access and remove the keys.

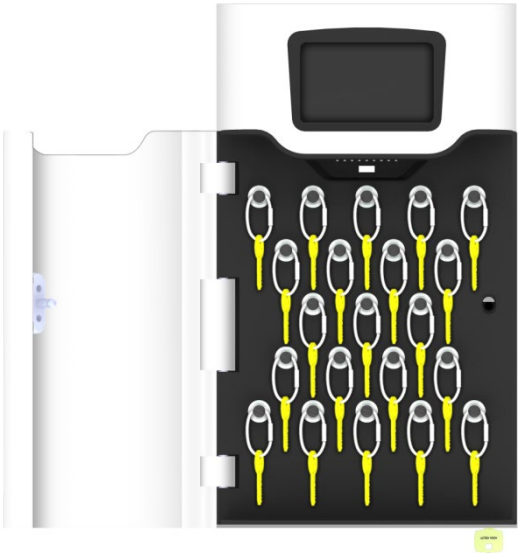
1. Insert the override key into the bottom of the system.



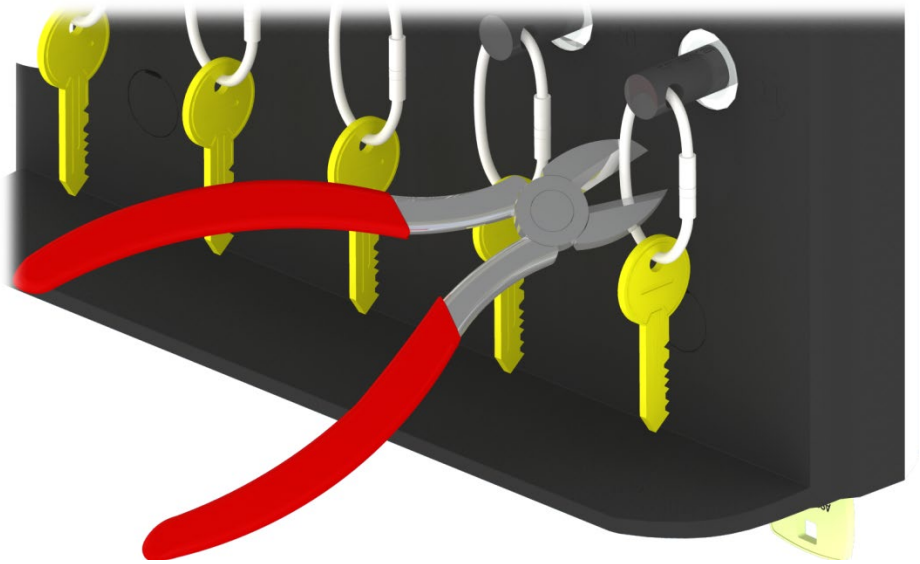
2. Turn the key 90° counter clockwise.



3. The door will now open, granting you access to the keys.



4. Using a pair of heavy duty cutters, you will need to cut the security seals for the keys you require.



5. Remove the Keys from the security seal.

10. TRAKA21 CLEANING GUIDANCE

10.1 INTRODUCTION

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 Traka21 Cabinet with wet hands as this may damage the touch screen.

10.2 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 absorbant cloth immediately

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

10.3 CLEANING THE TOUCH SCREEN

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

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

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

10.4 IFOBS

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

10.5 WARRANTY STATEMENT

Failure to comply with these cleaning instructions could damage the Traka21 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.

11. REGULATORY NOTICES

11.1 FCC COMPLIANCE

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modification not expressly approved by the manufacturer could void user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

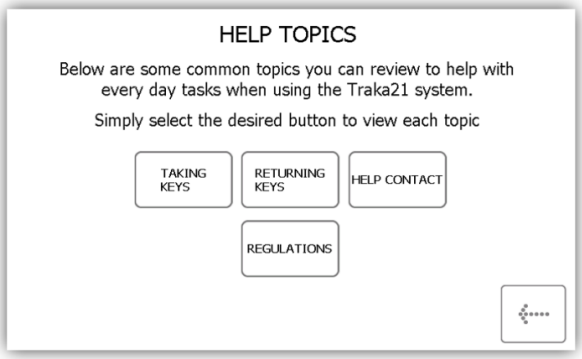
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

11.1.1 INFORMATION IN THE TRAKA21 APPLICATION

FCC regulatory information may be accessed directly on the product by viewing the appropriate help topic. Any user can access this information by selecting the help button from the login screen.

1. If the touch screen is black then the system is in power save mode. Simply touch the screen to 'wake the system up'
2. From the login screen select the help button 

3. At the help screen there are four options to choose from, select the Regulations button.



11.2 INDUSTRY CANADA

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Model: KC-1-0156

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

12. TECHNICAL SUPPORT

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

www.traka21.com

13. 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